

SX-GATE

User Guide

1 Preface.....	6
1.1 Guidelines.....	6
1.2 Acknowledgements.....	7
1.3 Trademarks.....	10
2 Precautions and Guidelines.....	11
2.1 Warning.....	11
2.2 For Your Safety.....	12
2.3 The Power Plug.....	13
2.4 Installation Site.....	14
3 Preparing the new SX-GATE unit.....	15
3.1 Packaging.....	15
3.2 Accessories Provided.....	16
3.3 Connecting the device.....	17
3.3.1 Connecting to ADSL dial-up lines.....	17
3.3.2 Connecting to an external router / xDSL-leased line Internet connection.....	18
3.3.3 Connecting to the local network (LAN).....	19
3.3.4 Connection with the power supply.....	20
4 Start-up.....	21
4.1 Prerequisites.....	21
4.2 Switching on and booting.....	22
4.3 Setting up SX-GATE's IP address.....	23
4.3.1 Changing the IP address with the display.....	23
4.3.2 Changing the IP address with the web browser.....	24
4.4 Check the connection to SX-GATE.....	25
5 First settings.....	26
5.1 Accessing the web administration interface.....	26
5.2 Basic configuration.....	27
6 Configuring computers in the LAN.....	28
6.1 Network parameters.....	28
6.2 Setting up the web browsers.....	29
7 Home.....	30
7.1 Getting started.....	31
7.2 Ressources.....	31
7.3 Network data rates.....	31
7.4 Disk space.....	31
7.5 Updates.....	32
7.6 Services.....	32
7.7 SX-GATE info.....	32
7.8 SX-GATE status.....	32
7.9 Ethernet Cards.....	32
7.10 Mail server.....	32
7.11 Live log.....	33

8 My Account.....	35
8.1 Change password.....	35
8.2 Email options.....	36
8.3 Groupware.....	42
8.4 Contact.....	43
9 Statistics.....	45
9.1 System load.....	45
9.2 Network.....	46
9.2.1 Connections.....	46
9.2.2 Throughput.....	46
9.2.3 Bandwidth.....	46
9.3 Firewall.....	48
9.3.1 Packet filter.....	48
9.3.2 IDS/IPS.....	48
9.4 Mail server.....	49
9.5 Proxies.....	50
9.5.1 Web proxy.....	50
9.5.2 Reverse proxy.....	51
9.6 Web server.....	52
10 Monitoring.....	53
10.1 Log files.....	53
10.2 Tools.....	58
10.3 Network.....	65
10.4 VPN.....	68
10.5 Firewall.....	72
10.6 DHCP.....	73
10.7 Mail server.....	74
10.8 Web proxy.....	78
11 Definitions.....	80
11.1 IP objects.....	80
11.2 Protocols.....	89
11.3 Periods.....	92
11.4 Domain lists.....	93
11.5 URL filter lists.....	96
12 System.....	104
12.1 Setup.....	104
12.2 Services.....	113
12.3 User administration.....	121
12.3.1 Settings.....	122
12.3.2 Users.....	127
12.3.3 Groups.....	150
12.4 Certificate manager.....	154
12.4.1 CA certificates.....	154
12.4.1.1 SX-GATE CA.....	154

12.4.1.2 SX-GATE CA - Certificates.....	158
12.4.1.3 Custom CAs.....	168
12.4.2 Keyring.....	169
12.4.3 MPKI profiles.....	183
12.5 Backup.....	185
12.6 Update.....	195
12.7 Apps.....	198
12.8 Management server.....	199
12.9 License.....	206
12.10 Shutdown / Reboot.....	207
13 Wizards.....	208
13.1 LAN integration.....	208
13.2 Internet access.....	213
13.3 Proxy configuration.....	222
13.4 Email configuration.....	231
13.5 IPsec VPN.....	250
13.6 Support access.....	257
14 Modules.....	259
14.1 Network.....	259
14.1.1 Settings.....	259
14.1.2 Interfaces.....	265
14.1.2.1 ADSL/Mobile broadband (adsl).....	267
14.1.2.2 Ethernet (eth).....	281
14.1.2.3 VLAN 802.1Q (vlan).....	297
14.1.2.4 WLAN (wlan).....	309
14.1.2.5 L2TP.....	317
14.1.2.6 Wireguard (wg).....	318
14.1.2.7 OpenVPN Client (ovpnc).....	325
14.1.2.8 OpenVPN Server (ovpns).....	328
14.1.2.9 OpenVPN Server (ovpns) - Per-client setup.....	333
14.1.2.10 IPsec VPN (ipsec).....	334
14.1.2.11 IPsec VPN (ipsec) - Connections.....	337
14.1.2.11.1 Connection with Server.....	339
14.1.2.11.2 Connection with AWS.....	347
14.1.2.11.3 Connection with Client.....	354
14.1.2.11.4 Connection with Windows IKEv2.....	359
14.1.2.11.5 Connection with XAuth Client.....	362
14.1.2.11.6 Connection with L2TP Client.....	367
14.2 Firewall.....	372
14.2.1 Settings.....	372
14.2.2 Policies.....	375
14.2.3 Bridge.....	398
14.3 DHCP.....	411
14.4 DNS.....	422
14.4.1 Settings.....	422
14.4.2 Zones.....	426

14.4.2.1 domain.....	428
14.4.2.2 IPv4 reverse lookup zone.....	432
14.4.2.3 IPv6 reverse lookup zone.....	436
14.5 Mail Server.....	440
14.5.1 POP/IMAP server.....	440
14.5.2 SMTP settings.....	442
14.5.3 SPAM/Virus/Malware.....	456
14.5.4 Archive.....	482
14.5.5 TLS Encryption.....	491
14.5.6 S/MIME gateway.....	494
14.5.7 Domains.....	504
14.6 POP/IMAP Client.....	515
14.6.1 Settings.....	515
14.6.2 Servers.....	515
14.7 Web proxy.....	523
14.7.1 Settings.....	523
14.7.2 URL filter.....	538
14.7.3 Content filter.....	542
14.8 Reverse proxy.....	552
14.8.1 Settings.....	552
14.8.2 Ports.....	554
14.8.2.1	555
14.8.2.2 - Virtual hosts.....	559
14.9 More Proxies.....	570
14.9.1 FTP proxy.....	570
14.9.2 SIP proxy.....	572
14.9.3 POP3/SMTP proxy.....	574
14.9.4 SOCKS proxy.....	576
14.10 HTTP server.....	578
14.11 FTP server.....	582
14.12 SNMP server.....	583
14.13 Logging.....	585
14.14 Virusscanner.....	592
14.15 Time server.....	596
15 Configuration of an L2TP IPsec VPN client.....	598
15.1 Microsoft Windows.....	598
15.1.1 Automatic configuration.....	599
15.1.2 Manual configuration.....	602
15.2 Mac OS X.....	618
15.3 Apple iPhone.....	619
16 Contact.....	622
17 SX-GATE Support.....	623

1 Preface

Thank you for choosing the SX-GATE product. This device includes a router, Internet appliance server, firewall and e-mail server... and all concentrated in just one box! SX-GATE also offers you a whole choice of other features, depending on the specific SX-GATE model. In order for you to optimally use and operate this product, we have tried to make this manual as easy as possible. Therefore please take the time to carefully read through this manual as some sections relate to preceding chapters.

As the SX-GATE product is continually being developed, we recommend that you obtain a service contract which will supply you with product updates and upgrades and plenty of new functions, all free of charge. You should also register your product with us so that we can quickly help you in cases of support.

Due to constant improvements, certain parts of this manual may not be complete. In this case please consult our homepage <http://www.sx-gate.de> to obtain any missing information.

If you experience problems configuring SX-GATE you cannot solve yourself, please contact the support numbers. All information and contacts are provided in chapter *Contact* [p.622].

1.1 Guidelines

This manual is composed with great care and accuracy. However, XnetSolutions KG accepts absolutely no guarantee or liability regarding completeness and flawless content.

Since this device provides critical security features, it is important, that all settings are monitored and checked when first set up.

This handbook describes all variations of SX-GATE. Please take note that the functionality of each model is different. If any functionality is missing on your device which is described in this manual, it can be reordered as long as it depends on software. In this situation please ask your sales partner (see chapter *Contact* [p.622]). Depending on the hardware setup, some features may not work. Your sales partner will also be able to advise you here.

XnetSolutions KG reserves the right to make technical alterations to the device without advance notice.

1.2 Acknowledgements

This product includes software developed by Christos Zoulas

This product includes software developed by Craig Metz

This product includes software developed by Daisuke Okajima and Kohsuke Kawaguchi (<http://relaxngcc.sf.net/>).

This product includes software developed by David Corcoran <corcoran@linuxnet.com> <http://www.linuxnet.com> (MUSCLE)

This product includes software developed by Emmanuel Dreyfus

This product includes software developed by Gunnar Ritter and his contributors

This product includes software developed by IAIK of Graz University of Technology.

This product includes software developed by Inferno Nettverk A/S, Norway

This product includes software developed by Jim Paris

This product includes software developed by Lars Fenneberg

This product includes software developed by Manuel Badzong

This product includes software developed by Marko Myllynen

This product includes software developed by Pedro Roque

This product includes software developed by Reuben Hawkins

This product includes software developed by The original development of BIND 9 was underwritten by the following organizations: Sun Microsystems, Inc., Hewlett Packard, Compaq Computer Corporation, IBM, Process Software Corporation, Silicon Graphics, Inc., Network Associates, Inc., U.S. Defense Information Systems Agency, USENIX Association, Stichting NLnet - NLnet Foundation, Nominum, Inc.

This product contains software (<https://github.com/creack/pty>) developed by Keith Rarick, licensed under the MIT License.

This product contains software (<https://github.com/kr/pty>) developed by Keith Rarick, licensed under the MIT License.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)

This product includes data from The Université Toulouse 1 Capitole "Blacklist UT1", maintained by Fabrice Prigent (<http://dsi.ut-capitole.fr/blacklists/>), available under the Creative Commons Attribution-ShareAlike 4.0 license. The data used in this product is available from <http://update.linogate.de/blacklists/>.

This product includes software developed at CoreOS, Inc. (<http://www.coreos.com/>).

This product includes software developed at Docker, Inc. (<https://www.docker.com>).

This product includes software developed by Adam Glass and Charle Hannum.

This product includes software developed by Berkeley Software Design Inc.

This product includes software developed by Bill Paul.

This product includes software developed by Chris Provenzano.

This product includes software developed by Christopher G. Demetriou for the NetBSD Project.

This product includes software developed by David A. Holland

This product includes software developed by HD Associates, Inc

This product includes software developed by HD Associates, Inc and Jukka Antero Ukkonen.

This product includes software developed by Inferno Nettverk A/S, Norway.

This product includes software developed by John Birrell.

This product includes software developed by Kawasaki LSI.

This product includes software developed by Kungliga Tekniska Högskolan and its contributors.

This product includes software developed by Niels Provos.

This product includes software developed by Paul Kranenburg.

This product includes software developed by Softweyr LLC, the University of California, Berkeley, and its contributors.

This product includes software developed by Trimble Navigation, Ltd.

This product includes software developed by Yen Yen Lim an North Dakota State University

This product includes software developed by the Computer System Engineering Group at Lawrence Berkeley Laboratory.

This product includes software developed by the Computer Systems Laboratory at the University of Utah.

This product includes software developed by the Kungliga Teknisk Hgskolan and its contributors.

This product includes software developed by the Politecnico di Torino, and its contributors.

This product includes software developed by the University of California, Lawrence Berkeley Laboratory.

This product includes software developed by the University of Michigan, Meri Network, Inc., and their contributors.

This product includes software developed for the NetBSD Project. See <http://www.NetBSD.org/> for information about NetBSD.

This product includes software developed or owned by Calder International, Inc.

This product includes software written by Tim Hudson (tjh@cryptsoft.com)

This product includes software written by Tim Hudson (tjh@mincom.oz.au)

This product includes software developed by freebxml.org (<http://www.freebxml.org/>).

This product includes software developed by the NetBSD Foundation, Inc. and its contributors.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit

This product includes software developed by the University of California, Berkeley and its contributors.

This product includes software developed by the University of California, Lawrence Berkeley Laboratory and its contributors

1.3 Trademarks

All companies and products that are named in this document are registered trademarks of their respective owners. SX-GATE is a registered trademark of XnetSolutions KG. The naming of unlisted trademarks does not necessarily mean their free availability.

Copyright ©, XnetSolutions KG

2 Precautions and Guidelines

Before you start to operate SX-GATE, please read through the following sections very carefully.

2.1 Warning

To prevent fire and electric shocks please keep this device away from rain and wet areas.

2.2 For Your Safety

Do not open the device casing or try to operate it while open under any circumstances, since this may cause an electrical shock. Furthermore, serious damage may be caused to the device itself. There are no parts inside the device which should be tampered with by non-specialists. Please refer to customer service with regard to upgrades or repairs.

2.3 The Power Plug

Do not try and use the power plug with moist or wet hands. Keep the network cable away from heat and do not place any heavy objects on it. If the device starts to emit smoke, unusual noises or smells, remove the power plug immediately and contact customer services.

2.4 Installation Site

Avoid installation in direct sunlight, near hot objects or in areas with a high temperature (more than 35°C), or areas that are moist (more than 90%) and dusty. Do not try and set up the device where vibrations may be present. Use a flat surface, otherwise the inside of the device will be prone to damage. Keep SX-GATE away from magnetic areas or areas that contain magnet, e.g. Speakers.

3 Preparing the new SX-GATE unit

3.1 Packaging

Remove the device carefully from the packaging. Keep the carton with all the packaging material for later transportation. If the device is exposed to extreme temperature fluctuations (e.g. from a cold vehicle to a heated room), wait approx. 1 hour so it can become acclimatised. This is advisable since condensation may have built up in the device which can cause serious damage.

3.2 Accessories Provided

Check the packaging contents with the following list. If any parts are missing, please contact your dealer (see chapter *Contact* [p.622]).

- SX-GATE (Internet-Firewall-Gateway)
- Power cable (220V)

3.3 Connecting the device

The connection methods described in the following chapters assume, that SX-GATE and the installation environment provide these connection sockets. The configuration of the device may vary in different stages of extension.

3.3.1 Connecting to ADSL dial-up lines

SX-GATE supports the following ADSL connections:

- ADSL / VDSL with PPP-over-Ethernet (PPPoE), also via VLAN
- ADSL with PPP-over-ATM (PPPoA) via modem with PPTP-to-PPPoA-Relay

We recommend to connect the DSL modem directly through an otherwise unused network interface of SX-GATE. For the Internet connection usually a second network interface is provided in the system. The interface is called "eth1" and may also be labeled with the acronyms "DSL" or "WAN".



The connection to an ADSL dial-up has to be set up via an external DSL modem. A suitable modem will be provided by your ISP. If a router with integrated DSL modem has been provided, it is recommended to put the router into modem mode (PPPoE passthrough).

3.3.2 Connecting to an external router / xDSL-leased line Internet connection

SX-GATE supports the connection to Ethernet networks with transfer rates of 10, 100 or 1000 Mbit/s.

Usually, the second built-in network interface is provided for an Internet connection. The interface is called "eth1" and may also be labeled with the acronyms "DSL" or "WAN". Connect this interface directly with the external router. This might require a crossover network cable which is not included. Alternatively you can connect via an additional switch. Please use a dedicated switch and not the LAN switch in this case.

3.3.3 Connecting to the local network (LAN)

SX-GATE supports Ethernet networks with 10, 100 or 1000 Mbit/s transfer rates.

SX-GATE is connected to your LAN via the first network interface of the system. The interface is called "eth0" and may also be labeled with the acronym "LAN". Connect this interface with an unused port of your LAN switch.



Make sure that you do not reverse the interfaces! Confusing can result in SX-GATE not being addressable!

3.3.4 Connection with the power supply

Use the supplied network cable or power supply to connect the device to the power outlet. Please note, that operation of the device is only possible at 230 volts alternating current (AC).

We recommend to connect the device with an uninterruptible power supply (UPS) unit. Otherwise, in case of a sudden power failure, the SX-GATE configuration and respective hardware components could be affected.

4 Start-up

4.1 Prerequisites

As all SX-GATE settings are made via web interface, a computer device with a web browser like for example Microsoft Internet Explorer or Mozilla Firefox is required. This device must be able to access SX-GATEs LAN interface via network. It might be necessary to temporarily change the device's IP configuration.

4.2 Switching on and booting

Push the power button on the front of the device. The boot process takes about two minutes. Please wait for this period before you continue!

Some SX-GATE models include an LCD display in the front panel. It indicates that the device is ready when the boot message is replaced by a status display.

4.3 Setting up SX-GATE's IP address

SX-GATE is delivered with the IP address 192.168.0.254 and network mask 255.255.255.0. Usually it will be necessary to adapt these settings to your LAN.



Before configuring a new IP address, please make sure that the new IP is not already in use. Each IP address must be unique on the network. All devices on the network must use the same network mask.

Note, that SX-GATE is not able to automatically obtain an IP address from an available DHCP server. SX-GATE must always have the same LAN IP address in order to provide its functionality.

It is not allowed to freely select an IP address for the LAN. For private networks, Internet standard RFC-1918 only allows addresses that start with 10, 172.16 to 172.31 or 192.168. All other IP addresses outside these ranges are officially allocated on the Internet and the property of others. Therefore it is highly recommended, to use only these private subnet ranges for internal LANs. For example, when using the 192.168.0.0 network with network mask 255.255.255.0, you can assign 254 IP addresses in the range 192.168.0.1 to 192.168.0.254 to your LAN devices.

To change SX-GATE's LAN IP the following options are available:

4.3.1 Changing the IP address with the display

Some SX-GATE models have built-in displays for status information. Via the display you can also configure SX-GATE's LAN IP address and network mask. Press the "Enter" button to enter the "IP-Configuration" screen. Use the arrow buttons "up" and "down" to select either the line with the IP address, the netmask or "Exit". Then hit the "enter" button.

The IP address is changed digit by digit. The currently selected digit is underlined. Use the buttons "up" and "down" to change the value of the current digit. Hit the arrow button "right" to move on to the next digit. Press the "Enter" button if you have set the desired IP address.

Use the arrow buttons "up" and "down" to change the network mask to the next bigger or smaller mask. Press the "Enter" button when the network mask is correct.

You can leave the "IP-Configuration" via menu item "Exit". If you have changed either the IP address or the netmask, you will be prompted if you want to save the changes. With the arrow button "right" you can toggle between "No" and "Yes". If you confirmed your changes, they will be saved and configured within a few seconds.

4.3.2 Changing the IP address with the web browser

If your SX-GATE model does not include a builtin display you will have to change the IP address in the web administration interface. This requires a computer device with a web browser and an IP address between 192.168.0.1 and 192.168.0.253 with netmask 255.255.255.0. If a system with suitable configuration is available, you can skip to the next chapter.

Otherwise you will have to adapt the IP configuration of your computer. Please refer to the operating system manual of the computer for details.

If the computer obtains its IP configuration automatically from a DHCP server, you can connect the computer directly with the LAN port of SX-GATE. By default SX-GATE acts as a DHCP server. You might need a crossover network cable which is not included. As an alternative you can place a network switch between SX-GATE and the computer, but please make sure that no other device is connected to the switch. Next release your computer's current IP address or reboot the system. Now your computer should have received a suitable IP address from SX-GATE's DHCP server.

If you don't want to change the cabling or obtaining an IP with DHCP is not an option, please configure a suitable IP address (e.g. 192.168.0.1) with netmask 255.255.255.0 in the computer's IP setup.

4.4 Check the connection to SX-GATE

To verify the network connection between your computer and SX-GATE use the "ping" command. If SX-GATE answers to your computer's ping request, the IP connection is ok.

Open the commandline of your computers operating system and enter the following command:

```
ping 192.168.0.254
```

If you have already changed SX-GATE's IP address, please replace 192.168.0.254 with its current IP.

If you receive an error message, please check all settings and correct faulty entries. Check the cabling and network ports. Are the link LED on the switch and the network cards illuminated? If a firewall is installed on your system, check to see if the firewall permits sending and receiving ping commands.

5 First settings

5.1 Accessing the web administration interface

Launch your web browser to start configuring SX-GATE. Enter "https://192.168.0.254:44344" in the browser's address bar. If the IP address of SX-GATE had been changed previously, enter the new IP address instead of the default IP "192.168.0.254".



The connection to SX-GATE's administration interface is encrypted using the HTTPS protocol (https://) and port 44344.

If you don't specify the port number (https://192.168.0.254) the browser will be redirected to port 44344.

The browser should now display a certificate warning. This is normal, as SX-GATE is not shipped with a valid server certificate. It uses a self-signed certificate issued to "Internet Appliance" instead. Please confirm that you want to continue connecting. You'll need to confirm twice in case of a redirect to port 44344.

In case you did not receive a certificate warning, please check the IP address you've entered in the browser. Also the address must start with "https://", not with "http://". Make sure the browser is not configured to use a proxy which might interfere with the connection.

In some cases a screen may appear, asking for the SX-GATE license key. You should have received the key from your SX-GATE dealer. The key consists of 5 groups of characters, each 5 characters long and separated by dashes. Please enter the key.

If the password for user "admin" has not already been set, you will have to set it when you access SX-GATE for the first time.



Please enter a long and complex password. It should be at least 10 characters long and consist of lower case and upper case characters, digits and special characters.

Finally SX-GATE's login screen should appear.

After you have logged yourself in SX-GATE's homepage appears on the screen.

5.2 Basic configuration

On the SX-GATE home page you will find the checklist "Getting started". Go through it one by one to complete the basic configuration of SX-GATE. Later you can open the menu on the left for a detailed configuration of all SX-GATE modules.



You will find detailed information on the setup options in the online help. Click the questionmark icon or the title of the option you're interested in to display the corresponding online help section.

If you still have to change SX-GATE's LAN IP, the wizard "LAN integration" will let you configure a new address. Please note that right after you finish this wizard, SX-GATE will no longer be reachable using its old IP. It's now time to reset your computer's IP address if you had to change it in order to access SX-GATE on its default IP. Then you will also have to adapt the IP in the browser's address bar to re-gain access to SX-GATE's administration interface.

6 Configuring computers in the LAN

In order to provide secure Internet access for LAN computers via SX-GATE, certain settings have to be made.

6.1 Network parameters

A suitable IP address and netmask is already sufficient for a computer system on the LAN to gain limited Internet access via SX-GATE. For full Internet access SX-GATE's LAN IP has to be configured as the computer's default gateway/router and DNS server. If the system obtains its IP configuration automatically from a DHCP server, these settings have to be configured in the DHCP server.



In a typical windows network the IP address of the Windows server instead of SX-GATE's IP is configured as DNS. Enter SX-GATE's LAN IP as forwarder in the server's DNS configuration.

For details on network configuration of the LAN systems please refer to the respective operating system manuals.

6.2 Setting up the web browsers

As far as possible, computer systems in your LAN should make use of SX-GATE's various proxy, forwarder and relay services. The SX-GATE web proxy is specialized in securing the Internet communication of web browsers. The proxy has to be configured in the browser settings.



The default policy of SX-GATE's firewall will deny any direct connections between local systems and the Internet! So for the moment there's no Internet access without proxy configuration.

Open the proxy settings of the browser. They can be found in different menus, depending on the web browser used. Look for network, connection or LAN settings or refer to the browser's manual. Enter the LAN IP of SX-GATE and port 8080 as proxy.



In browsers used to configure SX-GATE you should exclude SX-GATE's LAN IP from proxy access.

It is also possible to use a proxy configuration script or use the automatic proxy configuration. More information and the configuration of these options is available from the "Proxy configuration" wizard.



In Windows networks it is possible to assign the proxy configuration to all workplaces by using group policies.

7 Home

SX-GATE can be configured without relying on JavaScript or Cookies. However for full convenience and user experience JavaScript is required. Cookies are used to store each users individual customizations.



The following features all rely on a modern browser with JavaScript enabled.

Docks and Docklets

Various status and information windows called "Docklets" are shown on the homepage. The central area serves as the "Dock" for these docklets. Move the bar attached to the right border of the dock to change its width. If the browser window is wide enough, there'll be an other dock on the right which remains visible in all menus. So if you want to keep an eye on the information a certain docklet provides, place it on this dock.

Except for docklet "Getting started", you can move all docklets around by pressing and holding down the left mouse button in the docklet's title bar. Either change a docklet's position within a dock or move it between the dock of the homepage and the permanently visible dock on the right. On the top of each dock there's a multi-column area. Docklets dropped here will occupy the full width of the dock. Drop the docklet below to place it in one of the columns with normal width.



The docklet positions and also the dock width are stored in a browser cookie.

Click the icons on the left side of each docklet title bar to reduce the docklet to its title bar and restore it again, open the docklet in a dedicated browser window or refresh the docklet contents respectively. The icons on the right will show the online help or close the docklet.



To show a closed docklet again or to see the list of available docklets please move the mouse pointer towards the spanner icon in the right top hand corner of the administration interface.

Live Log

A constantly refreshed view on a log file is also available via the spanner icon in the right top hand corner of the administration interface. A new window will open at the bottom. Drag the bar in the middle to change the window height.

Online help

Click the question mark to open the help window with a detailed description of the settings on each screen. If the additional dock on the right is available, the help window will open in there. The information shown will follow the currently visible screen. Without the dock, a draggable help window will open on top of the screen. It is closed when the screen changes.



Click the title bar icon to open a separate browser window if you want a sticky view on the current help topic.

By default the text corresponding to the current tab is shown. Click on the coloured titles for a description of the options below or the menu items above. A missing arrow in front of the title indicates that no help text is available for this item.

7.1 Getting started

This docklet provides a checklist for SX-GATE's initial basic setup. Click on the texts to configure the corresponding subsystem or task. When done, close the docklet by clicking on the "X" icon in the top right hand corner so there's more space for the other docklets.

7.2 Ressources

This docklet shows a bar graph of the CPU load, the system load and the amount of used memory and swap space.

7.3 Network data rates

For each interface a bar graph for its inbound and outbound throughput is shown. The percentage value refers to the maximum throughput measured since the start of the service. An interface won't be shown unless there has been data.

7.4 Disk space

This docklet shows the used amount of disk space per partition. On systems with RAID, a green or red light indicates the RAID status. While rebuilding a RAID partition a progress indicator is displayed instead.

7.5 Updates

This docklet shows the available updates.

7.6 Services

A list of services started when booting is presented by this docklet. A red light indicates that a service has been stopped. A yellow light is shown for a service which is currently running but won't be started while booting.

7.7 SX-GATE info

This docklet gives a brief overview of your SX-GATE and its licenses.

7.8 SX-GATE status

If a quick system check reveals something unusual, the observations are reported here.

7.9 Ethernet Cards

This is an overview over the ethernet card settings.

The values show in detail:

- the hardware address (MAC) of the network card
- the working speed of the ethernet card in Mbit/s
- the negotiated respectively configured duplex mode (full, half)
- whether the auto negotiation is enabled or not
- the current link status

A dash or a white signal indicates that the system can't determine this value.

7.10 Mail server

Totals from menu "Monitoring > Mail server" are displayed here.

7.11 Live log

In the title bar of the live log you will find some additional icons which have not already been explained in the docklets section: Click the additional icons to clear the view, filter which lines you want to see and select the actual log file.

- With the pause/play symbols you can suspend and continue the log updates
- Click the symbol with the cross to clear the display area
- The filter symbol will open or close the area for entering filter expressions, which are explained in detail below
- To export the current contents of the live log to a text file, please click the floppy disk icon
- Finally there's a drop down list of the available logs

Filtering is case insensitive. For complex filter expressions so called "regular expressions" are supported. Here's a quick syntax overview:

`+ - ? . * ^ $ () [] { } \`

Characters with a special meaning. To match one of these characters, precede it with a backslash. So e.g. `"\"` will match a dot.

`-` (dash) at the beginning of the expression

Inverts the meaning of the expression. Search for lines NOT matching the following expression.

`.` (dot)

An arbitrary character.

`[...]`

One character from the given set. For example `"[0-9a-f:]"` will match either a digit, one of the letters a through f or a colon.

`(...)`

Grouping of elements. See `"|"` for an example.

`?` (question mark), `*` (asterisk), `+` (plus sign)

These are all multipliers referring to the directly preceding character, set or group. The question mark makes it optional (zero or once), with an asterisk it may occur zero or more times, with the plus sign at least once (one or more times).

`|` (pipe symbol)

Means "or". The expression `"(19|20):"` would be suitable to filter the time to 7pm or 8pm.

`^` (circumflex), `$` (dollar)

These characters represent the start and the end of a text respectively. For instance `"^error"` would match lines with the word "error" at the beginning of a column text.

Each expression may either apply to all columns or just to a single column. Click the plus symbol to get additional lines if you need to combine expressions. The expressions can be combined with either "AND" or "OR".

Click the symbol on the right end of the row with the column titles to toggle the display of individual columns.

8 My Account

The mainmenu "My Account" offers the possibility for users to change some of the settings of their own account by themselves (e.g. changing the password). In cases of getting into trouble, contact information can be deposited in the submenu "Contact".

8.1 Change password

Current password

To change your password you have to enter the current password first.

New password

Here you can change your password which is required to access various services of SX-GATE. To verify the new password you have to enter it twice.

8.2 Email options

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

8.2-A Forwarding.....	36
8.2-B SPAM filter.....	36
8.2-C SPAM scores.....	38
8.2-D SPAM lists.....	39
8.2-E Vacation.....	40
8.2-F Folders.....	41

8.2-A Forwarding

Forward email to

It is possible to automatically forward your incoming emails to other internal or external addresses. Enter the address and then click on the button "Add". You can enter as many recipients as you want and they will all receive a copy of the email that is addressed to your mailbox. To remove an address select it in the list and push the button "Remove".

Keep copy of forwarded emails

With this option you can control if a copy of each mail will be delivered to your mailbox even when forwarding your mail to other addresses. If the option is not checked, your mailbox will not receive emails any longer.



If forwarding is not active, this option is without effect.

8.2-B SPAM filter

If you enable at least one of the thresholds, every incoming mail has to pass a SPAM mail filter before it is delivered to your mailbox. A SPAM mail is an unsolicited email, usually with dubious origin.

The SPAM mail filter of SX-GATE classifies emails by identifying typical phrases and other attributes indicating an unsolicited email. SX-GATE contains a database of checks to perform and all matches result in a score which in turn allows filtering emails. Characteristics indicating a SPAM mail will add a value to the score while other characteristics indicating that it's not a SPAM mail will subtract a certain value. The higher the final score, the more likely it's a SPAM mail.



Emails exceeding the size of 1MB will not be classified to save system resources. However this is not a drawback, as a SPAM mail is usually very small.

A few headers will be added to each email examined by the SPAM mail filter. The header "X-Spam-Status" shows the final score (hits=...) and give the name of the matches (tests=...). This allows the recipient of the mail to check the score of any mail. The header "X-Spam-Level" will contain one "x" per scored point (e.g. "X-Spam-Level: xxx" for a score between 3.0 and 3.99). This header allows automatic sorting in the user's mail client.



Most mail clients will display only the most important headers by default. Usually the full header information is available after selecting a specific menu option.

Tag an email as SPAM when it is scored more than

If the score exceeds the threshold for tagging an email as SPAM, the subject of the mail is prefixed by the text "***** SPAM *****" and the SPAM score.

Deliver tagged emails to

As an option SX-GATE can deliver tagged SPAM mails into a separate SPAM folder. This folder is accessible with SX-GATE's groupware or via IMAP (folder Mail/SPAM). A POP3 client will not be able to open the SPAM folder.

Delete SPAM/HAM after

Mails from the "SPAM" and "HAM" folders are automatically deleted after the given number of days.



This feature does not depend on the previous option. Mails will also be deleted if you create and fill the SPAM folder yourself instead of having tagged mails automatically delivered to the SPAM folder.

Silently discard a mail when it is scored more than

Exceeding this threshold, an email will be silently discarded. There will be no notification and it is not possible to undelete the email. The email is lost irrecoverable! If you want to make sure that no requested email gets lost, you should not enable this option. Activate the threshold "Tag an email as SPAM when it is scored more than" instead and make use of the features offered by your mail program to sort emails based on header lines.



To avoid loss of important emails you should be very carefully when activating this option. You should select a value which is rather to high than to low. Please note that automatically deleting email may be subject to legal constraints or might even be prohibited by law.

8.2-C SPAM scores

Userdefined SPAM checks

This control allows you to extend the SPAM checks by self-defined rules. First you have to decide to which part of the mail a new rule applies. If the specified pattern is found in a mail, the selected score is accounted.

The following types of SPAM filter rules are available:

Subject

The pattern is looked up in the email's subject.

Sender

This will check the sender of the mail (From header).

Recipient

Use this option to match the recipient (To header).

Message header

Allows you to examine an arbitrary mail header.

Message text

The actual text contents of the email, including the subject, are analyzed when selecting this value.

Raw HTML text

Just like the previous option, but including HTML tags of HTML emails.

Web links

Checks web links (either plain text or HTML links) found in the subject or the message body.

Rule

This setting differs from the previous ones. It allows you to modify the score of SX-GATE's builtin rules. Accordingly you don't specify a search pattern here. Instead you have to supply the internal ID of the rule. The ID together with the original score is listed in the content analysis of mails, that have been marked as SPAM (e.g. "HTML_MESSAGE" or "FORGED_MUA_OUTLOOK").



When the builtin rulesets are updated, internal ID's may change without notice. The rules defined here will not be adjusted.

Search patterns ("matches") are case-insensitive. If the pattern starts/ends with a letter or a digit, the pattern matches only if the pattern is found at the beginning/end of a word. So e.g. the pattern "pace" won't match "spaces" but will match "Learn at your own pace!".

Some characters have a special meaning:

***** (Asterisk)

It represents a sequence of arbitrary characters. The sequence may also be missing. As searching for such a sequence of any length is rather time-consuming, an asterisk matches no more than 30 characters. The pattern "a*d" will match e.g. "ad", "a_d" and "abcd". The asterisk helps you to find patterns within words. So e.g. the pattern "*pace*" will match "spaces".

? (Question mark)

Any single character is matched by a question mark. If for instance "a?d" is looked up, "a_d" is a hit. In contrast "ad" and "abcd" do not apply.

_ (Underscore)

An underscore matches any amount of whitespace characters, i.e. spaces, tabs and new-lines. As an example, "a_d" will match "a d", but not "ad" or "a_d".

Please keep an eye on the configured thresholds when selecting the score for a new rule. For a rule which refers to SPAM mails you have to select a positive value. Negative numbers reduce the probability of matching emails to be classified as SPAM.

English language indicates potential SPAM

The majority of SPAM mails is written in English language. Activate this switch to add some points to the SPAM score of every English email. This will result in a significant increase of the probability that the score of English mails will exceed the configured SPAM filter thresholds.

8.2-D SPAM lists

Of course the SPAM mail filter will not achieve a hit ratio of 100% when classifying emails automatically. Some SPAM mails will pass undetected. It might even occur, that a "normal" email is classified as SPAM by mistake. With the white- and blacklists it is possible to force a specific result of the classification based on the email address of the sender.



If no SPAM filter threshold is defined, the SPAM mail filter is not active and so the list entries are without effect.

SPAM filter whitelist

If an email was identified as SPAM by mistake, you can add the sender to this list. The SPAM filter will subtract 100 points from the SPAM score of a mail, if the sender is found in this list. Thus all future emails of senders listed here will never be recognised as SPAM.

You can add a complete email address (e.g. user@example.com) to prevent filtering emails from this specific address. If you want to allow every email from a specific domain to pass, add only the domain part of the address (e.g. example.com).

SPAM filter blacklist

If you receive SPAM mails from the same sender again and again and the SPAM mail filter does not identify these emails as SPAM, you should add the sender to this list. The SPAM filter will add 100 points to the SPAM score of a mail, if the sender is found in this list. Thus all future emails of senders listed here will always be recognised as SPAM.

You can add a complete email address (e.g. user@example.com) to intercept emails from this specific address. If you want to classify every email from a specific domain regardless of the actual sender, add only the domain part of the address (e.g. example.com).

8.2-E Vacation

On this tab you can configure autoresponses and schedule a forwarding rule for your mails.

The selected actions will apply to every email delivered to your mailbox. In particular this affects also emails not addressed to you personally but to a distribution list (group) you're a member of.



When emails are forwarded to other addresses (see tab "Forwarding"), the settings will apply only if the option "Keep copy of forwarded emails" has been selected.

Vacation settings

Choose from the list of actions taken for each mail.

Start date

Either schedule a date to enable the vacation feature or enable it immediately. Please use date format YYYY-MM-DD HH:MM.

End date

You may also enter a date the vacation feature is expected to stop working. Please use date format YYYY-MM-DD HH:MM.

Forward email to

You can forward emails to a different recipient during the configured period of time.

Keep copy of forwarded emails

When enabled, you will still receive a copy of each mail even when forwarding to a different address.

Vacation message

It is possible to generate an automatic reply to incoming mails. Typically it is used for a vacation autoreply. However you could also use this feature to automatically confirm email delivery.



No reply will be generated for emails which have been tagged as SPAM.

Please fill in the text message to be sent. If there's no text, no reply will be sent.

8.2-F Folders

It is possible to automatically distribute mails into different subfolders of your mailbox. Access to these folders requires IMAP or groupware. POP3 does not support folders.

8.3 Groupware

This menu item allows users to open their mailbox with a web browser, provided that the groupware extensions has been installed. Access is granted for all users who are member of the group "system-mail".



It is not required to be member of group "system-admin". However, users with this limitation will not be able to access the groupware through the menu of SX-GATE's administration interface. They have to type in the URL
URL `https://NAME_or_IP/groupware/`

The groupware requires that the browser is JavaScript enabled. Cookies have to be accepted, too.

In addition to email, the groupware features address book and calendars with appointments and tasks, which can be shared with other users.

8.4 Contact

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

8.4-A ID card.....	43
8.4-B Company.....	43
8.4-C Administrator.....	43
8.4-D Provider.....	44
8.4-E Support.....	44
8.4-F Company	44
8.4-G Administrator	44
8.4-H Provider	44
8.4-I Support	44
8.4-J Info.....	44

8.4-A ID card

The values displayed here identify your SX-GATE. Please state these values whenever you contact technical support. Click on "Download" if you want to see more detailed information about your SX-GATE.

Mail detailed ID card to ...

Privacy statement

Clicking on this button will send the contents of the detailed ID card to the displayed email address. The included information will be stored and used solely for marketing and support of SX-GATE. The data will be made available to authorised SX-GATE partners only. You can have your details removed anytime by sending an email to the stated email address.

8.4-B Company

Here you can enter or change information about your company.

8.4-C Administrator

Here you can enter or change contact information of the SX-GATE administrator. Any user who is privileged to access the administration GUI has read-only access to the details specified here.

8.4-D Provider

Here you can enter or change contact information of your Internet Service Provider. Any user who is privileged to access the administration GUI has read-only access to the details specified here.

8.4-E Support

Here you can enter or change contact information of the technical support for your SX-GATE. Please do not forget to include the information stated on tab ID card in your inquiry. Any user who is privileged to access the administration GUI has read-only access to the details specified here.

8.4-F Company

Here you can find information about your company.

8.4-G Administrator

Here you can find the details of your SX-GATE administrator.

8.4-H Provider

Here you can find the details of your SX-GATE Internet Service Provider. Get in touch with the provider if you should encounter problems with the Internet connection.

8.4-I Support

Here you can find the details of the technical support for SX-GATE. Please do not forget to include the information stated on tab ID card in your inquiry.

8.4-J Info

Here you can find the details of the manufacturer.

9 Statistics

In mainmenu "Statistics" you can look at various statistics for some of SX-GATE's modules.

9.1 System load

Selecting this menu item you will be presented graphical statistics which inform you about the system status. On the main page a scaled down image of all hourly stats is available. Open the item in the tree menu of the user interface to see the complete statistics. These include hourly, daily, weekly, monthly and yearly graphs for each topic.



The hourly and daily statistics are updated every 10 minutes. All other graphs are generated daily at midnight.

Some details to the different topics:

Load average

The most important graph is the load statistics. It shows the average count of processes ready for execution. When 100% have been reached, every moment in time a process is active. Whenever values above 100% occur, processes have to wait for resources to become available (like e.g. CPU or harddisk).

Cpu

This graph shows the usage of the system processor.

Memory

The positive values indicate the usage of main memory (RAM). In addition a swap space is available on harddisk. The percentage of swap space used is displayed as a negative value.

9.2 Network

In this menu several different network statistics are available. These include hourly, daily, weekly, monthly and yearly graphs on each topic.



The hourly and daily statistics are updated every 10 minutes. All other graphs are generated daily at midnight.

9.2.1 Connections

The connection table of the stateful inspection firewall is used for this graph. Once per minute a snapshot of all listed connections is taken. Frequently encountered well known protocols are depicted in a colour of its own. All other connections are summarised as "misc".



Connections which have not been closed properly will expire after a quite long timeout. Thus the number of active connections is usually lower than the value stated in the graph.

9.2.2 Throughput

The used data rate of the internet link is displayed here. The current default route determines the interface which is connected to the Internet. Positive values indicate the data rate used by data packets received from the Internet. The outgoing data rate is stated with negative values. The scale refers to kilobyte per time.

An additional tab shows the transmitted amount of data per month.

A table gives you an overview of the available objects. If multiple columns are displayed you can change the sort order by clicking the column title. If there are more than 20 entries, a navigation bar will appear below the bottom right hand corner of the table. You can switch between a grouped view or a pager. The full screen mode allows you to see all entries at the same time. Pick an entry by clicking its title in the left column. A pencil icon or a trashcan in the right column allow you to rename or delete an entry.

9.2.3 Bandwidth

In many interfaces it is possible to enable bandwidth management. It divides traffic into five priority classes. The statistics shows the percentage distribution of these five classes.

A table gives you an overview of the available objects. If multiple columns are displayed you can change the sort order by clicking the column title. If there are more than 20 entries, a navigation bar will appear below the bottom right hand corner of the table. You can switch between a grouped view or a pager. The full screen mode allows you to see all entries at the same time. Pick an entry by clicking its title in the left column. A pencil icon or a trashcan in the right column allow you to rename or delete an entry.

9.3 Firewall

9.3.1 Packet filter

This menu provides a statistics of firewall events. The stats are updated daily at midnight.

Besides an overview of the last 12 months, a detailed statistics is available for each month. Click on the respective month to change the view. The monthly statistics will provide an overview of each day and the distribution of events by hour. Furthermore there are listings of the interfaces, source and destination addresses (anonymised) and target ports involved.

The following terms are used in the statistics:

Accepted

The connection was accepted. Only connections with logging enabled in the firewall configuration will be counted.

Faked

A ping or traceroute wasn't forwarded to the actual target system but answered by the SX-GATE firewall.

Rejected

The connection was denied. The initiator was informed about that by a network control message.

Dropped

The connection was denied. The IP packet was discarded without notification of the sender.

9.3.2 IDS/IPS

This menu offers statistics of the events detected by SX-GATE's Intrusion Detection System (IDS). The stats are updated daily at midnight.

Besides an overview of the last 12 months, a detailed statistics is available for each month. Click on the respective month to change the view. The monthly statistics will provide an overview of each day and the distribution of events by hour. In addition there are tables with the top events and the source addresses (anonymised) and services involved.

9.4 Mail server

If the mail server of SX-GATE has been activated, access statistics are provided here. The stats are updated daily at midnight.

Besides an overview of the last 12 months, a detailed statistics is available for each month. Click on the respective month to change the view. The monthly statistics will provide an overview of each day and the distribution of requests per hour. Furthermore a list of the most frequently found SPAM characteristics and viruses is displayed. The top destination domains are also listed.



The SPAM filter statistics is available for the user-independent relay SPAM filter only.

The following terms are used in the statistics:

Sent

Each mail successfully sent by the mailserver is counted in this column.

Discarded

All mails blocked by the virus scanner are declared as discarded and are shown in this column. In individual cases the figure can also include individual mails which had to be discarded due to a critical error.

Rejected

In this column mails are counted that have been rejected by the mail system. This includes emails blocked by the SPAM filter.

Spam (Rejected)

This column gives the total number of SPAM mails. This includes both, tagged and rejected mails. The value in brackets specifies the number of rejected SPAM mails.

Virus

This value shows the number of virus mails.

KBytes

The amount of data sent is given in kilobytes.

9.5 Proxies

9.5.1 Web proxy

This menu item allows you to inspect the usage of SX-GATE's web proxy. The statistics are updated daily at midnight.



If the virusscan option of SX-GATE's web proxy is active, requests can bypass the scan when sent to the web cache running on port 8081. These requests will not be included in the statistics.

Besides an overview of the last 12 months, a detailed statistics is available for each month. Click on the respective month to change the view. The monthly statistics will provide an overview of each day and the distribution of requests per hour. Furthermore a list of the most frequently requested domains is displayed.



For privacy reasons, no lists per source IP or user are available. However at "Monitoring > Log files" the proxy's access log can be archived externally for further processing. Please inform yourself about privacy regulations and laws which have to be satisfied.

The following terms are used in the statistics:

Hits

Every single request sent to the proxy counts as a hit. A typical web page consists of several objects. For instance to download an image which belongs to a page, an additional request has to be sent.

Files

Not for every request a file is returned. Sometimes the reply is a simple status or error code. These requests are not counted here.

Pages

Only those requests which typically refer to the text parts of a web page will be considered here. Therefore, embedded objects like e.g. images are not included.

Visits

A visit is a sequence of requests sent from the same source address with no more than 5 minutes between the hits.

Sites

This value refers to the number of different source addresses.

KBytes

The amount of data received is given in kilobytes.

9.5.2 Reverse proxy

If the reverse proxy of SX-GATE is running, access statistics are available here. The stats are updated daily at midnight.

Besides an overview of the last 12 months, a detailed statistics is available for each month. Click on the respective month to change the view. The monthly statistics will provide an overview of each day and the distribution of requests per hour. Furthermore a list of the most frequently requested files is displayed. Finally a ranking of source addresses per country is depicted.

The following terms are used in the statistics:

Hits

Every single request sent to the web server counts as a hit. A typical web page consists of several objects. For instance to download an image which belongs to a page, an additional request has to be sent.

Files

Not for every request a file is returned. Sometimes the reply is a simple status or error code. These requests are not counted here.

Pages

Only those requests which typically refer to the text parts of a web page will be considered here. Therefore, embedded objects like e.g. images are not included.

Visits

A visit is a sequence of requests sent from the same source address with no more than 5 minutes between the hits.

Sites

This value refers to the number of different source addresses.

KBytes

The amount of data sent is given in kilobytes.

9.6 Web server

If the internet web server of SX-GATE has been activated, access statistics are provided here. The stats are updated daily at midnight.

Besides an overview of the last 12 months, a detailed statistics is available for each month. Click on the respective month to change the view. The monthly statistics will provide an overview of each day and the distribution of requests per hour. Furthermore a list of the most frequently requested files is displayed. Finally a ranking of source addresses per country is depicted.

The following terms are used in the statistics:

Hits

Every single request sent to the web server counts as a hit. A typical web page consists of several objects. For instance to download an image which belongs to a page, an additional request has to be sent.

Files

Not for every request a file is returned. Sometimes the reply is a simple status or error code. These requests are not counted here.

Pages

Only those requests which typically refer to the text parts of a web page will be considered here. Therefore, embedded objects like e.g. images are not included.

Visits

A visit is a sequence of requests sent from the same source address with no more than 5 minutes between the hits.

Sites

This value refers to the number of different source addresses.

KBytes

The amount of data sent is given in kilobytes.

10 Monitoring

In mainmenu "Monitoring" you can choose from a variety of diagnostic functions in order to get an impression about the current status of SX-GATE or to figure out reasons for any functionality problems.

10.1 Log files

Here you can inspect SX-GATE the most important logfiles generated by SX-GATE. These are especially helpful when troubleshooting. Before consulting technical support, please check the log files. When sending emails to technical support, it is appreciated if you include relevant details of the log.

Internally, several log files will be written, depending on topic and importance. The log files will be archived daily just after midnight. Unless otherwise stated, up to 12 archived files will be kept in the system. After that, they will be automatically deleted.

Log file

Please select a log file from the list first. The following log files are available:

important messages

Errors and other important messages from all modules of SX-GATE. The log will also contains some system messages generated during the booting procedure.

messages

This log file contains further messages from different SX-GATE modules.

firewall

The SX-GATE firewall logs to this file.

Each line begins with the date and time when the IP packet was registered by SX-GATE. The next important information is the firewall stage at which the packet was intercepted.

These stages are as follows:

- fw-in: The packet was addressed to SX-GATE itself
- fw-out: The packet was created by SX-GATE itself
- fw-fwd: The packet was about to be routed through SX-GATE
- fw-chk: For packets failing to pass a plausibility check

The next field indicates what happened to the packet:

- drop: The packet was discarded
- rej: The packet was discarded and the sender was notified (with an ICMP packet or a TCP reset)
- fake: SX-GATE replied with a faked answer
- acc: the packet was accepted. Normally accepted packets are not logged, so it is unlikely that you will see this value

In brackets the reason is stated, why the packet was logged. The value "restricted" indicates, that the current firewall policy does not allow this kind of connection. However it is possible to add a firewall rule to grant access.

Among others, the following fields show the name of the interface through which the packet was received and through which it would have been sent. Next are the layer 3 protocol of the packet and its source and destination IPs. For TCP and UDP, the respective source port and destination port (DPT=) is listed. For ICMP packets the ICMP type and code can be found in the port columns, which indicate the message type. For TCP connections the TCP flags are shown. The last column contains the MAC address of the sender.

IDS/IPS

Shows alerts logged by the Intrusion Detection and Prevention System (IDS/IPS). The IDS/IPS examines the contents of IP packets and compares them with a signature database.

Besides date and time the log will show you what happened to the packet. The text "Drop" indicates that the corresponding IP packet has been discarded by the IPS instance running within the firewall, whereas "wDrop" indicates that the IDS logged the packet. In contrast to the IPS, the IDS is a passive component on the monitor port of a switch.

The reference is the combination of module ID (usually 1), rule ID and revision number, separated by colons (e.g. 1:2345678:9). You need the rule ID (here: "2345678") to disable a rule in the IDS/IPS configuration.

The next columns contain the rule name and a classification, indicating the type of the event. The priority indicates if it's a critical problem (priority 1) or less critical (priorities 2, 3 or 4). The final columns contain the layer 3 protocol, source and destination IP and the ports.

IPSec

This file contains the messages logged by SX-GATE's IPSec VPN server.

OpenVPN

This file contains the messages logged by SX-GATE's OpenVPN server.

Wireguard

This file contains the messages logged by SX-GATE's Wireguard server.

Clustering

This logfile records the actions of the cluster.

Mail

This log contains information about incoming and outgoing mails, messages of the mail server and its filters as well as connections to the POP3 and IMAP4 server of SX-GATE.

Web proxy access

In this file any access made to SX-GATE's proxy server on port 8080 are logged.

Web proxy messages

Messages from SX-GATE's web proxy can be found in this log.

Reverse proxy access

In this file any access made to SX-GATE's reverse proxy are logged.

Reverse proxy messages

Errors and other messages of the reverse proxy are logged into this file.

Reverse proxy WAF

Choose this setting to view alerts of the Web Application Firewall. The alerts are written to the same logfile as the reverse proxy messages, but displayed separately.

SOCKS proxy access

In this file any access made to SX-GATE's SOCKS proxy are logged.

WWW server access

If the Internet web server of SX-GATE is running, all requests will be recorded in this file.

WWW server messages

Errors while accessing the Internet web server are logged in this file. A typical problem is a request for a non existing document.

Intranet server messages

If errors occur when trying to access the web server for the local intranet, these will be logged here.

Debugging

Debug messages generated by various processes. In contrast to other logs, no more than three archived versions of this log file will be stored.

PPP

Select this log to spot problems establishing PPP dial-up connections.

Virusscanner

In this log you'll find messages from virus scanners and signature updates.

(APP) Web Client

In this log you'll find messages from the Web Client app.

Administration

Access to the web administration and configuration changes are logged in there.

External systems

In this logfile you can find messages that have been sent to SX-GATE by other systems.

Display up to

The display is normally limited to 100 lines. However, you can define a different limit using this selection field.

Search lines containing

Enter a search pattern to display only matching lines from the selected log. The pattern must confirm to the rules of the so called "regular expressions".

Some common directives are

- | logical "or"
- (...) grouping of alternatives: e.g. "a(b|c)" means "ab" or "ac"
- [...] an arbitrary character from the given set: e.g. "[3-6X]" means one of the characters 3, 4, 5, 6 or X
- [^...] an arbitrary character except characters from the given set: "[^3-6X]" means any character except for 3, 4, 5, 6 or X
- . an arbitrary character
- ^\$()[]{}+*?\. characters with a special meaning
- \ disables the special meaning of the following character: Enter "\" to search for a dot, "\\$" to search for a dollar sign

You can search for the month abbreviations Jun and Jul in the following ways:

- Jun|Jul
- Ju[nl]
- Ju(n|l)

Skip lines containing

This option is complementary to the previous one. Only those lines which do not include the given text will be displayed.

Search

Press this button to actually start searching in the logs, using the previously entered parameters. The results will be displayed in a new browser window.



Please note the floppy disk symbol in the upper right which allows you to export the log into a text file.

In the first line of the results window you will find the parameters which led to current results. You can now filter those results interactively. On the right there's a histogram, showing the chronological distribution of the results. Start dragging at the left or right side to change the width of the gray area, which represents the timeframe to show. On the left you can define filter expressions. A detailed explanation can be found in the live log documentation.

10.2 Tools

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

10.2-A IPv4 Ping.....	58
10.2-B IPv6 Ping.....	59
10.2-C IPv4 Traceroute.....	60
10.2-D IPv6 Traceroute.....	60
10.2-E ARP scan.....	61
10.2-F DNS query.....	61
10.2-G WoL.....	63
10.2-H Packet Dump.....	63

10.2-A IPv4 Ping

To test network connections the "ping" command is very helpful. It sends a small IP packet (ICMP echo-request) to a specific address. If a packet of type "ICMP echo-reply" is returned, the IP connections to this address is obviously ok.

Send ping to

Here you can specify where to send the "ping". You can specify either an IP address or a DNS name. If you enter a DNS name, the name server of SX-GATE must be running and name resolution must be working.

Source IP

When trying to ping through a VPN tunnel, it can be necessary to use a specific source IP.

Packet size

Here you can select the packet size (plus 8 byte ICMP header). In particular via VPN it can happen, that large packets (e.g. of size 1500 byte) fail to be transmitted. In this case the packets are sent via a system which discards fragmented IP packets.

Start ping

Press this button to send 5 ping packets to the specified address. If no reply is returned, some common reasons are:

- The remote system is switched off or does not exist
- The remote firewall discards ping packets
- The network connection to the specified address is not available
- The external IP address of SX-GATE is a RFC1918 address (192.168.*, 172.16.* - 172.32.*, 10.*) and these internal addresses are blocked in the firewall settings of the corresponding SX-GATE interface.

10.2-B IPv6 Ping

To test network connections the "ping" command is very helpful. It sends a small IP packet (ICMP echo-request) to a specific address. If a packet of type "ICMP echo-reply" is returned, the IP connections to this address is obviously ok.

Send ping to

Here you can specify where to send the "ping". You can specify either an IP address or a DNS name. If you enter a DNS name, the name server of SX-GATE must be running and name resolution must be working.

Interface / source IP

To ping a link local address you have to select an interface. When trying to ping through a VPN tunnel, it can be necessary to use a specific source IP.

Packet size

Here you can select the packet size (plus 8 byte ICMP header). In particular via VPN it can happen, that large packets (e.g. of size 1500 byte) fail to be transmitted. In this case the packets are sent via a system which discards fragmented IP packets.

Start ping

Press this button to send 5 ping packets to the specified address. If no reply is returned, some common reasons are:

- The remote system is switched off or does not exist
- The remote firewall discards ping packets
- The network connection to the specified address is not available

10.2-C IPv4 Traceroute

Traceroute is an other tool to test network connections. In contrast to "ping" it also shows the path IP packets take towards their destination.



Many systems do not reply to traceroute packets. Asterisks are shown in this case.

Send traceroute to

Here you can specify where to send the "traceroute". You can specify either an IP address or a DNS name. If you enter a DNS name, the name server of SX-GATE must be running and name resolution must be working.

Source IP

When trying to trace packets through a VPN tunnel, it can be necessary to use a specific source IP.

DNS reverse lookup

When enabled, an attempt is made to resolve each hop's IP into a hostname.

Start traceroute

Press this button to start the traceroute.

10.2-D IPv6 Traceroute

Traceroute is an other tool to test network connections. In contrast to "ping" it also shows the path IP packets take towards their destination.



Many systems do not reply to traceroute packets. Asterisks are shown in this case.

Send traceroute to

Here you can specify where to send the "traceroute". You can specify either an IP address or a DNS name. If you enter a DNS name, the name server of SX-GATE must be running and name resolution must be working.

Source IP

When trying to trace packets through a VPN tunnel, it can be necessary to use a specific source IP.

DNS reverse lookup

When enabled, an attempt is made to resolve each hop's IP into a hostname.

Start traceroute

Press this button to start the traceroute.

10.2-E ARP scan

The ARP scan uses the ARP protocol to list devices directly connected to the selected interface, i.e. that are in the same network segment. It is not possible to scan network segments beyond routers.



Only IPv4 enabled systems will be detected.



Scanning large networks may take several minutes (netmask 255.255.0.0) or even hours (netmask 255.0.0.0).

Interface IP

Select the interface used for scanning.

IP range

Without further specification all IPv4 addresses matching the primary IP and netmask of the selected interface will be tested. Enter a single IP, a network address with corresponding netmask or an IP range (e.g. 192.168.0.10-192.168.0.20) to override.

Start arp scan

Press this button to start the arp scan. You will be able to download a text file with the results when the scan is finished.

10.2-F DNS query

On this screen you can test name resolution or get information from the DNS.

Start DNS query for

Here you have to enter the term you are looking for.

Type

Select the type of information you are looking for:

A/AAAA/PTR

IP address of a hostname or hostname of an IP address

CAA

List of CAs allowed to issue certificates for a domain.

MX

Mail server for the specified domain

NAPTR

Complex entry, often used for cloud and telecommunication services.

NS

Name server for the specified domain

SOA

Meta information for the specified domain

TXT

Text information for the specified domain

Using name server

Here you can make a choice, to which name server the request will be sent. Usually name resolution uses SX-GATE's DNS. However if name servers of your provider have been configured, these will also be available here, so they can be contacted directly. This is particularly handy if you want to test the availability of these servers.

Name servers currently used by SX-GATE

The servers SX-GATE currently uses to resolve names are shown here. If the list is empty, SX-GATE uses the Internet root name servers. If SX-GATE is configured to accept DNS addresses on dial-up links, the server addresses received from the ISP will show up here.

Start DNS query

Press this button to start the DNS query.

10.2-G WoL

On this tab you can wake up a suspended computer by sending Wake-on-Lan packets.

Mac address of host to wake up

Please enter the hardware address of the computer here. The expected format is "XX:XX:XX:XX:XX:XX". Each "X" must be a digit or a letter from "A" to "F". The delimiters may be colons, dots, hyphens or underscores.



Click "Apply" to save the mac address as default.

10.2-H Packet Dump

In order to further debug a network, it is sometimes necessary to examine individual packets. A packet dump will let you see a packet's source and destination ports, IP and MAC addresses, and many other things. It will also let you observe packet direction and if a packet even exists it all.

First Hostname, Net or IP

Packet dumps can grow quite large rather quickly, here you can filter the recorded traffic by IP, network or hostname.

Second Hostname, Net or IP

Enter a second address to record the traffic between two specific hosts only.

Interface

Here you can select the specific interface you would like to record traffic from.

Protocol

This options allows you to specify the protocol of interest to be recorded in the packet dump. This helps keeps the packet dump size down and reduces the amount of extraneous information in the dump.

Port (not for ARP or ICMP)

Here you can also restrict the packet dump to a specific port number. This setting must not be used for the protocols ARP and ICMP.

Exclude Port (not for ARP or ICMP)

Here you can also exclude a specific port number from the packet dump. This setting must not be used for the protocols ARP and ICMP.

Exclude IP

Here you can also exclude a specific IP from the packet dump.

Run time

Here you can specify how long (in seconds) you want the packet dump to run for.

Start Packetdump

Press this button to begin recording traffic. After the given run time or 500 packets, whichever is reached first, download buttons will appear that can be used to view or download the resulting packet dump for further analysis.

Stop Packet Dump

Here you can stop a running packet dump. This is particularly useful for packet dumps with unlimited runtimes.

Download Pcap-File

Here you can download the .pcap file just created by this dialog.

View Packet Dump

Here you can view the packet dump just created in text.

10.3 Network

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

10.3-A Routing.....	65
10.3-B Interfaces.....	65
10.3-C ADSL.....	65
10.3-D WLAN.....	66
10.3-E ARP.....	67

10.3-A Routing

Routing table

On this screen you can inspect the current routing table of SX-GATE.

10.3-B Interfaces

Interface table

On this screen you can find an overview of all physical interfaces of SX-GATE. Per interface there is also a packet counter for incoming (RX) and outgoing (TX) packets. These can be useful to track down problems. For instance a high "carrier" counter indicates a faulty physical network connection. The network cable might be damaged or disconnected.

In the interface configuration of SX-GATE, logical interface names are used for some types of interfaces. The physical names of those interfaces always start with "ppp". From the interface table you cannot deduce the name of the logical interface which belongs to a "ppp" interface.

10.3-C ADSL

If an ADSL interface exists you can manually hangup a connection or test the DSL line on this screen.

ADSL monitor

On this screen you can watch the status of ADSL dial-up connections. The displayed information is updated every 3 seconds.

The following information is provided here:

Interface

The name of the SX-GATE ADSL interface is displayed here.

Status

This column indicates the status of the connection: "Offline" or "Online".

Interface

Please select the respective interface here.

Hang up now

Click this button to hang up the ADSL line if it is online.

Test ADSL line

SX-GATE will send out a PADI packet on the selected interface if you click this button. If it is answered with a PADO packet, the name of your provider's DSL access concentrator is printed.



This function will test the physical connection between SX-GATE, the DSL modem and the access concentrator at your ISP. Even if the test is successful, the network connection may fail.

10.3-D WLAN

On this page you will find information about the clients currently connected with SX-GATE's WLAN. The table includes the following columns:

wlan

Name of the WLAN interface. The tooltip shows the WLAN name (SSID) and the channel number.

MAC

The MAC address of the client.

IP

The client IP if it was assigned by SX-GATE's DHCP server. If the client sent a name to the DHCP server, it will be shown as a tooltip.

Signal

The current signal strength in dBm

received bytes

The amount of data SX-GATE received from the client. The tooltip shows the number of packets.

sent bytes

The amount of data SX-GATE sent to the client. The tooltip shows the number of packets and information about problems while sending.

connected since

The time elapsed since the WLAN connection was established.



Data counters and connection time will be reset when the SX-GATE WLAN is restarted or when the client re-connects to the WLAN.

More details about a client are available by clicking the info icon in the last column.

10.3-E ARP

ARP cache

This screen lists the contents of the ARP cache.

10.4 VPN

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

10.4-A IPsec.....	68
10.4-B OpenVPN.....	69
10.4-C Wireguard.....	70
10.4-D Web client.....	70
10.4-E SSH TCP forwarding.....	71

10.4-A IPsec

IPsec connections

On this screen you can see a list of all IPsec VPN connections which are currently active or at least routed. Each line shows the following information:

Name

Connection name given in SX-GATE's configuration section

ipsec

Name of the corresponding ipsec interface



Displayed only if multiple ipsec interfaces are configured.

Type

Connection type (Server, Client, L2tp, etc.)

Peer

The peer's current IP address if the tunnel is active

ID

Peer's ID

local / remote Net

Local and remote end of the tunnel this connection refers to

received/sent

Amount of data received and sent via the tunnel

Status

Green

Tunnel is connected

Yellow

Tunnel is pending



When stopping these connections, it may happen that the connection attempt has received a new status number in the meantime. In this case, simply press Stop again for this connection.

Red

Tunnel is not connected

White

Tunnel is not connected (dynamic or passive)

10.4-B OpenVPN

Routed OpenVPN connections

On this screen you can see a list of all OpenVPN connections which are currently active. Each line shows the following information:

ovpn

Name of the corresponding OpenVPN interface

Typ

Connection type (Server or Client)

Peer

The peer's current IP address

Certificate

Common Name (CN) of the peer's certificate

IPv4 addr.

The IPv4 address assigned to the client

IPv6 addr.

The IPv6 address assigned to the client

received bytes

Byte counter for incoming traffic

sent bytes

Byte counter for outgoing traffic

connected since

Timestamp of last successful connection

10.4-C Wireguard

Wireguard connections

On this screen you can see a list of all active Wireguard connections. Each line shows the following information:

Interface

Name of interface

Connection

Name of connection. The public key of the peer is displayed as tooltip.

Peer

IP and port of other endpoint. The public key of the peer is displayed as tooltip.

Allowed IPs

Networks that are allowed from the peer and that are routed through this connection to the peer

Status

green

Data is currently being sent through this connection

yellow

The last handshake was more than 3 minutes ago

red

Connection has not been established yet

gray

There is no status information

Transfer rx

Bytes received through this connection

Transfer tx

Bytes sent through this connection

10.4-D Web client

Active web client connections

On this screen you can see a list of all web client connections which are currently active. Each line shows the following information:

User

Web client username

Protocol

Name of the used connection protocol (rdp, vnc or ssh)

Server

IP address of the server

Connected since

Shows the connection time

10.4-E SSH TCP forwarding

SSH TCP forwarding

On this screen you can see a list of all SSH TCP forwarding connections which are currently active. Each line shows the following information:

User

Username

Source

Source IP

Destination

Destination IP

Port

Destination port

10.5 Firewall

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

10.5-A Connections.....	72
10.5-B Dynamic firewall.....	72

10.5-A Connections

Active connections

This tab shows the active connections passing SX-GATE during the last seconds. The "service" column denotes the protocol and the destination port. If application control is enabled, the detected application and possibly also a hostname are shown. The "bytes" column shows the total amount of transferred data in each direction and "Duration" the elapsed time since the connection has been initiated.

10.5-B Dynamic firewall

IP address reputation

The dynamic firewall permanently evaluates the actions of IP addresses connected with or via SX-GATE. You can inspect the current scores here. Depending on the firewall configuration, addresses with a bad score may be blocked automatically. In this case the remaining blocking time will be listed as well.



The score automatically decreases over time. In particular when an IP address is blocked for a longer period of time it may occur that the score is 0 even though the IP is still blocked.

You can delete an IP along with its current score if it has been blocked by mistake. If the same IP is blocked by mistake again, you should examine the firewall log to find out why. If the cause cannot be fixed, consider adding the IP address to the whitelist in menu "Modules > Firewall > Settings" on tab "General" to keep it from being blocked again.

10.6 DHCP

The lists of currently assigned DHCP addresses is available here.

IP address

The assigned IP

state

The current status of the IP, either "free" or "active" (currently assigned)

ends

Date and time of expiry. For a free IP the timestamp indicates since when the IP is available again. In case of an active lease, the lease has to be renewed before the given point in time.

MAC address

The MAC address of the client to which the IP was assigned.

Hostname

Some clients include the hostname while talking to the DHCP server. If available, the name is displayed in this column.

10.7 Mail server

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

10.7-A Queue.....	74
10.7-B Poll for Mails.....	75
10.7-C MIME filter quarantine.....	75
10.7-D S/MIME certificates.....	76
10.7-E Mailboxes.....	77

10.7-A Queue

Queued emails

Mails waiting in SX-GATE's outgoing mail queue are listed in this area. Apart from the internal ID of the mail, you can also see its size in bytes, the time it was queued, the sender and the recipient. In case of any problems, the respective error message is displayed, too.

Delete selected emails

To delete specific mails from the queue, please mark them in the list first. Press this button to delete all selected emails. Neither the sender nor the recipient of the mail will be notified.

Delete all emails

To delete all mails from the queue, please click this button. Senders and recipients won't be notified either.



If more mails are queued than displayed in the list, also the mails which have not been listed will be deleted. New mails which arrived between displaying the list and pressing this button will be deleted, too.

Run the queue now

If you press this button, SX-GATE tries to deliver all queued mails.

10.7-B Poll for Mails

Retrieve mails now

Press this button to start a recorded poll for emails by the SX-GATE mail client. A new browser window will open which allows you to observe the entire process of retrieving mails from the configured POP3 and ETRN servers. This is especially useful to trace problems e.g. with POP server authentication and the distribution of multi-drop mailboxes.

Abort retrieval in progress

If the message "another foreground fetchmail is running" is displayed while trying to interactively poll for emails, SX-GATE mail client is already retrieving emails. Press this button to terminate the process.



Already retrieved emails of the currently processed POP account will not be deleted when aborting. These emails will be retrieved again during the next poll.

10.7-C MIME filter quarantine

Quarantined attachments

You can download email attachments which have been quarantined by SX-GATE's MIME filter here. They will be deleted automatically after the "Storage time" configured in menu "Modules > Mail Server > SPAM/Virus/Malware" on tab "MIME filter" has been reached.

Often attachments are quarantined which in fact contain a virus which was still unknown to the virus scanner at the time the mail arrived. So quarantined attachments will be re-scanned by the installed virus scanners after each signature update. If a virus has been detected, the corresponding quarantine directory will not be re-scanned anymore.

For each email with quarantined attachments the following information is provided:

Quarantine directory

Each line starts with the directory name. It shows you the date and time when the attachments have been quarantined.

Mail ID

The mail server assigns an id to each email it processes. With this id you can find the entries which correspond to an email in the mail server log. The "Mail" column gives you the mail server id and links to the complete headers of the mail.

Sender

Recipients

State

If the attachments have not been re-scanned yet the state will be "unknown". It will change to either "OK" or "Virus" after scanning. Point at the status of a quarantine directory with the mouse to see when the mail has been scanned the last time or when the virus was detected.

Mail attachments

This column lists the quarantined attachments for download. The download won't be saved using the original filename. Please rename the file to make file extension associations work as expected.



Be very careful when downloading quarantined attachments. You should never download attachments from untrusted senders or with unusual filename extensions.

Icon column

Depending on the selected quarantine mode, emails may be retained. A green arrow is shown for these mails. Click the arrow to authorize delivery.

Click the dustbin icon to delete an email from the quarantine directory.

10.7-D S/MIME certificates

S/MIME certificates extracted from signed mails, waiting for approval

If both, verification of signatures and encryption have been enabled in SX-GATE's S/MIME gateway, certificates received as part of inbound signed emails can be used for future encryption of outbound emails. On this screen you can manage certificates waiting for approval.



Certificates which have not been approved within 6 days will be deleted automatically.

The following information is displayed for each certificate:

Email

The email address used by the sender when SX-GATE received the certificate as part of the signature. After approval outbound emails to this address will be encrypted with the certificate. Any additional email addresses in the certificate will be ignored.

received

Timestamp when SX-GATE received the mail.

Status

Yellow if the certificate verification failed. Green upon success.

Certificate

The certificate subject (Distinguished Name, DN).

expires

The certificate's expiry date

Click the info icon to get more information about a certificate. With the green arrow you can approve a certificate for encryption of outbound emails. To delete a certificate from the list, click the dustbin.

In menu "Modules > Mail Server > S/MIME gateway" on tab "Verify" you can configure if SX-GATE will use the certificates for encryption automatically or after manual approval. In the same menu on tab "Encrypt" you can see and edit the list of approved certificates.

10.7-E Mailboxes

Local mailboxes

Here you see a list of all mailboxes of SX-GATE's POP3/IMAP4 sever. Apart from the account name, the total size of the mailbox is listed.



Accounts of users who have been created but were never accessed might not be included in the overview. The mailbox will be created automatically when a mail is to be delivered.

A mail account is deleted as soon as the respective user has been completely deleted from the user administration. If the user is only removed from the group "system-mail", the mailbox will still exist. The user can continue to use it when he is a member of group "system-mail" again.

10.8 Web proxy

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

10.8-A URL filter.....	78
10.8-B Content filter.....	78

10.8-A URL filter

Here you can test the web proxy's URL filter.

URL

The URL you want to check.

IP

The source IP for the query.

User

The user you want to check.

Run query

This will run the query. You'll see if access is allowed or not and the cause of the block.

10.8-B Content filter

Content filter quarantine

A list is shown of cached downloads in descending order of their size. This list contains username (if web proxy user authentication is enabled), client IP, state of virus scanning, filename and size of download and the server, where the download came from.

The state of virus scanning can be one of the following, in case multiple virus scanners are installed, it can also be a combination:

green

No known virus scanner has been found.

yellow

The state is not clear.

- No virus scanner installed.
- expired: The installed virus scanner's license had been expired.
- unknown: The virus scanner reported errors while scanning the file.
- encrypted: The file is (partly) encrypted, so it was not possible to completely scan the file.

It will also be noted if the file contains MS Office macros (including automatically started macros).

red

A virus has been found.



We suggest that files having a yellow or red state are scanned for viruses before accessing them on a workstation.

11 Definitions

In mainmenu "Definitions" you define various objects which will be used by various setup options.

11.1 IP objects

Give a name to individual IP addresses or networks or group them. You can then use these definitions in various configuration options, e.g. firewall rules. This enhances readability and clarity.

For settings expecting IP addresses, DNS based IP objects can build the bridge to DNS data like hostnames.

Exclusively for firewall rules it is possible to create IP objects for geolocation by countries.

A table gives you an overview of the available objects. If multiple columns are displayed you can change the sort order by clicking the column title. If there are more than 20 entries, a navigation bar will appear below the bottom right hand corner of the table. You can switch between a grouped view or a pager. The full screen mode allows you to see all entries at the same time. Pick an entry by clicking its title in the left column. A pencil icon or a trashcan in the right column allow you to rename or delete an entry. Add new objects by clicking "New Entry" below the table on the left.

Object type

Select the type of object here.

Group

Objects of this type represent an arbitrary amount of addresses. It is also possible to nest objects by including other definitions.

URL Download (for Firewall)

Select this type to download an IP list from a webserver. This type of list is optimized for efficient handling in the firewall. Up to 65535 entries are possible.



IP objects of this type can only be used in firewall rules.
Nesting in IP groups is not possible.

URL Download (small lists)

Select this type to download an IP list from a webserver. Up to 999 entries are possible per list.



If you plan to use the object in the firewall, please use object type "URL Download (for Firewall)" instead, which has been optimized for this purpose.

DNS entry

The name of this group is a DNS host name. The list of IP addresses is updated automatically using DNS lookups. The DNS information is always updated after system restarts and after changes in IP objects. It is also updated when the maximum allowed cache time of the DNS entry (TTL) expires or after 3 hours, whichever occurs first.



DNS names with a digit as first character won't be accepted. Please group these DNS names in a subfolder (e.g. "123test.example.com" won't be accepted. Prepend a subfolder prefix like e.g. "dns/123test.example.com" to add this host).



Since DNS data can be forged comparatively easily, we do not recommend to use them for sensitive settings like e.g. inbound firewall rules.

DNS capture

In groups of this type you can configure DNS domains and hostnames. This always includes both, the name itself (e.g. example.com) as well as hostnames and subdomains (*.example.com). Whenever a client sends a matching DNS query to the SX-GATE DNS server, the IP addresses from the DNS response packet will be added to the IP object.



As this process takes a certain amount of time, there will be a delay when connecting to an IP address that has not been registered yet.



IP objects of this type are suitable for outbound firewall rules only. The client has to resolve DNS names using the SX-GATE name server, either directly or indirectly.

An IP address is removed automatically from the IP object when its maximum allowed cache time (TTL) has expired.

Azure servicebus (WCF relay)

This special object type retrieves the IP addresses of a WCF relay in the Azure cloud from DNS. You have to know the namespace of the WCF relay.



Since DNS data can be forged comparatively easily, we do not recommend to use them for sensitive settings like e.g. inbound firewall rules.

Host

An object of this type represents a single networking device with the three parameters MAC address, IPv4 address and IPv6 address. All three parameters are optional. Which of these three parameters are actually used depends on the context referring to the object. If a certain context requires a parameter which is not defined in the object, the object will be ignored.



Usually only the IP addresses of this object will be used. If additionally or solely the MAC address is used, the documentation of the setting will say so.

The IPv6 address may depend on a prefix. For details please see the documentation of type "IPv6 address".

IPv6 prefix

This object type represents an IPv6 prefix. It may depend upon an other, shorter prefix. This lets you split up the prefix you received from your provider.

Let's assume a prefix object contains your company's global prefix "2001:db8::/48". Now create an other prefix object, refer it to the provider prefix and configure the subnet ID "0.0.0:1::/64". The prefix object now represents "2001:db8:0:1::/64".

IPv6 address

This option lets you create a single IPv6 address. An object of this type is often needed to define the address of a SX-GATE interface. If you want to create an object which represents an other, especially local system, we recommend object type "Host" instead.

The IPv6 address may depend upon a prefix. Let's assume a prefix object represents the prefix "2001:db8:0:1::/64". If you configure the interface ID "::1234" and you let the IPv6 address refer to the prefix object, you will get the IP "2001:db8:0:1::1234".

IPv4 network

This object type represents an IPv4 network.

IPv4 address

You can define a single IPv4 address here. If you want to create an object which represents an other, especially local system, we recommend object type "Host" instead.

Geolocation (country codes)

Select this option to enter country codes. A builtin database associates each country code with a list of corresponding IP addresses.



IP objects of this type can only be used in firewall rules.
Nesting in IP groups is not possible.

Label / DNS name

Specify a name for the new network object here. You can select it later in various configuration options. If you have enabled the grouped display of table contents you can group objects by entering a folder name, '/' as separator and finally the actual object name (e.g. "dns/123test.example.com" or "vpn/subsidiary1").

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

11.1-A List download.....	84
11.1-B Addresses.....	85
11.1-C IPv6 address.....	86
11.1-D IPv4 address.....	87
11.1-E Addresses.....	87
11.1-F Geolocation.....	88
11.1-G Usage.....	88

Object type

Select the type of IP object here.

Group

Objects of this type represent an arbitrary amount of addresses. It is also possible to nest objects by including other definitions.

DNS entry

The name of this group is a DNS host name. The list of IP addresses is updated automatically using DNS lookups. The DNS information is always updated after system restarts and after changes in IP objects. It is also updated when the

maximum allowed cache time of the DNS entry (TTL) expires or after 3 hours, whichever occurs first.



Since DNS data can be forged comparatively easily, we do not recommend to use them for sensitive settings like e.g. inbound firewall rules.

11.1-A List download

Downloads a list of IP addresses from a webserver. The download may contain single IPv4/IPv6 addresses and IPv4/IPv6 networks (e.g. 192.0.2.0/24, 192.0.2.0/255.255.255.0 or 2001:db8::/64). IP objects of type "URL Download (small lists)" also support IP ranges like e.g. "192.0.2.3-192.0.2.9".

The download must be an ASCII file. The file may be compressed with gzip or bzip2 and multiple files may be joined in a ZIP or tar archive. An automatic download can be scheduled but may also be triggered manually. Entries in this list can be separated by space, tabulator or new line.



The list needs to be smaller than 25 MB.

Verify SSL-certificate

Enable this option to verify the server certificate in case of a HTTPS connection.

Username

If the web server requires a login via basic auth, please enter the username here.

Password

The password is required only if a username has been entered.

Hostname/IP

Please enter the name or IP address of the server that provides the list for download.

Port

If the server does not offer the download on standard port 80 (http) or 443 (https), please enter the port number here.

Filepath

Enter the path and the name of the file to download here. You may also add URL parameters if necessary.

Max. number of entries

Please enter the maximum number of imported entries here.



If this value is exceeded, the import will be aborted and the old values will remain.

Scheduled download

Enable the scheduled automatic download here.

Starting time

For a daily download this parameter selects the hour of the download. If the download is scheduled multiple times a day, the parameter controls the hour of the first run. The exact time, i.e. the minutes, is determined at random.

Manual Download

You can trigger a download anytime. Debug messages may be enabled for diagnostic purposes.

11.1-B Addresses

Description

This field serves for documentation only.

Last Update

Date and time of the last successful download where the list contents actually changed.

Addresses

Enter individual IP addresses or network addresses with their corresponding netmask (e.g. 192.168.0.0/24). It is also possible to include other objects.

Domains and hostnames

Enter the domains and hostnames for which the IP addresses are to be collected. This always includes all subdomains as well. If, for example, you enter "example.com", IP addresses from DNS replies for both, "example.com" and "www.example.com" will be collected.

DNS record type

Select the DNS record type to query. Usually you want to resolve a hostname into its IPv4 (A) or IPv6 (AAAA) addresses. In special cases you might want to query the IP addresses of certain services (SRV), mail servers (MX) or name server (NS).

Namespace

Enter the servicebus namespace here. If you don't know the namespace, you can temporarily enable "Log all DNS queries" in menu "Modules > DNS > Settings" on tab "Client access". Then restart the application. Now check the logs for DNS queries in format "NAMESPACE.servicebus.windows.net" (e.g. "testns.servicebus.windows.net"). You have to ignore entries where the namespace ends with "-sb" or "-mgmt" though (e.g. "g0-prod-xy3-001-sb.servicebus.windows.net").

Remove expired IPs

The IP addresses of some DNS entries are constantly changing. But often, when looking at a longer period of time, the same set of IPs is used all of the time. In these cases it makes sense to keep expired IPs for a while and let SX-GATE collect the whole set of addresses, so it doesn't have to update the configuration or even restart services unnecessarily.

Last successful verification

Date and time of the last successful DNS resolution are shown here. If the information is already pretty old, most likely the DNS record is no longer available.

11.1-C IPv6 address

Description "..."

This field serves for documentation only.

Routing prefix

You can bind this object to a routing prefix. Changes of the routing prefix are automatically reflected by this object. If the selected routing prefix currently contains no address, this object will also represent no address.

Prefix / Subnet ID

Enter the prefix. If this prefix is based on a routing prefix, it typically has to start with zeros. All bits taken from the higher level prefix must be zero, to be precise. The prefix length must not be smaller than the prefix length of the higher level prefix.



You may leave this input field empty. If a routing prefix has been selected, its value is taken instead.

IP address / Interface ID

Enter an IPv6 address. If the address is based on a routing prefix, the address typically has to start with zeros. All bits taken from the prefix must be zero.

11.1-D IPv4 address

Description "..."

This field serves for documentation only.

Network

Enter a network address with corresponding netmask.

IP address

Please enter an IPv4 address.

11.1-E Addresses

An object of this type represents a single networking device with the three parameters MAC address, IPv4 address and IPv6 address. All three parameters are optional. Which of these three parameters are actually used depends on the context referring to the object. If a certain context requires a parameter which is not defined in the object, the object will be ignored.



Usually only the IP addresses of this object will be used. If additionally or solely the MAC address is used, the documentation of the setting will say so.

Description "..."

This field serves for documentation only.

MAC address

Please enter a MAC address hexadecimal using format XX:XX:XX:XX:XX:XX. This parameter is optional. It's actually used at only a few places (e.g. for filtering by source MAC address in firewall rules).

IPv4 address

Please enter an IPv4 address. This parameter is optional.

IPv6 routing prefix

You can bind this object to a routing prefix. Changes of the routing prefix are automatically reflected by this object. If the selected routing prefix currently contains no address, this object will also represent no IPv6 address.

IPv6 address / Interface ID

Enter an IPv6 address. This parameter is optional. If the address is based on a routing prefix, the address typically has to start with zeros. All bits taken from the prefix must be zero.

11.1-F Geolocation

You can use IP objects of this type in firewall rules only.

SX-GATE includes a builtin database of all IP addresses associated with the respective country. So this is not a DNS based solution.



Database updates are shipped as part of the SX-GATE updates. So the database is only as current as the release date of your SX-GATE version.



Even though the database quality is very good, it may well include wrong entries.

Description "..."

This field serves for documentation only.

Country codes

Please enter ISO 3166 country codes as known from Internet top-level domains.

11.1-G Usage

This table show in which settings the definition is used.

11.2 Protocols

The protocol and port signature for connections can be defined in here. Capital service names are predefined and can neither be altered nor deleted.

A table gives you an overview of the available objects. If multiple columns are displayed you can change the sort order by clicking the column title. If there are more than 20 entries, a navigation bar will appear below the bottom right hand corner of the table. You can switch between a grouped view or a pager. The full screen mode allows you to see all entries at the same time. Pick an entry by clicking its title in the left column. A pencil icon or a trashcan in the right column allow you to rename or delete an entry. Add new objects by clicking "New Entry" below the table on the left.

Protocol nickname

Specify a name for the new protocol here. You can select it later on in all masks where protocols are involved.

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

11.2-A Protocol signature.....	89
11.2-B Application control.....	91
11.2-C Usage.....	91

Configuration type

Please select how the protocol is configured.

from DNS SRV records

DNS SRV records can be used to publish which servers offer a specific service on which ports. You can configure DNS based IP objects in menu "IP objects" which will query those SRV records. While the IP object will then hold the corresponding IP list, you can gain access to the port signature through a protocol definition.

11.2-A Protocol signature

In multiple SX-GATE configuration screens you will find protocol selection lists. The firewall and the SOCKS proxy configuration are good examples. The available choices for these selection lists are configured here. There are already a couple of predefined protocols, but it's also possible to add your own entries here.

There's no need to take the title "protocol" too literally. It is often handy to combine multiple protocols into one entry. For instance you could create one protocol entry for a single client or server system and then configure all acceptable protocols for this host

in there. Of course you still have to add a rule which associates the protocol with the host's IP.

From the technical point of view each "protocol" you define here refers to a list of signatures. Each signature contains the three fields IP protocol number, source port and destination port. Port numbers are only defined for the IP protocols TCP and UDP.

Description

This field serves for documentation only.

IP object with SRV port information

Select the IP object which contains the port information. The selected object may be an IP group which contains multiple SRV entries.

Signature

The protocol signature is a combination of the following columns:

Protocol

Select one of TCP and UDP. For other protocols select the lowest switch and enter either the number or the name of the requested IP protocol.

Src.port

Select the source port here. TCP based applications usually allocate a random port from the range 1024-65535. Though many UDP based applications use the same convention, other ports are frequently used, too. If you have no detailed information, you might want to select "** (any)". For ICMP you can enter the ICMP message type here.



Only UDP and TCP use port numbers, only ICMP knows about ICMP types. For all other protocols you have to select "** (any)".

Dest.port

Here you have to enter the destination port which is used to access the requested application. For ICMP you can enter the ICMP message code here.



Only UDP and TCP use port numbers, only ICMP knows about ICMP codes. For all other protocols this field has to be blank.

Included protocols

The current protocol can include the definitions of other protocols.

11.2-B Application control

With application control enabled, the firewall will analyse the transmitted payloads to detect the actual application. By enabling application control in a protocol, application control becomes available in firewall rules (except for SNAT) and bandwidth management.



If the firewall, while processing the rules, hits a protocol with application control enabled, communication has to be granted at first to allow further analyses. Rule processing won't continue until the configured application has either been detected or can be ruled out. The firewall "leaks"!

The settings on this screen apply to the protocols and ports configured at "Signature" only. They don't apply to "Included protocols" which come with their own application control settings.

If a protocol with configured application control is used in a context that doesn't support application control, the protocol is still effective. However only the settings configured on tab "Protocol signature" are used.

Application

Please select an application.



For encrypted connections often "TLS" is the right choice.

Server name (incl. subdomains)

For the applications "HTTP" and "TLS" it is possible to limit the detection on specific servers. Enter a server or domain name or select a list. You can create and manage lists in menu "Definitions > Domain lists".



"HTTP" will compare the entry with the "Host" header, "TLS" with the server name indication (SNI).

11.2-C Usage

This table shows in which settings the definition is used.

11.3 Periods

You can restrict a firewall policy rule to a certain period of time on specific weekdays by assigning to it one of the periods defined here.

A table gives you an overview of the available objects. If multiple columns are displayed you can change the sort order by clicking the column title. If there are more than 20 entries, a navigation bar will appear below the bottom right hand corner of the table. You can switch between a grouped view or a pager. The full screen mode allows you to see all entries at the same time. Pick an entry by clicking its title in the left column. A pencil icon or a trashcan in the right column allow you to rename or delete an entry. Add new objects by clicking "New Entry" below the table on the left.

Period nickname

Specify a name for the new period here. You can select it later on in the firewall configuration masks.

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

11.3-A Specification.....	92
11.3-B Usage.....	92

11.3-A Specification

Description

This field serves for documentation only.

Included intervals

The whole period is a combination of multiple time ranges. Note that in order to specify an overnight range, the start time value may be larger than the end time.

11.3-B Usage

This table show in which settings the definition is used.

11.4 Domain lists

In this menu you can define lists of host and domain names. These lists can be used in various configuration options, particularly in menu "Modules > Web proxy".

A table gives you an overview of the available objects. If multiple columns are displayed you can change the sort order by clicking the column title. If there are more than 20 entries, a navigation bar will appear below the bottom right hand corner of the table. You can switch between a grouped view or a pager. The full screen mode allows you to see all entries at the same time. Pick an entry by clicking its title in the left column. A pencil icon or a trashcan in the right column allow you to rename or delete an entry. Add new objects by clicking "New Entry" below the table on the left.

List type

manual

This type is for a manually maintained list. It is possible to import text files with server names or domains.

URL download

Select this type to download a list of server names or domains from a webserver.

Name of list

Determine the name of the new URL filter list here.



Besides small letters and digits only dashes (-) and underscores (_) are allowed. The name must begin with a letter. Particularly space characters are not allowed.

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

11.4-A List download.....	94
11.4-B Entries.....	95
11.4-C Usage.....	95

Type of list

manual

This type is for a manually maintained list. It is possible to import text files with server names or domains.

URL download

Select this type to download a list of server names or domains from a webserver.

11.4-A List download

Downloads a list of server names and domains from a webserver. The download may also contain IP addresses, however these will be checked by a simple text comparison and not by using DNS. URL like e.g. `https://www.example.com` are not supported.

The download must be an ASCII file. The file may be compressed with gzip or bzip2 and multiple files may be joined in a ZIP or tar archive. An automatic download can be scheduled but may also be triggered manually. Entries in this list can be separated by space, tabulator or new line.



The list needs to be smaller than 25 MB.

Verify SSL-certificate

Enable this option to verify the server certificate in case of a HTTPS connection.

Username

If the web server requires a login via basic auth, please enter the username here.

Password

The password is required only if a username has been entered.

Hostname/IP

Please enter the name or IP address of the server that provides the list for download.

Port

If the server does not offer the download on standard port 80 (http) or 443 (https), please enter the port number here.

Filepath

Enter the path and the name of the file to download here. You may also add URL parameters if necessary.

Max. number of entries

Please enter the maximum number of imported entries here.



If this value is exceeded, the import will be aborted and the old values will remain.

Scheduled download

Enable the scheduled automatic download [here](#).

Starting time

For a daily download this parameter selects the hour of the download. If the download is scheduled multiple times a day, the parameter controls the hour of the first run. The exact time, i.e. the minutes, is determined at random.

Manual Download

You can trigger a download anytime. Debug messages may be enabled for diagnostic purposes.

11.4-B Entries

Description

This field serves for documentation only.

Last Update

Date and time of the last successful download where the list contents actually changed.

Hostnames and domains

Compile your own list of domains here. This includes all subdomains. For instance if you enter "example.com" this will include e.g. "www.example.com" or "ftp.example.com" as well.

Included domain lists

Here you can include other domain lists into the current domain list.

11.4-C Usage

This table show in which settings the definition is used.

11.5 URL filter lists

In this menu you can define Internet access lists for the SX-GATE web proxy. These lists will then be applied to certain users, IPs or networks in the web proxy configuration.



The URL filter has to be enabled and the lists must be assigned in the web proxy configuration. Otherwise the URL filter lists won't be considered at all.

In every URL filter list you can define your own list of domains and filename extensions. An integrated, free of charge URL database or an optional commercial URL database may be used to control access based on categories.



In the web proxy configuration access to a filter list is either allowed or denied. Therefore you must not mix up contents you want to allow and contents you want to deny in one single list. Create two lists instead. Consider using postfixes in the list names like e.g. "_accept" and "_deny" to indicate the intended use.

If access is denied, a special page will be displayed to the user. URLs listed in the "Advertising" database category are an exception. If the URL includes a filename extension commonly used for images, access will be diverted to a transparent image in order to hide advertising banners if detailed "Access denied" messages have been enabled.

A table gives you an overview of the available objects. If multiple columns are displayed you can change the sort order by clicking the column title. If there are more than 20 entries, a navigation bar will appear below the bottom right hand corner of the table. You can switch between a grouped view or a pager. The full screen mode allows you to see all entries at the same time. Pick an entry by clicking its title in the left column. A pencil icon or a trashcan in the right column allow you to rename or delete an entry. Add new objects by clicking "New Entry" below the table on the left.

List type

manual

This type is for a manually maintained list. It is possible to import text files with either domains or filename extensions. Furthermore, you can select categories from the builtin URL database.

URL download

Select this type to download a URL list from a webserver.

Name of list

Determine the name of the new URL filter list here.



Besides small letters and digits only dashes (-) and underscores (_) are allowed. The name must begin with a letter. Particularly space characters are not allowed.

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

11.5-A List download.....	97
11.5-B Domains.....	99
11.5-C Files.....	99
11.5-D Database categories.....	99
11.5-E Allowed categories.....	100
11.5-F Extended.....	103
11.5-G Usage.....	103

11.5-A List download

Downloads a URL list from a webserver. The download may contain server names, domains and URLs (e.g. "http://example.com" or "https://example.com/images/ad.png?a=b"). The download may also contain IP addresses, however these will be checked by a simple text comparison and not by using DNS.



With regard to encrypted connections (HTTPS), URLs including path of filenames can only be found if the option to break encrypted connections is enabled.

The server name, domain name or IP may contain the wildcard character "*" (e.g. "srv*.example.com" or "https://www.example.*/index.html"). It matches any characters within the respective name or IP component. The wildcard character won't match multiple name components (so e.g. "www.example.*" will not match "www.example.co.uk"). The wildcard character has no special meaning in URL paths, filenames or parameters.

The download must be an ASCII file. The file may be compressed with gzip or bzip2 and multiple files may be joined in a ZIP or tar archive. An automatic download can be scheduled but may also be triggered manually. Entries in this list can be separated by space, tabulator or new line.



The list needs to be smaller than 25 MB.

Verify SSL-certificate

Enable this option to verify the server certificate in case of a HTTPS connection.

Username

If the web server requires a login via basic auth, please enter the username here.

Password

The password is required only if a username has been entered.

Hostname/IP

Please enter the name or IP address of the server that provides the list for download.

Port

If the server does not offer the download on standard port 80 (http) or 443 (https), please enter the port number here.

Filepath

Enter the path and the name of the file to download here. You may also add URL parameters if necessary.

Max. number of entries

Please enter the maximum number of imported entries here.



If this value is exceeded, the import will be aborted and the old values will remain.

Scheduled download

Enable the scheduled automatic download here.

Starting time

For a daily download this parameter selects the hour of the download. If the download is scheduled multiple times a day, the parameter controls the hour of the first run. The exact time, i.e. the minutes, is determined at random.

Manual Download

You can trigger a download anytime. Debug messages may be enabled for diagnostic purposes.

11.5-B Domains

Custom domain list (incl. subdomains)

Compile your own list of domains or IP addresses here. In the web proxy configuration you can then grant or deny access to this URL filter list and so to the listed domains. For domain names, this includes all subdomains. For instance if you enter "example.com", access to e.g. "www.example.com" or "ftp.example.com" is affected as well. The comparison is case-insensitive.



The entries listed here will be compared with the destination of a request without performing any DNS lookups. Therefore a blocked domain might still be accessible when using the corresponding IP address and vice versa.

11.5-C Files

Blocked file extensions

The URL filter can grant or deny access to certain types of files based on the filename extension. Simply add the requested extensions to the list. It makes no difference, if you specify an extension as e.g. "mp3", ".mp3" or "*.mp3". All three formats refer to the extension "mp3". SX-GATE tests each request, if the filename ends with a dot, followed by one of the listed extensions. The comparison is case insensitive.



SX-GATE will compare the filename from the requested URL with the extensions from the list. There won't be any analysis of contents received from the Internet.

11.5-D Database categories

Entertainment

Chat, private forums, gaming, shopping, sports and many more.

German school project "Deutscher Bildungsserver"

The German school project "Deutscher Bildungsserver" has kindly provided us with an online resources database. A whitelist has been generated which allows access to the addresses included. However, links from these online resources to other servers or server areas are generally not covered.

Harmless servers

Banks, blogs, health, jobs searches, references, news and papers and many more not found in other categories.

11.5-E Allowed categories**Porn**

Adult content (pornography) and websites which are unsuitable for children.

Violence

Websites about violent behavior and aggressive sales of arms.

Arms and weapons

Websites about shooting ranges, real weapons and toy/game weapons that look like real weapons. Toy guns and water guns that do not look like a real weapon are excluded. If gun sport sites do not display arms in a prominent or aggressive way, they are excluded and part of the Sports category.

Warez (cracks, license keys)

Websites with illegal software, illegal software codes, hacker's sites, warez and cracks.

Illegal acts

Websites explaining how to perform illegal activities.

Hard drugs

Websites about hard drugs. Educational sites about drugs and sites about soft drugs are excluded.

Softdrugs

Websites of producers and sellers of soft drugs and websites that promote or discuss the use of soft drugs. Websites that exclusively have cannabis-based products for medicinal use and websites of governments and health institutions are excluded.

Alcohol

Websites of producers of alcohol and websites where most content is about sales or consumption of alcohol. Restaurants, bars, supermarkets etc. are not included. Some beverage markets are included.

Proxy server

Sites that can be used to download content of other sites, URL rewriting sites and VPNs. Proxies are commonly used in an attempt to circumvent a URL filter and should always be blocked. Sites that translate words or text but not websites are excluded.

DNS-over-HTTPS

Websites and IP addresses and domainnames of services for DNS lookups over HTTPS. DNS over HTTPS is a simple and effective way to circumvent URL filtering and it is recommended to use this category.

Microsoft data collection

URLs used by Microsoft to collect user and system data from workstations, browsers and apps.

Advertising

Websites with advertisements, user behavior monitors, traffic trackers and web page counters.

Parked domains

Parked domains no longer have regular content. They are parked to be sold and/or make revenue from ads. Some parked domains use low-quality ad brokers with relatively high rates of scams and malware.

Peer-to-Peer

Sites where one can exchange files. You will often find movies, music and adult content, that also violates copyright.

Blogs, private sites/web disks

Blogs, private homepages and private online storage.

Dynamic Addresses

Computer systems without a static address use dynamic addresses which are usually managed by dynamic DNS servers (DDNS servers). DDNS is often used to gain remote access to computer systems at home and can also be used as proxies.

Toolbars

Websites for toolbars of browsers. A toolbar is an extension to a web browser that may violate your privacy or make private files public.

Entertainment

Entertainment, lifestyle, hobby, arts, museums, fashion, electronic cards, magazines, horoscopes, desktop wallpapers, clip art, photos, portals, events, fan sites, baby-related, child sites, picture sharing and other sites for interest of private persons that are not related to business.

Education

Websites of schools, universities, driving schools and various other educational institutions.

Restaurants and recipe sites

Websites of restaurants and recipe sites. Note that supermarkets, take-away and fast food chains are in the Shopping category.

Health, healthcare, health insurance

Websites of hospitals, clinics, doctors and websites with information about health.

Buy or rent a place to live

Websites of real estate agents and construction companies with a focus on houses and apartments

AI bot chats

Websites where people can talk with an AI bot. Chatbots for education, business and customer support etc. are not included.

Chat

Websites for chat and messaging.

External web-based applications

Web-based text editors, spreadsheet applications, desktops and groupware.

Private forums

Websites with a forum. Business-related forums are not included.

Sports

Websites related to sports including sports sections of news sites, fans of sports, sites about actively doing a sport.

Shopping

Websites with shops, price comparisons, and auctions aimed at consumers. Websites focused on business clients are excluded.

Travel

Websites about travel agencies, airliners, tourism sites, hotels, holiday resorts.

Job search

Websites about and for job applications. Websites for student job experience applications are not included.

Finance

Websites of banks, insurance companies, stock markets and stock brokers.

Stock markets and trading systems

Websites about stock markets and trading systems as well as websites related to investments.

German school project "Deutscher Bildungsserver"

The German school project "Deutscher Bildungsserver" has kindly provided us with an online resources database. A whitelist has been generated which allows access to the addresses included. However, links from these online resources to other servers or server areas are generally not covered.

Harmless servers

This database contains addresses serving content which does not fit into any of the other categories.

11.5-F Extended

Description

This field serves for documentation only.

Last Update

Date and time of the last successful download where the list contents actually changed.

Block addresses containing porn keywords

If this option is activated, the requested address (URL) will be scanned for key words that may insinuate pornographic content.



Also here only the address itself will be checked, not the actual contents of the addressed Internet server.

Remove adult sites from search results

Many search engines offer a filter mode, removing adult sites from search results. If access to this URL filter list is denied and the option is enabled, filter mode will be enforced for most of the common search engines.

11.5-G Usage

This table show in which settings the definition is used.

12 System

You can find all needful issues for the day by day administration of your SX-GATE in the mainmenu "System". Among others it comprises the user administration as well as the backup and update functions.

12.1 Setup

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

12.1-A LAN parameters.....	104
12.1-B Download proxy.....	105
12.1-C Clustering.....	105
12.1-D Administration server.....	108
12.1-E Management access.....	110

12.1-A LAN parameters

On this screen you can modify the most important parameters of SX-GATE's LAN interface. Many other settings of SX-GATE use these values as default setting.

Hostname

Enter the hostname of SX-GATE here.

Domain

Insert the domainname for SX-GATE here. If your company already reserved or connected an Internet domain you should use this one. Otherwise enter a name which is guaranteed not used in the Internet (e.g. "company.internal") to avoid domain conflicts.



The domain mentioned here has nothing to do with a Windows NT domain.

IP address

Enter the IP address of the primary Ethernet adapter of SX-GATE here. Usually this interface is connected with your internal LAN.

Netmask

The netmask which corresponds to the internal IP address has to be specified here.

Language

Select the default language of SX-GATE's administration GUI here.



To reflect a change of the default language you will have to reenter the GUI. You might have to clear your browser's cache first.

12.1-B Download proxy

Here you can configure a global proxy that must be used for downloads initiated by SX-GATE. This includes e.g. updates of SX-GATE, antivirus signatures, IDS and URL filter lists.

12.1-C Clustering

With this function you have the ability to use two SX-GATEs as a failover cluster. No additional interface is needed, since the synchronisation can be done over the lan interface. The lan interfaces of the two SX-GATEs should be connected to the same switch.



We recommend to contact technical support before using this feature in order to clarify technical constraints.

Each cluster node has its own interface definitions. The rest of the settings are configured on the backup node. Use the "Update configuration on master" button to update the master's configuration. Before the configuration can be transferred, you have to upload the public ssh-ed25519 key or ssh-rsa key of the backup node to the master.

The cluster is monitored by the service called "Cluster node". It must be activated in menu "System > Services".

To make the cluster appear as one single server, you have to configure a shared virtual ip address (vip). This will be done at "Modules > Network > Interfaces". Choose the corresponding interface and insert the appropriate address at "Additional IPv4 addresses (aliases) / Cluster IP addresses". Make sure that a corresponding interface with the same name is also configured on the master node.

Member in failover cluster

Choose the role of this SX-GATE in the failover cluster.

Master IP

In this field you insert the IP address for the interface on the master node, which is used for the synchronisation between the master and backup. Normally the lan interface is used.

Backup IP

In this field you insert the IP address for the interface on the backup node, which is used for synchronisation between the master and backup. The IP addresses of master and backup must be from the same address range.

Export public SSH key

Here you can download the public ssh key. Please import the key on the master, otherwise the backup won't be able to update the master's configuration.

Manage SSH Keys

Here one can manage the Master's Public SSH Key entries on the backup. In case the Backup is unable to communicate with the master, the Master has been replaced, or a new Master has been added, please click here.

Manage SSH Keys

In order for the Backup to be able to sync configuration and mail to the Master, the two need to be able to communicate together via SSH. To ensure the Backup is talking to the correct node, we need to import the Master's Public SSH keys onto the Backup. This wizard allows one to examine the current Public SSH key entries for the Master, as well as the Public SSH keys seen from the configured IP for the Master. If at least one of the different types of these known and seen keys match, then everything is already in order, and this dialog can be exited. If not, then one can delete, add, and replace keys here. When adding keys seen from the Master's configured IP, one should first check if these match with the Keys on the Master as displayed in the Master's Admin interface.

Current Public SSH Key Entries for the Master Node

These are the current entries for the Master's public SSH keys as they exist here on the Backup. If public SSH keys from the Master node are also displayed, at least one of these should be identical.

Last seen Public SSH Keys from the Master node

These are the public SSH keys that have just now been reported by the IP configured for the Master node. If any current Public key entries are also displayed above, and at least one of these is identical, no further action is required. If not, these keys should be double checked against their entries on the Master node visible through the Admin interface. If these keys are the same as those displayed by the Master node, and are not

already displayed above, then they should be added, or used to replace any previously existing keys.

Please select

Do nothing

In case everything is already in order, you can click [here](#).

Replace current entries with newly found keys

In case the current entries for the Master's public SSH keys should be completely removed, and then replaced with those just seen from the IP configured for the Master, please click [here](#). This is expected if the Master node has been replaced. It is important that the newly added keys have been confirmed against those displayed in the Master's Admin interface.

Add the newly found keys

In the case of a new Master node, new Master keys, a key rotation, or similar, this option can be used to import the Public SSH keys just seen from the IP configured for the Master. It is important that the newly added keys have been confirmed against those displayed in the Master's Admin interface.

Delete current entries

In case the cluster has been dismantled, our entries for the Master's public SSH keys are incorrect, or for some other reason it is wished to delete the current entries for the Master's public SSH keys, please click [here](#).

Temporary access to all settings

Gain access to all settings until you log out. All changes to otherwise unavailable settings will be lost when the next synchronization with the backup node is performed.

Upload public ssh key

Here you import the public ssh key of the backup node.

Synchronize automatically

Configuration changes on the backup system must be propagated to the master. A manual synchronization is started by clicking on "Update configuration on master". Enable the automatic update to ensure that no one forgets this step.



We recommend to enable automatic synchronization at least for user settings if users have access to the "My Account" menu. As the Administrator never knows when a user changes personal settings, this is the only way to guarantee their prompt propagation.

Delay after last change

If set to "0", each configuration change immediately propagates to the master. Otherwise the synchronization will be delayed until the configured period of time has elapsed since the most recent modification. So multiple subsequent configuration changes will aggregate to one single update. This reduces the number of service restarts on the master.

Update configuration on master

With this option you transfer the current configuration to the master node. In addition to the user and system configuration, private keys and certificates are copied as well. Keys and certificates on the master node are overwritten. As an exception, if a service is using a self-signed certificate, it is not transferred. The following components are affected:

- SX-GATE CA (the private key is not copied!)
- SX-GATE VPN server (IPSec and OpenVPN)
- connection specific keys of OpenVPN client interfaces
- SX-GATE mail server (SMTP, IMAP and POP3)
- SX-GATE reverse proxy

The following keys and certificates are excluded as they are either individual for each node or the use on the master node does not make sense:

- private key of the SX-GATE CA
- SSL proxy CA for inspecting SSL connections
- SX-GATE administration

My Public SSH Keys

Display the SSH public key(s) of this computer. This is needed to verify this computer to any connecting clients. Typically the backup node of a cluster.

12.1-D Administration server

On this screen you can configure the administration webserver.

One-time passwords for direct access

In addition to login and password a one-time password may be required to access the administration interface. With this option you can configure if one-time passwords are required for direct access to port 44344 (or unencrypted to port 8000).



Direct access is usually used from clients in the local networks. Please use the reverse proxy if Internet access to the administration interface is required.

Changing this setting will affect the current session, so it cannot be reverted without successful one-time password authentication.



Enable one-time passwords gradually. First you should make sure that a second user has access to this menu. Enable one-time passwords only for one of the users, then pick option "optional".



No one-time password is required for direct access from the console (127.0.0.1).

optional

Only users with one-time passwords enabled in the user administration have to provide a one-time password when this option is selected. All other users can authenticate themselves without a one-time password.

mandatory

All users have to provide a one-time password when this option is selected. Users with one-time passwords disabled in the user administration cannot login this way.

One-time passwords for access via reverse proxy

In addition to login and password a one-time password may be required to access the administration interface. With this option you can configure if one-time passwords are required for access via reverse proxy. Usually the reverse proxy is used when Internet access to the administration interface is required.

optional

Only users with one-time passwords enabled in the user administration have to provide a one-time password when this option is selected. All other users can authenticate themselves without a one-time password.

mandatory

All users have to provide a one-time password when this option is selected. Users with one-time passwords disabled in the user administration cannot login this way.

Temporary access to hidden menus

Gain access to otherwise hidden menus until you log out.

Select HTTPS key/certificate

This certificate is needed for direct encrypted access to the administration interface. When using the reverse proxy, this certificate is not taken into account.



Use the reverse proxy to access the administration from the Internet. The reverse proxy can limit access to certain parts of the administration interface (e.g. email quarantine only). Or the reverse proxy can enforce authentication by client certificate to securely provide Internet access to the administration server.

Please select one of the keys managed in menu "System > Certificate manager > Keyring".

12.1-E Management access

If SX-GATE is to be managed by a central system you have to enable the remote access on this screen.

Connection type

Select how the connection between SX-GATE and the central management server should be established.



When changing this setting any established outgoing tunnels are terminated.

incoming

Select this option if the management server opens a direct connection to your SX-GATE. The management server uses a Secure-Shell (SSH) connection to port 22.

This type of connection is probably the best choice if you already have a VPN connection between the management server and SX-GATE. The management server should connect to the internal IP of SX-GATE.

If there's no VPN connection, but the SX-GATE SSH server is reachable from the Internet and the management server has a static IP, you can use this connection type as well. In the firewall configuration of the Internet interface you need to grant "SSH" access for the management server to SX-GATE.



Do not grant firewall access for any source IP. Only the management server should be allowed.

Cluster nodes can use this connection type only if the management server can address both nodes with an individual IP.

outgoing

This connection type is a bit more complicated to configure but works in almost any situation. Here the managed SX-GATE initiates an SSH tunnel connection to the management server, using port 2222 (SSH TCP-Forwarder). The management server is then able to connect to your SX-GATE using this tunnel. It is not necessary to configure firewall rules in this case.

Managementserver

Here you specify the address of the management server to which SX-GATE should connect in case of "Connection type outgoing".

Connection ID

In case of "Connection type outgoing", enter the connection ID which is allocated by the administrator of the management server.

Private key for access to management server

In case of an outbound connection SX-GATE will use this key to authenticate at the management server.



Private keys are managed in menu "System > Certificate manager > Keyring".

Corresponding public key

Please pass this public key to the administrator of the management server to grant access for your SX-GATE.

Public ed25519 key, which grants the owner of the corresponding private key access to your SX-GATE

Please ask the administrator of the management server for this key. It grants access to your SX-GATE for the management server via ssh.

Show error messages

If the connection to the management server should fail, you can inspect the error messages here.

Update public key of management server's SSH TCP forwarder.

If it became necessary to change the SSH key of the management server's TCP forwarder, you can update the stored public key here.

Import installation package for management access

To configure management access to this device easily, you may have been provided with an installation package. All you have to do is upload the file and enter the corresponding password.

Upload installation package***Installation package (*.rin)***

12.2 Services

Most SX-GATE services are shown in this menu. You can start, stop or restart services here. The green and red symbols indicates the current status of the services.



"Start", "restart" and "stop" also determine if the service will be launched next time the system is booted.

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

12.2-A Network.....	113
12.2-B Server.....	115
12.2-C More servers.....	117
12.2-D System.....	118

12.2-A Network

On this screen you can see the current status of SX-GATE network services.



On the backup node of a cluster a "yellow" status is displayed for paused services. A service is paused if it may only run on the active node.

Ethernet

This service represents the network interfaces of SX-GATE. Since these are vital, this service can only be restarted. It is not possible to stop this service, as otherwise even access to the web interface of SX-GATE would be impossible.

WLAN

This service allows clients to connect via wireless lan.

IPv6 router advertisement

This service is required to run SX-GATE as IPv6 router.

ADSL (PPP over Ethernet)

ADSL dial-on-demand connections are the subject of this service. A restart of this service will disconnect all established ADSL dial-up connections.



If all ADSL interfaces have been configured to keep the dial-on-demand connection permanently online, this service will be marked as stopped until at least one connection has been established successfully.

Wireguard VPN

If you want to use Wireguard VPNs (Virtual Private Networks), this service must be started. Restarting this service will terminate all currently active Wireguard connections.



It is not possible to start this service if no wg interface has been configured yet.

IPSec VPN

If you want to use IPSec VPNs (Virtual Private Networks), this service must be started. Restarting this service will terminate all currently active IPSec connections. However the peers will be notified, so a new connection can be negotiated just after the reinitialization.



It is not possible to start this service if no ipsec interface and a corresponding connection has been configured yet.

L2TP server

Activate this service if you want to use IPSec L2TP connections. When restarting this service all currently active L2TP sessions will be disconnected.

OpenVPN

If you want to use OpenVPN based VPNs (Virtual Private Networks), this service must be started. Restarting this service will terminate all currently active connections.



It is not possible to start this service if no ovpn or ovpn interface has been configured yet.

Firewall

The SX-GATE firewall is always active. Therefore it is not possible to stop this service. However it can be restarted.

Intrusion Detection

The Intrusion Detection System (IDS) analyzes the contents of IP packets, using a signature database. Suspicious packets will be logged. The IDS can be activated per interface in the firewall setup.

DHCPv4 server

The DHCP service is used to automatically assign the IP configuration to systems in the LAN. These systems have to be configured accordingly.

DHCPv4 relay

The DHCP relay service forwards queries to a DHCP server in another network.

DHCPv6 server

The DHCP service is used to automatically assign the IP configuration to systems in the LAN. These systems have to be configured accordingly.

12.2-B Server

On this screen you can see the current status of SX-GATE's server applications.

Name server (DNS)

This service is required for DNS name resolution. Clients in internal networks should send DNS requests to this service which in turn forwards them into the Internet. Besides using it as DNS forwarder, SX-GATE' DNS can also manage the DNS information of internet domains.



All components on SX-GATE which rely on DNS informations will contact this server application. Therefore it is crucial that this service is running in normal operation.

Mail server

This service provides an SMTP mail server. Internal clients as well as internal mail servers should relay outgoing emails via the SMTP server of SX-GATE. Use this service also for the delivery of incoming emails. SX-GATE can accept SMTP connections for incoming emails. In combination with SX-GATE's mail client, the mail server is also used to deliver emails retrieved from POP servers in the Internet. Incoming mails can either be delivered to local mailboxes or forwarded to an internal mail server.



For the delivery of system generated emails, this service is not required.

POP/IMAP server

This service provides access to mailboxes stored on SX-GATE.



You can also use the SX-GATE groupware to access mailboxes.

Web proxy

Browser access to the Internet should make use of SX-GATE's web proxy. The web browser has to be configured accordingly.

Reverse proxy

The reverse proxy provides access to web servers in the LAN or it can be used as a load balancer for access to DMZ web servers.

SIP proxy

This service provides an outbound proxy for the Voice-over-IP protocol SIP.

POP3/SMTP proxy

This transparent proxy allows users to connect with POP3 and SMTP server on the Internet. The proxy runs on port 8110.

SOCKS proxy

SOCKS is a generic proxy running on port 1080.

SSH TCP forwarder

Secure-shell clients can establish authenticated and encrypted channels with the TCP forwarder. Then TCP connections to (usually internal) servers can be opened using these channels. The SSH TCP forwarder is available on port 2222.

HTTP server

If this server is running, SX-GATE provides a simple web server. It can be used to publish documents for the internal networks. An additional web space can be configured, which will also be available on the Internet.

Windows shares

Activate this service if you want to have access to SX-GATE's web server directories via Windows network shares.

NTP time server

The NTP time server allows clients to synchronise their system time with SX-GATE's.



If the clients synchronise using the protocols time, daytime or the windows shares, it is not necessary to activate this service.

Though this service is not required for synchronising SX-GATE's system time with NTP servers in the Internet, it permanently adjusts the time when enabled.

SNMP-Server

The SNMP server is used to monitor the SX-GATE via the Simple Network Management Protocol. The service is configured in menu "Modules > SNMP server".

12.2-C More servers

The services listed below are often used quite infrequently. To save system resources the corresponding server is not active permanently. A meta server is monitoring the port corresponding to the respective application and will launch the server on demand. Determine on this tab which services the meta server will provide.

Service

This service makes all of the following server applications available.



Stopping this service will terminate all the servers below.

FTP proxy

An FTP proxy is available on TCP port 2121. FTP clients should make use of this proxy whenever they need to contact FTP servers in the Internet. Configure the FTP proxy in the menu "Modules > More Proxies > FTP proxy".



Only "real" FTP clients can use this proxy. For FTP access with a web browser the web proxy on TCP port 8080 must be used instead.

FTP server

FTP is used to download or upload files. On SX-GATE this is allowed for specific users only. Please refer to "Modules > FTP server" for further information.

TFTP server

TFTP is a very simple protocol for sharing files. It has neither options for encryption nor for authentication. Everyone with access to the TFTP port of SX-GATE is able to upload and download files!



So please make sure that only those devices have access to TFTP port 69 (UDP) that really need it. Configure firewall deny rules as appropriate.

Files on the TFTP server are managed by the pre-defined user "ftpadmin", that can be enabled in menu "Modules > FTP server". Connect to the SX-GATE FTP server, log in as "ftpadmin", go up to the topmost directory and then change into directory "_tftp". You can publish files for download there and you will find any files uploaded with TFTP in there.

File uploaded to SX-GATE with TFTP can be overwritten, but it is not possible to download them via TFTP. To allow the download, "ftpadmin" has to grant read permissions to everyone on the file.

Time

On TCP port 37 SX-GATE offers its current system time in machine readable form. Enable this service to synchronise clients using the time protocol according to RFC 868.

Daytime

The system time is available on TCP port 13, too. In contrast to the previous service the time is presented in human readable form.

12.2-D System

On this screen you can see the current status of some system services.

Logging

The majority of SX-GATE's components use this service to log various informational messages, status reports or errors.



It is not advisable to disable this service for a longer period of time. Not only the cause of problems, also security-related incidents can not be analyzed in this case.

Scheduled commands

This service is required for the scheduled execution of various programs. For example, this included generating statistics, archiving and rotating logfiles, scheduled mail retrieval and also the automatic update of virusscanner signatures.



Also this service should not be disabled for a longer period of time. Several important functions will not be available otherwise.

Service monitoring

This system service is used to monitor the following services:

- Name server (DNS)
- Mail server
- Web proxy
- Reverse proxy
- SIP proxy
- POP3/SMTP proxy

A service exiting without any reason will be automatically restarted by the service monitor.



The monitor checks the system's process list. A service which is still running but no longer responding won't be detected.

If a service keeps failing it will remain stopped and has to be restarted manually. On a cluster master this will cause a failover until the service is either disabled or running again.

Cluster node

This service is used for the clustering (Menu "System > Setup", tab "Clustering").

Windows domain membership

With this service SX-GATE can join a Windows domain. Currently this is only necessary for the web proxy NTLM authentication feature.



Before SX-GATE can join the domain, a machine trust account has to be created for SX-GATE. We suggest using the wizard "Proxy configuration" for this.

Apcupsd UPS client

If SX-GATE's power supply is backed by an APC UPS which is monitored with apcupsd, SX-GATE can query the UPS status and shutdown in time if necessary.

Secure shell server (SSH)

This service allows encrypted network access to the operating system level of your SX-GATE. Its primary use is for technical support. If the service is not running it will be started on demand by the support access wizard. In some situations the service can be helpful for the local administrator, too.



On the master node of a SX-GATE cluster the SSH server is required for synchronizing the configuration.

SX-GATE configuration

The web administration interface of SX-GATE is operated by this service. Therefore it is not possible to stop it.



When restarting this service, the browser will most likely report an error just after submitting the request. Due to the restart it was not possible to send a response.

12.3 User administration

The primary purpose of SX-GATE's user administration is to control access to certain SX-GATE services. For this, SX-GATE provides four builtin groups which cannot be deleted: "system-mail", "system-proxy", "system-ras" and "system-admin". Users who are member of these groups have a personal account and password which allows them to use the services that belong to the respective group.

The purposes of these system groups are:

system-mail

The "system-mail" group contains all users who have an email account on SX-GATE. Users can access this account with POP3, IMAP4 or the SX-GATE groupware.



If a user is removed from the "system-mail" group, the corresponding mailbox will be kept. The user can continue to use it when he is re-added to the group at a later point in time. However, if the user is deleted completely, the mail box will be deleted, too.

Every group acts as a mail distributor. As every local user must be member of "system-mail" to get an email account, emails addressed to this group will be delivered to every local user automatically.



To make this mail distributor available under a more common name (e.g. "staff") add a new group with the requested name and add the entry "system-mail" to the list "External mail addresses" on tab "Mail settings".

system-proxy

A user must be member of this group to gain access to those SX-GATE proxies which require authentication.

system-admin

Members of this group have access to the SX-GATE administration. The "My Account" menu is always available for every member. Access to additional menu items can be granted by the administrator.

system-ras

For some IPSec connections SX-GATE requests user authentication. Only members of this group will be accepted by SX-GATE.

12.3.1 Settings

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

12.3.1-A Active Directory link.....	122
12.3.1-B Import of users and groups.....	124
12.3.1-C Synchronisation of passwords.....	127

12.3.1-A Active Directory link

You can link SX-GATE with Microsoft's Active Directory. This feature can be used to import users and groups once or sync them regularly. If SX-GATE's mail server forwards inbound emails to an internal Exchange server, SX-GATE can verify recipient addresses by looking them up in the Active Directory.



SX-GATE doesn't modify the contents of the Active Directory.
Read only access is sufficient.

Active Directory server

Enter the IP address of the Active Directory server which keeps the user information. Usually this is the IP of the domain controller.

LDAP searchbase

Specify the LDAP path used by SX-GATE when binding to the Active Directory. All relevant users and groups must be situated below this path in the LDAP hierarchy.

The simplest searchbase is the name of the Active Directory server (e.g. ad.example.com). But you can also enter any Distinguished Name (DN) like for example "CN=users,DC=ad,DC=example,DC=com" or "OU=internet-users,DC=ad,DC=example,DC=com".

Login for searching in Active Directory

Leave this field empty if an anonymous search is allowed in the Active-Directory or else specify the login of a user which has the required permissions (Bind DN). If the user is a member of Active Directory container "users", entering the user name (e.g. "searchuser") is sufficient. Otherwise you have to specify the complete DN here (e.g. "CN=searchuser,OU=it,DC=ad,DC=example,DC=com").



In Microsoft's SBS you have to use a DN like e.g. "cn=searchuser,OU=SBSUsers,OU=Users,OU=MyBusiness,DC=example,DC=com".

Password

If authentication is required by the Active Directory, the password goes in here.

Use SSL encryption

Enabling this option will encrypt all communication between SX-GATE and Active Directory.

Check LDAP connection

If at least the server address has been configured you can test the LDAP connection with this button.



Please press "Apply" to commit any changes you have made on this screen before starting the test.

12.3.1-B Import of users and groups

Users and groups can be imported from an Active Directory. The Active Directory has to be prepared for the import as follows:

- Create a distribution group (e.g. "internet-users"). Later this group will contain all objects to be imported.
- All the groups which have to be imported by SX-GATE must become a member of this distribution group.



Only direct group members will be taken into account. Subgroups will not be imported.

Usually you will create the relevant SX-GATE system groups in the Active Directory.

- All direct and indirect user members of each selected group will become a member of the imported group on SX-GATE.



The results of a hierarchical search in the group structure below the currently processed group will determine the indirect members.

- The set of users which has been collected that way decides which users have to be available in the user administration of SX-GATE.

Now what about the users and groups which are available on SX-GATE but not in the Active Directory? In general it makes no difference if the respective user or group has been added on SX-GATE by hand or if it is an imported object which is no longer selected in the Active Directory.



During the import procedure neither users nor groups will be deleted completely on SX-GATE. This avoids the loss of data and settings.

- The members of a SX-GATE system group will not be changed if this group is not or no longer found in the Active Directory.
- A non-system group will lose all of its members. Note that the group will still serve e.g. as a mail distributor for external recipients. Delete the group by hand if it is no longer needed.
- From this it follows that a user will continue to be a member of the system groups which are not available in the Active Directory. He will no longer be member of any other group. Delete redundant users manually.

SX-GATE uses the standard windows name (Common Name) when importing a group. For a user, the compatibility name for "pre-Windows 2000" is used instead (SAMAccountName). Upper case characters in user or group names will be translated to lower case automatically.



Users and groups which do not comply with the naming conventions of SX-GATE won't be imported. The name must begin with a letter and must consist of the letters "a" through "z", digits, dots, dashes and underscores.

In addition to the user and group structure the user's passwords can be imported, too. However this requires the installation of a library (DLL) on the windows domain controller. Please refer to tab "Synchronisation of passwords" for further information.



The account of a new imported user is locked until the administrator assigns a password on SX-GATE. If the password DLL is installed on the domain controller and a password has been stored in the Active Directory the account will be enabled immediately.

Active Directory SX-GATE group

Determine the Active Directory group which contains all the objects to be imported by SX-GATE. If all users and groups are members of the Active Directory container "users", entering the group name (e.g. "internet-users") is sufficient. Otherwise you have to specify the complete Distinguished Name (DN) here (e.g. "CN=internet-users,OU=it,DC=ad,DC=example,DC=com").



In Microsoft's SBS you have to use a DN like e.g. "cn=internet-users,OU=SBSUsers,OU=Users,OU=MyBusiness,DC=example,DC=com".

In Active-Directory, all direct members of this group should be group objects. These object will become groups on SX-GATE. All user objects found below this layer of groups will eventually become SX-GATE users. Note that the users may be members of sub-groups, however the sub-groups themselves won't be imported as group objects.



Active Directory user objects which are direct members of the group you specified here are not taken into account while importing.

Time interval of automatic import

With this parameter you can either disable the automatic synchronization or specify the interval between two imports.

Send import protocol

An import log can be mailed to the administrator. Please choose under which circumstances the log will be sent.

Test import

With this button you can test if the expected user and group structure can be found in Active Directory.



Please press "Apply" to commit any changes you have made on this screen before starting the test.

Import now

Press this button to start the user and group import. If the SX-GATE password DLL has been installed on the domain controller the user's password will be updated, too. A log of the whole process will be displayed in a new browser window.



Please press "Apply" to commit any changes you have made on this screen before starting the import procedure.

12.3.1-C Synchronisation of passwords

The Microsoft Active Directory denies access to the stored user passwords. To make the password replication possible, a library (DLL) has to be installed on the Windows domain controller. The DLL becomes part of its password change procedure. Anytime a user password is changed it is passed to the DLL in plaintext. The DLL will then compute a one-way hash which is used by SX-GATE to authenticate users. This hash value is saved in the Active Directory and SX-GATE reads it while importing the users.



A one-way hash allows no reverse engineering of the original password.

To install the DLL, please download and start the setup program. Reboot the domain controller to activate the library.

12.3.2 Users

A table gives you an overview of the available objects. If multiple columns are displayed you can change the sort order by clicking the column title. If there are more than 20 entries, a navigation bar will appear below the bottom right hand corner of the table. You can switch between a grouped view or a pager. The full screen mode allows you to see all entries at the same time. Pick an entry by clicking its title in the left column. A pencil icon or a trashcan in the right column allow you to rename or delete an entry. Add new objects by clicking "New Entry" below the table on the left.

User login

Determine the login of the new user here.



Besides small letters and digits only dashes (-), dots (.) and underscores (_) are allowed in the login. The user login must begin with a letter. Particularly space characters are not allowed.

First name

Here you can enter the user's firstname. This field is optional.

Surname

Optionally enter the user's surname here.

Password

Determine here the password for the new user.



By default, a new user will not be able to access any SX-GATE service which requires a password. The new user has to be added to system groups to be authorised for the respective services.

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

12.3.2-A Groups.....	128
12.3.2-B Password.....	129
12.3.2-C Mail administration.....	130
12.3.2-D Mail forwarding.....	132
12.3.2-E SPAM filter.....	133
12.3.2-F SPAM scores.....	134
12.3.2-G SPAM lists.....	136
12.3.2-H Vacation.....	137
12.3.2-I Mail folders.....	138
12.3.2-J SOCKS proxy.....	138
12.3.2-K RDP Web Client.....	139
12.3.2-L VNC Web Client.....	143
12.3.2-M SSH Web Client.....	144
12.3.2-N SSH TCP forwarding.....	146
12.3.2-O RAS settings.....	147
12.3.2-P Docklets.....	148
12.3.2-Q Menu Statistics	149
12.3.2-R Menu Monitoring	149
12.3.2-S Menu Definitions	149
12.3.2-T Menu System	149
12.3.2-U Menu Wizards	150
12.3.2-V Menu Modules	150
12.3.2-W Login options.....	150
12.3.2-X User details.....	150

12.3.2-A Groups

This mask will show you the group membership of the selected user. To add or remove the user from several groups at a time you can select multiple entries from the respective list. Hold down the CTRL key while selecting a group to accomplish this.



When creating a new user he will not be member of any group. Particularly no account will have been created for the user yet. Add the user to the respective system groups to grant privileges.

The following list will give you a brief overview of the system groups:

system-admin

Members of this group have access to the administration GUI of SX-GATE. By default users will only gain access to the "My Account" menu. However the administrator can grant access to other menus, too.

system-mail

The user has a mailbox on SX-GATE. Access to this mailbox is possible via POP3, IMAP4 or groupware with login and password.

Optionally the user can be entitled to use the credentials for authenticated access to the mail relay server of SX-GATE. This is necessary if the mail server has been configured to forward mail to the Internet only after a successful SMTP-Auth login.

system-proxy

Some of SX-GATE's proxies can be configured to allow authenticated access only. By adding a user to this group you can grant the required right.

system-ras

Members of this group are able to authenticate IPsec-XAuth and IPsec-L2TP connections to SX-GATE.



The user "admin" is always member of the system groups "system-mail" and "system-admin". Therefore these groups are not listed when "admin" has been selected.

12.3.2-B Password

On SX-GATE there are two types of passwords. The user password already has to be assigned when adding a new user. The user can change this password anytime at "My Account > Change password", provided he is member of group "system-admin" and therefore has access to the administration GUI.

The administrator can assign a static password per system group. This password can only be set on this screen and therefore it is only changeable by administrators.

Reset user password

In this area you can change the user password. This will affect all accounts of the user which have not been configured to use a fixed password.

One-time passwords

Enables one-time passwords by setting a key. Delete the key to disable one-time passwords.



SX-GATE uses time-based one-time passwords (TOTP) with 6 digits, valid for 30 seconds and calculated with SHA1.

Fixed password for system-admin

Set or clear a fixed password for access of the selected user to SX-GATE's administration GUI.

Fixed password for system-mail

This function allows you to set or clear a fixed mail password for the selected user. This password is required to access the POP3, IMAP4 and groupware server on SX-GATE. Also SX-GATE's mail relay server uses this password for SMTP-Auth.



Use this feature if the user is not able to specify the password to access his mailbox. This is the case if e.g. a central mail server polls for the users' mails.

Fixed Password for system-proxy

This function allows you to set or clear a fixed proxy password for the selected user.

Fixed password for system-ras

Set or clear a fixed RAS password for the selected user.

12.3.2-C Mail administration

Mail aliases

The email address of a user corresponds to the login name. To map an additional email address to a user you can insert the respective local part of the address here. The local part of an email address is the part before the "@" character. If for instance the login of a user is "brown", the email address "brown@example.com" corresponds to the user automatically. To map the address "charly.brown@example.com" to the same user, you have to add the alias "charly.brown".



If the same alias was added to multiple users they will all receive a copy of mails addressed to this alias. When adding the name of a SX-GATE group as a user's alias, emails to the group will also be delivered to the user. In theory aliases can be used to implement a distribution list. However you should use aliases only for personal email addresses of a user. Otherwise the configuration might become confusing. Use groups to setup distribution lists or mail addresses associated with a certain role like e.g. "sales" or "concierge".

S/MIME keys

If SX-GATE acts as an email encryption gateway you can select the S/MIME keys of the respective local users here. The keys are managed in menu "System > Certificate manager > Keyring".



Please see the note below regarding certificate expiry.

This is the preferred configuration when users submit mails directly to SX-GATE and are able to authenticate themselves.



If users submit outbound mails to an internal mailserver, the certificates are usually configured independent of users in menu "Modules > Mail Server > S/MIME gateway".

Outbound emails will be signed if the sender address (according to From or Sender header) matches the email address of the certificate and if the email isn't already signed or encrypted. To be able to use one of the certificates in this list, the sender additionally has to authenticate himself (SMTP auth).

An encrypted email will be decrypted automatically if SX-GATE has the required key and the email recipient matches the email address of the certificate. The decryption process is not related to user accounts in any way. Strictly speaking it doesn't even matter to which user account a key has been uploaded. Just the recipient addresses according the SMTP protocol are considered.



After removing a key from the list SX-GATE is no longer able to decrypt emails encrypted with this key. These emails will be delivered encrypted. If the key has already been destroyed everywhere it is no longer possible to decrypt the mail.

In the transitional period after a certificate has been re-newed you will continue to receive mails encrypted with the old key for quite a while. This can even happen after the old certificate has expired. This is how SX-GATE supports you in the transition phase: When replacing a key-pair in menu "System > Certificate manager > Keyring" the previous key-pair will be kept. The S/MIME gateway will continue to use the it for decrypting inbound mails while the new key-pair is used for both, decrypting and signing mails. So if a certificate is about to expire, please re-new it within the existing entry in the "Keyring" menu. Do not add a new entry. It is not necessary to modify the S/MIME gateway configuration.



Only the previous key-pair is kept, not multiple generations of it.

12.3.2-D Mail forwarding

The settings on this screen can also be modified by the user himself at "My Account > Email options". The user has to be member of group "system-admin" to be able to access this menu.

Forward email to

With this control you can forward the emails of the selected user to other internal or external addresses. Any number of recipients can be entered. They will all receive a copy of the respective emails.

User keeps copy of forwarded emails

With this option you can control if a copy of each mail will be delivered to the user's mailbox even when forwarding mails to other addresses. If the option is not checked, the mailbox will not receive emails any longer.



If forwarding is not active, this option is without effect.

12.3.2-E SPAM filter

The settings on this screen can also be modified by the user himself at "My Account > Email options". The user has to be member of group "system-admin" to be able to access this menu.

If you enable at least one of the thresholds, every incoming mail has to pass a SPAM mail filter before it is delivered to the mailbox of the selected user. A SPAM mail is an unsolicited email, usually with dubious origin.

The SPAM mail filter of SX-GATE classifies emails by identifying typical phrases and other attributes indicating an unsolicited email. SX-GATE contains a database of checks to perform and all matches result in a score which in turn allows filtering emails. Characteristics indicating a SPAM mail will add a value to the score while other characteristics indicating that it's not a SPAM mail will subtract a certain value. The higher the final score, the more likely it's a SPAM mail.



Emails exceeding the size of 1MB will not be classified to save system resources. However this is not a drawback, as a SPAM mail is usually very small.

A few headers will be added to each email examined by the SPAM mail filter. The header "X-Spam-Status" shows the final score (hits=...) and give the name of the matches (tests=...). This allows the recipient of the mail to check the score of any mail. The header "X-Spam-Level" will contain one "x" per scored point (e.g. "X-Spam-Level: xxx" for a score between 3.0 and 3.99). This header allows automatic sorting in the user's mail client.



Most mail clients will display only the most important headers by default. Usually the full header information is available after selecting a specific menu option.

Tag an email as SPAM when it is scored more than

If the score exceeds the threshold for tagging an email as SPAM, the subject of the mail is prefixed by the text "***** SPAM *****" and the SPAM score.

Deliver tagged emails to

As an option SX-GATE can deliver tagged SPAM mails into a separate SPAM folder. This folder is accessible with SX-GATE's groupware or via IMAP (folder Mail/SPAM). A POP3 client will not be able to open the SPAM folder.

Delete SPAM/HAM after

Mails from the "SPAM" and "HAM" folders are automatically deleted after the given number of days.



This feature does not depend on the previous option. Mails will also be deleted if you create and fill the SPAM folder yourself instead of having tagged mails automatically delivered to the SPAM folder.

Silently discard a mail when it is scored more than

Exceeding this threshold, an email will be silently discarded. There will be no notification and it is not possible to undelete the email. The email is lost irrecoverable! If you want to make sure that no requested email gets lost, you should not enable this option. Activate the threshold "Tag an email as SPAM when it is scored more than" instead and make use of the features offered by your mail program to sort emails based on header lines.



To avoid loss of important emails you should be very carefully when activating this option. You should select a value which is rather to high than to low. Please note that automatically deleting email may be subject to legal constraints or might even be prohibited by law.

12.3.2-F SPAM scores

The settings on this screen can also be modified by the user himself at "My Account > Email options". The user has to be member of group "system-admin" to be able to access this menu.

Userdefined SPAM checks

This control allows you to extend the SPAM checks by self-defined rules. First you have to decide to which part of the mail a new rule applies. If the specified pattern is found in a mail, the selected score is accounted.

The following types of SPAM filter rules are available:

Subject

The pattern is looked up in the email's subject.

Sender

This will check the sender of the mail (From header).

Recipient

Use this option to match the recipient (To header).

Message header

Allows you to examine an arbitrary mail header.

Message text

The actual text contents of the email, including the subject, are analyzed when selecting this value.

Raw HTML text

Just like the previous option, but including HTML tags of HTML emails.

Web links

Checks web links (either plain text or HTML links) found in the subject or the message body.

Rule

This setting differs from the previous ones. It allows you to modify the score of SX-GATE's builtin rules. Accordingly you don't specify a search pattern here. Instead you have to supply the internal ID of the rule. The ID together with the original score is listed in the content analysis of mails, that have been marked as SPAM (e.g. "HTML_MESSAGE" or "FORGED_MUA_OUTLOOK").



When the builtin rulesets are updated, internal ID's may change without notice. The rules defined here will not be adjusted.

Search patterns ("matches") are case-insensitive. If the pattern starts/ends with a letter or a digit, the pattern matches only if the pattern is found at the beginning/end of a word. So e.g. the pattern "pace" won't match "spaces" but will match "Learn at your own pace!".

Some characters have a special meaning:

* (Asterisk)

It represents a sequence of arbitrary characters. The sequence may also be missing. As searching for such a sequence of any length is rather time-consuming, an asterisk matches no more than 30 characters. The pattern "a*d" will match e.g. "ad", "a_d" and "abcd". The asterisk helps you to find patterns within words. So e.g. the pattern "*pace*" will match "spaces".

? (Question mark)

Any single character is matched by a question mark. If for instance "a?d" is looked up, "a_d" is a hit. In contrast "ad" and "abcd" do not apply.

_ (Underscore)

An underscore matches any amount of whitespace characters, i.e. spaces, tabs and new-lines. As an example, "a_d" will match "a d", but not "ad" or "a_d".

Please keep an eye on the configured thresholds when selecting the score for a new rule. For a rule which refers to SPAM mails you have to select a positive value. Negative numbers reduce the probability of matching emails to be classified as SPAM.

English language indicates potential SPAM

The majority of SPAM mails is written in English language. Activate this switch to add some points to the SPAM score of every English email. This will result in a significant increase of the probability that the score of English mails will exceed the configured SPAM filter thresholds.

12.3.2-G SPAM lists

SPAM filter whitelist

If an email was identified as SPAM by mistake, you can add the sender to this list. The SPAM filter will subtract 100 points from the SPAM score of a mail, if the sender is found in this list. Thus all future emails of senders listed here will never be recognised as SPAM.



The menu "Modules > Mail Server > SPAM/Virus/Malware" allows you to define a whitelist which applies to all users.

You can add a complete email address (e.g. user@example.com) to prevent filtering emails from this specific address. If you want to allow every email from a specific domain to pass, add only the domain part of the address (e.g. example.com).

SPAM filter blacklist

If a user receives SPAM mails from the same sender again and again and the SPAM mail filter does not identify these emails as SPAM, you should add the sender to this list. The SPAM filter will add 100 points to the SPAM score of a mail, if the sender is found in this list. Thus all future emails of senders listed here will always be recognised as SPAM.



The menu "Modules > Mail Server > SMTP settings" allows you to block incoming mails from certain sources for all users.

You can add a complete email address (e.g. user@example.com) to intercept emails from this specific address. If you want to classify every email from a specific domain regardless of the actual sender, add only the domain part of the address (e.g. example.com).

12.3.2-H Vacation

On this tab you can configure autoresponses and schedule a forwarding rule for the user's mails.

The selected actions will apply to every email delivered to the user's mailbox. In particular this affects also emails not addressed to the user personally but to a distribution list (group) the user is member of.



When emails are forwarded to other addresses (see tab "Mail forwarding"), the settings will apply only if the option ""User keeps copy of forwarded emails" has been selected.

The settings on this screen can also be modified by the user himself at "My Account > Email options". The user has to be member of group "system-admin" to be able to access this menu.

Vacation settings

Choose from the list of actions taken for each mail.

Start date

Either schedule a date to enable the vacation feature or enable it immediately. Please use date format YYYY-MM-DD HH:MM.

End date

You may also enter a date the vacation feature is expected to stop working. Please use date format YYYY-MM-DD HH:MM.

Forward email to

You can forward emails to a different recipient during the configured period of time.

Keep copy of forwarded emails

When enabled, the user will still receive a copy of each mail even when forwarding to a different address.

Vacation message

It is possible to generate an automatic reply to incoming mails. Typically it is used for a vacation autoreply. However you could also use this feature to automatically confirm email delivery.



Option "User's primary mail address" on tab "User details" let's you determine the autoreply's sender address.



No reply will be generated for emails which have been tagged as SPAM.

Please fill in the text message to be sent. If there's no text, no reply will be sent.

12.3.2-I Mail folders

It is possible to automatically distribute mails into different subfolders of the user's mailbox. Access to these folders requires IMAP or groupware. POP3 does not support folders.

12.3.2-J SOCKS proxy

To provide internet access to applications, that are not able to use other proxies or firewall NAT rules, you can use the generic SOCKS-proxy. Supported protocols are SOCKS4 and SOCKS5. With the help of a SOCKS wrapper application nearly every networking application should be able to use the SOCKS proxy. Some programs even provide builtin SOCKS support.



For protocols like e.g. HTTP, HTTPS and FTP SX-GATE offers dedicated proxy services. SOCKS should not be used for these protocols. Specialized proxies provide more features and better protocol support than a generic proxy.



Data transmitted via the SOCKS proxy is not checked by any virus scanner. Also the integrity of the transported protocol is not verified.

By default the SOCKS proxy denies any connection request. Rules have to be added to grant access. Rules configured in menu "Modules > More Proxies > SOCKS proxy" apply to every SOCKS enabled application without further restrictions. The rules configured on this screen will apply to the respective user only. Authentication with username and password is required.



From the conceptual point of view, per-user SOCKS rules implement "user specific firewall rules".

Per-user rules

The rules configured here indicate which connections the selected user may establish after successful authentication.

First select the desired protocol. Specify a single IP address or a network address with its corresponding netmask if you want to restrict the acceptable source or destination IPs.



Protocols are defined in menu "Definitions > Protocols".



Non UDP and TCP protocol signatures will be ignored.

12.3.2-K RDP Web Client

The HTML5 based RDP Web Client allows access to Windows computers via any HTML5 capable browser. No special software or plugin is required on the client.



Connections to the Web Client are established via SX-GATE's reverse proxy, which must be configured accordingly. Use the URL path "/webclient" (e.g. <https://SX-GATE/webclient>).



Any configuration changes will become effective when the user opens a new connection to the Web Client. It is not sufficient to open a new RDP session.

These settings are only available if the Web Client App is installed and the user is a member of group "system-ras".

Colour depth

Here you enter the used colour depth in bits per pixel. A lower value will reduce the amount of data transmitted.

Resize method

The method to use to update the RDP server when the width or height of the client display changes. If set to None, no action will be taken when the client display changes size.

Uses the "Display Update" channel added with RDP 8.1 to signal the server when the client display size has changed.

When set to Reconnect automatically disconnects the RDP session when the client display size has changed, and reconnects with the new size.

Clipboard

With this option you can control the behaviour of the Web Client clipboard.



This option requires at least version 1.2.0-1 of the Web Client.

File transfer

If the "File transfer" is active, a SX-GATE directory is made available in the RDP session, which allows data exchange between RDP server and browser in both directions. On the server the directory becomes available as a network folder. On the browser side you can access the SX-GATE directory through the Web Client menu bar.



You can display and hide the Web Client menu bar with the key combination "Ctrl-Alt-Shift".



The options "download only" and "upload only" requires at least version 1.2.0-1 of the Web Client.

Printing

When you enable "Printing", a virtual printer is made available in the RDP session which can be used to transfer documents to the client. Unfortunately web browsers don't allow printing directly, so printouts are actually provided as PDF files. Let the browser display the document to print it or save the document for printing it later.

Microphone

If the Browser has access to a microphone, this switch enables a channel for audio input.



This option requires at least version 1.1.0-2 of the Web Client.

Client name

The RDP server make this name available in the environment variable CLIENTNAME.

RDP connections

Configure the available RDP connections for the user here. The following parameters are available:

Active

Allows you to temporarily disable a connection. Any established connections will not be disconnected.

Servename, IP or host object (WoL)

Determines the destination machine. When configuring a DNS name, please make sure that SX-GATE is able to resolve it. For internal DNS names it may be necessary to configure a forwarding zone in the DNS settings.



Select an IP object of type "Host" which has a MAC address an an IPv4 address configured and you will be able to power on the device with Wake-on-LAN. You can add these objects in menu "Definitions > IP objects".

Port

The port is usually 3389.

Domain (optional)

If you enter the Windows domain here, it will be pre-selected in the RDP server's login screen.

Username (optional)

If you enter the Windows username here, it will be pre-selected in the RDP server's login screen.

Password

The RDP server password usually has to be entered by the user. If the passwords on SX-GATE and on the RDP server are equal, you can select the option "pass-through".

The password the user entered to access the SX-GATE Web Client is then passed through to the RDP server.

Security

The security mode for the connection between SX-GATE and RDP server depends on the server configuration.

Specified by the server

The best security level that the server specifies is selected.

Standard encryption

In this mode RDP will encrypt the payloads only.

TLS encryption

In this mode the connection is TLS encrypted from the beginning.

NLA + TLS encryption

Select this option if the server requires Network Level Authentication (NLA). In this mode a prompt for username and password will appear before opening the connection. The actual RDP session will start after successful authentication. The connection is also TLS encrypted.

Keyboard layout

Please select the keyboard layout configured on the Windows system if you encounter problems with swapped keys while typing. Problems usually occur on Windows clients systems only. Server systems usually support different layouts and adapt to the client automatically.

Font Smoothing

If enabled text will be rendered with smooth edges. Text over RDP is rendered with rough edges by default, as this reduces the number of colors used by text, and thus reduces the bandwidth required for the connection.

Terminal server console

This option is only required for administrators when accessing a terminal server. It will connect with the terminal server administration instead of opening a normal terminal server session.

Comment or Display name

The comment is displayed in the Web Client administration to make it easier for the user to pick the right connection. If no comment has been entered, the server address and port and, if available, the username are displayed.

12.3.2-L VNC Web Client

The HTML5 based VNC Web Client allows access to vnc servers via any HTML5 capable browser. No special software or plugin is required on the client.



Connections to the Web Client are established via SX-GATE's reverse proxy, which must be configured accordingly. Use the URL path "/webclient" (e.g. <https://SX-GATE/webclient>).



Any configuration changes will become effective when the user opens a new connection to the Web Client. It is not sufficient to open a new VNC session.

These settings are only available if the Web Client App is installed and the user is a member of group "system-ras".

Colour depth

Here you enter the used colour depth in bits per pixel. A lower value will reduce the amount of data transmitted.

Clipboard

With this option you can control the behaviour of the Web Client clipboard.



This option requires at least version 1.2.0-1 of the Web Client.

VNC connections

Configure the available VNC connections for the user here. The following parameters are available:

Active

Allows you to temporarily disable a connection. Any established connections will not be disconnected.

Servername, IP or host object (WoL)

Determines the destination machine. When configuring a DNS name, please make sure that SX-GATE is able to resolve it. For internal DNS names it may be necessary to configure a forwarding zone in the DNS settings.



Select an IP object of type "Host" which has a MAC address and an IPv4 address configured and you will be able to power on the device with Wake-on-LAN. You can add these objects in menu "Definitions > IP objects".

Port

The port is usually 5900.

Password

Select "ask" if the VNC server is password protected. The user is then asked to enter the password when trying to connect with the VNC server. If the passwords on SX-GATE and on the VNC server are equal, you can select the option "pass-through". The password the user entered to access the SX-GATE Web Client is then passed through to the VNC server.

Remote cursor

Enable this option if you see no mouse pointer. Usually the client takes care of the cursor. However if this isn't supported by the VNC server, the server must render the mouse pointer. The mouse will react slower then.

Swap red blue

Enable if the colours red and blue are swapped. Some VLC server transmit image data incorrectly.

Read-only

If set, no input will be accepted on the connection at all. Users will only see the desktop and whatever other users using that same desktop are doing.

Comment or Display name

The comment is displayed in the Web Client administration to make it easier for the user to pick the right connection. If no comment has been entered, the server address and port are displayed.

12.3.2-M SSH Web Client

The HTML5 based SSH Web Client allows access to vnc servers via any HTML5 capable browser. No special software or plugin is required on the client.



Connections to the Web Client are established via SX-GATE's reverse proxy, which must be configured accordingly. Use the URL path "/webclient" (e.g. <https://SX-GATE/webclient>).



Any configuration changes will become effective when the user opens a new connection to the Web Client. It is not sufficient to open a new SSH session.

These settings are only available if the Web Client App is installed and the user is a member of group "system-ras".

Color scheme

Here you specify the desired color scheme of the SSH console.

Font name

Select the desired font of the SSH console.

Font size

Here you can determine which font size should be used in the SSH console.

SSH connections

Configure the available SSH connections for the user here. The following parameters are available:

Active

Allows you to temporarily disable a connection. Any established connections will not be disconnected.

Servername, IP or host object (WoL)

Determines the destination machine. When configuring a DNS name, please make sure that SX-GATE is able to resolve it. For internal DNS names it may be necessary to configure a forwarding zone in the DNS settings.



Select an IP object of type "Host" which has a MAC address and an IPv4 address configured and you will be able to power on the device with Wake-on-LAN. You can add these objects in menu "Definitions > IP objects".

Port

The port is usually 22.

Username (optional)

Here you can specify the user name to be used for logging on to the SSH server. If the user name is not specified, the user will be prompted while connecting.

Password

The SSH server password usually has to be entered by the user. If the passwords on SX-GATE and on the SSH server are equal, you can select the option "pass-through". The password the user entered to access the SX-GATE Web Client is then passed through to the SSH server.

Comment or Display name

The comment is displayed in the Web Client administration to make it easier for the user to pick the right connection. If no comment has been entered, the server address and port and, if available, the username are displayed.

12.3.2-N SSH TCP forwarding

Secure-shell clients can establish authenticated and encrypted channels, carrying TCP connections to (usually internal) servers. From the technical point of view an SSH forwarding is situated somewhere between simple DNAT and VPN. In contrast to DNAT the connection is secured with authentication and encryption. Compared to VPN, the SSH tunnel lacks among others transparency in respect of the client application, only unidirectional TCP connections are supported and inexperienced users might be fooled easier by man-in-the-middle attacks. In return an SSH forwarding is easier to configure and maintain.

The corresponding SX-GATE SSH server is available on port 2222. A separate firewall rule might be necessary for the remote access over the internet. Use the predefined protocol "SSH-FWD".



Using firewall DNAT rules it is possible to make the server appear on a different port. You could e.g. redirect HTTPS port 443 to 2222 to make it easier for SSH client to pass firewalls and proxies.

Public SSH key (ed25519 or RSA)

Please enter the client's public SSH key. The key starts with either "ssh-rsa" or "ssh-ed25519", followed by one space character and at least 68 letters, digits, slashes, plus and equal signs in a single long row. Space characters or newlines are not allowed

in there. An optional space character and comment may be appended. Extremely shortened example of a key: "ssh-rsa AA3x/5+eW48oPvX= Comment".

Permitted connections

The SSH client may connect only to addresses and ports from this list.



For technical reasons protocol signatures with a port range as destination port will be ignored. This limitation may be dropped in future SX-GATE releases.

12.3.2-O RAS settings

These settings are available for members of group "system-ras" only. The settings apply to remote access using IPsec VPNs.

Send WoL upon dial-in to Mac address

If you enter the hardware address of some computers network card here, SX-GATE will send a Wake-on-LAN packet to it when the user logs in. This works for IPsec-L2TP connections and for OpenVPN if user authentication is enabled.

The expected format is "XX:XX:XX:XX:XX:XX". Each "X" must be a digit or a letter from "A" to "F". The delimiters may be colons, dots, hyphens or underscores.

Assigned IP address

All of SX-GATE's RAS services which require the client to authenticate will assign an IP address to the client. You can select among two options. Either an interface specific but user independent IP is assigned or a user will be assigned his own dedicated IP address.



If you assign an unallocated LAN IP to the RAS client, SX-GATE will setup a proxyarp entry for its address. No routing entries will be necessary on the LAN machines in this case in order to communicate with the RAS client.



IP addresses always have to be unique. Therefore no intersections between interface specific IPs, individual IPs and elsewhere used IPs may occur. In case of intersections the connectivity of the affected systems is no longer guaranteed.

The following RAS services support userspecific RAS IPs:

- L2TP/IPSec VPN (l2tp0)
- IPSec VPN with XAUTH

IP address of RAS interface

With this option, the IP address configured in the actual RAS interface will be assigned to the user.

personal IP

Select this option to assign a dedicated RAS IP to this user when connecting to one of SX-GATE's RAS services. This allows you to configure an individual firewall policy for the RAS users.

You will be able to configure per RAS service if the user is allowed to use it and which IP is assigned. Usually the same IP is used for all of the allowed services, however it is also possible to assign different IPs. The IP address which has been configured in the corresponding RAS interfaces will be ignored for this user.

L2TP/IPSec VPN

Use this control to determine if the currently selected user is accepted by SX-GATE's L2TP server and which IP is assigned.



The maximum number of concurrent L2TP connections results from the number of IP addresses configured below "Modules > Network > l2tp0". This limit is not affected by the configuration of userspecific IPs. Even if only userspecific IP addresses should be used, it is necessary to supply enough IPs in the L2TP interface configuration.

XAuth/IPSec VPN

Use this control to determine if the currently selected user is accepted by SX-GATE's XAuth/IPsec server and which IP is assigned.

12.3.2-P Docklets

Activate the switches below to grant access to the various status and information windows usually displayed on the homepage.



These settings are only available for members of group "system-mail".

12.3.2-Q Menu Statistics

Activate the switches below to grant access to the corresponding item from the "Statistics" menu.



These settings are only available for members of group "system-mail".

12.3.2-R Menu Monitoring

Activate the switches below to grant access to the corresponding item from the "Monitoring" menu.



These settings are only available for members of group "system-mail".

12.3.2-S Menu Definitions

Activate the switches below to grant access to the corresponding item from the "Definitions" menu.



These settings are only available for members of group "system-mail".

12.3.2-T Menu System

Activate the switches below to grant access to the corresponding item from the "System" menu.



These settings are only available for members of group "system-mail".

12.3.2-U Menu Wizards

Activate the switches below to grant access to the corresponding item from the "Wizards" menu.



These settings are only available for members of group "system-mail".

12.3.2-V Menu Modules

Activate the switches below to grant access to the corresponding item from the "Modules" menu.



These settings are only available for members of group "system-mail".

12.3.2-W Login options

Message after logging in

After this user logged in this message will be shown until the user closes it.

12.3.2-X User details

The values on this tab are mostly exploratory. For users with a local mailbox (members of group "system-mail") the details will be available as address book in SX-GATE's groupware.

User's primary mail address

Specify the user's main address. It's used as the sender address when SX-GATE generates an email on behalf of the user (autoresponse feature).

12.3.3 Groups

A mail distributor is automatically created for each group by the same name. Therefore you can for example set up a group "info". All members of this group will then receive a copy of emails addressed to this group. Users who are not member of the "system-

mail" group and thus have no local mailbox will be ignored however. Further external mail recipients can also be added to any of the groups.

If the URL filter option of the web proxy is enabled, URL filter lists can be associated with groups to allow for individual settings per user group.

A table gives you an overview of the available objects. If multiple columns are displayed you can change the sort order by clicking the column title. If there are more than 20 entries, a navigation bar will appear below the bottom right hand corner of the table. You can switch between a grouped view or a pager. The full screen mode allows you to see all entries at the same time. Pick an entry by clicking its title in the left column. A pencil icon or a trashcan in the right column allow you to rename or delete an entry. Add new objects by clicking "New Entry" below the table on the left.

Name of group

Determine the name of the new group here.



Besides small letters and digits only dashes (-), dots (.) and underscores (_) are allowed in group names. The name must begin with a letter. Particularly space characters are not allowed.

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

12.3.3-A Users.....	151
12.3.3-B Mail settings.....	152
12.3.3-C Usage.....	153

12.3.3-A Users

Users

In this input section you can see all users that have already been assigned to the selected group and all those who have not yet been assigned. To add or remove several users at a time you can select multiple entries from the respective list. Hold down the CTRL key while selecting a user to accomplish this.



The user "admin" will not be listed in groups "system-mail" and "system-admin" as this user is always member of these groups.

12.3.3-B Mail settings

Relay mails when authenticated (SMTP Auth)

SX-GATE's mail server can be configured to relay mails to external recipients only for authenticated users. Use this switch to select the users which should be allowed to relay mails into the Internet after successful authentication. All users who are member of at least one group with this option enabled will be allowed for authenticated relaying.



Only members of group "system-mail" actually have the necessary account to log in.

By default authentication is disabled in the mail server configuration. Every client connecting from an internal IP address is allowed to send emails to external recipients without authentication, while relaying for external senders to external recipients is always denied. In menu "Modules > Mail Server > SMTP settings" you will find two options to enable authentication on tab "Relay control". Enable "SMTP-Auth required for local users" if not every local client should be allowed to send emails into the Internet, just specific users after authentication. Enable "Always propose SMTP-Auth" to allow authentication for some external clients, so e.g. mobile workers can use SX-GATE as relay server.

Mail group feature

Based on the information which users are members of this group (as configured on tab "Users"), SX-GATE can automatically create a mail group. It only contains those users who are also member of group "system-mail", i.e. have a local mail account.



Whenever a member is added or removed from group "system-mail" or when a user is deleted completely, this will be reflected automatically by the mail group.

The group name determines the email address of the group. If the local domain is "example.com", you can address the group "group" with "group@example.com".

Please select which type of mail group you want to get.

none

No email address is associated with this group.

Distribution list

Each group member and each external mail address receives a copy of emails delivered to this group.

IMAP folder

An IMAP folder is associated with this group which all group members can access. An email delivered to the group will be placed in this folder. If there are entries in "External mail addresses", each address will receive a copy of the mail.

External mail addresses

This control allows you to add also external mail addresses or local groups to the mail distributor.



An email address which refers to a local user or group will not be removed automatically when the corresponding user or group is deleted.

12.3.3-C Usage

This table show in which settings the definition is used.

12.4 Certificate manager

12.4.1 CA certificates

You can maintain the list of CA certificates known to SX-GATE in this menu. This includes SX-GATE's own CA, which allows you to issue certificates yourself. But you can also upload CA certificates for verification purposes.

A table gives you an overview of the available objects. If multiple columns are displayed you can change the sort order by clicking the column title. If there are more than 20 entries, a navigation bar will appear below the bottom right hand corner of the table. You can switch between a grouped view or a pager. The full screen mode allows you to see all entries at the same time. Pick an entry by clicking its title in the left column. A pencil icon or a trashcan in the right column allow you to rename or delete an entry. Add new objects by clicking "New Entry" below the table on the left.

Name

Here you have to specify a name for the CA or the CA bundle. It is only used to identify the entry, so you can choose any appropriate name.

12.4.1.1 SX-GATE CA

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

12.4.1.1-A CA certificate.....	154
12.4.1.1-B CA revocation list.....	156
12.4.1.1-C SSL proxy CA.....	157

Working with certificates in a closed group of users usually does not require certificates issued by an official certification authority (CA). While an official CA will charge for a certificate, you can create certificates for free with SX-GATE.

12.4.1.1-A CA certificate

On this screen you can administrate the root certificate, which is sometimes also referred to as "CA certificate".



There's no pre-installed default CA certificate. On a new SX-GATE you have to create one first.

The CA certificate is used to sign all certificates issued by SX-GATE. As it is the root of the certificate trust chain any certificate based authentication relies on it. Therefore the CA certificate is protected by a password which has to be entered for any operation which involves the CA certificate.



For security reasons the CA certificate is not saved along with the SX-GATE backup. Use the export function on this screen to download and save a password protected copy.

Export public key

Here you can download the CA certificate's public key. Any applications using a CA certificate based authentication need to know it.



SX-GATE will include the CA's public key with every issued certificate, so if a client receives a certificate issued by SX-GATE, there's usually no need to forward the CA certificate separately.

Create a new or import a CA certificate

This feature allows you to create a CA certificate on a new SX-GATE. You can also restore the CA certificate from a backup file here.



A CA certificate which was created by SX-GATE will be valid for 20 years. Generally it does not make sense to issue a new certificate long before the old one expires. Except of course the privacy of the certificate can no longer be guaranteed.

Create a new CA certificate

This feature allows you to create a CA certificate on a new SX-GATE.



A CA certificate which was created by SX-GATE will be valid for 20 years. Generally it does not make sense to issue a new certificate long before the old one expires. Except of course the privacy of the certificate can no longer be guaranteed.

Backup CA key-pair

The key pair of the SX-GATE CA can be exported in PKCS#12 format to save a backup. Please note that this export also contains the private key which must remain completely secret.

Delete CA private key

To improve the security of the SX-GATE CA, you can erase the private key of the root certificate. You should do so if you don't need to issue new certificates in the near futures.



Of course you have to backup the CA certificate before deleting its private key. Use the export function to create the backup. You should store it on a reliable medium in a safe place. Reinstall the private key with the import feature as soon as you need to use the CA again.

12.4.1.1-B CA revocation list

If applications rely on the certificate trust chain for authentication you might have to face the problem, that a certain certificate must no longer be accepted, although it didn't expire yet. A typical example is the certificate of an employee who leaves the company or the certificate which is installed on a stolen notebook. A certification authority (CA) can publish a certificate revocation list (CRL) to invalidate certificates ahead of time.



The CRL has to be installed on every system which could be a potential target of an unauthorised connection authenticated with a revoked certificate.

Configure CRL distribution point

When issuing a new certificate a URL can be included which will always serve an up-to-date copy of the current CRL. So a system which is trying to verify the certificate can access the current CRL itself.



When a new CRL has been issued, you must not forget to copy it to the server.

Export certificate revocation list

You can download the CRL in PEM format [here](#).

Create a new certificate revocation list

Every time you revoke a new certificate, you have to generate a new CRL [here](#).



The CRL has to be signed by the CA with the root certificate.



Don't forget to install the new revocation list on all relevant systems. At the end of the CRL update process you can continue installing the new CRL in SX-GATE's VPN server. Updating the VPN server CRL is also possible in menu "Modules > Network > Settings".

Copy local CA revocation list to VPN server

If SX-GATE's VPN server uses certificates issued by its own CA, you can transfer the current certificate revocation list (CRL) into the VPN server [here](#). A CRL offers the possibility to invalidate a certificate before it expires. This is useful if for example an employee leaves the company and VPN access has to be denied.

12.4.1.1-C SSL proxy CA

The SSL interceptor feature of SX-GATE's web proxy allows virusscanning of encrypted connections by breaking them open. Instead of delivering the original web server certificate, a locally generated certificate with the same contents is presented to the client. These proxy certificates need to be signed by a dedicated certificate authority (CA) which can be created [here](#).



For security reasons the CA certificate is not saved along with the SX-GATE backup. Use the export function on this screen to download and save a password protected copy.

Export public key

Here you can download the CA certificate's public key. It should be installed in all browser clients.

Backup proxy key-pair

The key pair of SX-GATE's proxy CA can be exported in PKCS#12 format to save a backup. Please note that this export also contains the private key which must remain completely secret.

Create a new or import a proxy certificate

This feature allows you to create a new proxy CA certificate or you can restore the CA certificate from a backup file.



A CA certificate which was created by SX-GATE will be valid for 20 years. Generally it does not make sense to issue a new certificate long before the old one expires. Except of course the privacy of the certificate can no longer be guaranteed.

12.4.1.2 SX-GATE CA - Certificates

In this area you can issue certificates which will be signed with the root certificate of SX-GATE's built-in certification authority (CA). Instead of buying certificates issued by a commercial CA, using the SX-GATE CA is sufficient for certificates used by closed user groups.

In the first place, the SX-GATE CA is used to issue certificates for VPN. The VPN server of SX-GATE requires a certificate of its own, too. Select the predefined entry "VPN" to issue the certificate for SX-GATE's VPN server.

A table gives you an overview of the available objects. If multiple columns are displayed you can change the sort order by clicking the column title. If there are more than 20 entries, a navigation bar will appear below the bottom right hand corner of the table. You can switch between a grouped view or a pager. The full screen mode allows you to see all entries at the same time. Pick an entry by clicking its title in the left column. A pencil icon or a trashcan in the right column allow you to rename or delete an entry. Add new objects by clicking "New Entry" below the table on the left.

Name of certificate

Here you have to specify a name for the certificate. It is only used to identify the certificate, so you can choose any appropriate name.

Export certificate

You can download the certificate here. The certificate is the CA signed public key. The file format is PEM.



The private key is not stored on SX-GATE.

Revoked on

Shows date and time when the certificate was marked for inclusion in the certificate revocation list (CRL) of SX-GATE's CA.



The certificate is not invalidated just by the fact that some point in time was entered here. First you have to generate a new CRL using the corresponding CA function and then the new CRL has to be installed in all relevant applications.

Revoke certificate

When authenticating with certificates an application often verifies the trust chain only. If a certificate has been signed by a trusted certification authority (CA), the authentication will succeed if the certificate is not expired. It can however be necessary to invalidate a certificate ahead of time, e.g. when an employee leaves the company or a notebook with such a certificate has been stolen.



To create a complete CRL, certificates must not be deleted before the original expiration date has been reached.

Undo revocation

A revoked certificate can be re-activated. Remember to generate and distribute a new CRL after unlocking the certificate.

Issue new certificate

With this function you can issue or renew the certificate. The new certificate will be signed by the SX-GATE CA and is valid for one year.



You should renew a certificate only right before it expires. Otherwise it will not be possible to include the old certificate in the certificate revocation list.

Issue certificate

On this screen you have to enter the certificate subject.

CN

If this certificate is to be used by a server program, you should enter the DNS name or the Internet IP address of the system. You can also issue a wildcard certificate (e.g. *.example.com). For a user certificate you might want to enter the name or email address.

Subject alternative names

Most clients prefer this certificate property while verifying that the server certificate belongs to the expected server. Enter all required names and IPs used to address the server. You can also issue a wildcard certificate (e.g. *.example.com). For a user certificate you should enter the email address.

Enter password

A private key which has to remain secret will also be part of the new certificate. To guarantee the privacy of the certificate while it is forwarded to the intended user, the PKCS#12 file is protected with a password. Forward PKCS#12 file and password separately. The password should be transmitted using a secure channel.

Certificate request

Entering this screen, a certificate request will be generated on SX-GATE. You can sign it now with the CA certificate.

Extended Key Usage: server authentication

Enable this option if the certificate is used by a server (e.g. web or VPN server).



Depending on the client and its configuration, a client may refuse to connect if the server certificate does not include this attribute.

Extended Key Usage: client authentication

Enable this option if the certificate is used by a client (e.g. web browser or VPN client). This may keep other clients from connecting, if this certificate is misused as a server certificate.

Extended Key Usage: email protection (S/MIME)

Enable this option for a user certificate, which is used for S/MIME signing and end-to-end encryption of emails.

Signing certificate

Entering this screen, the certificate will be signed and can be downloaded.

Create setup package***Windows IPsec-L2TP parameters******Internet IP or servername of SX-GATE***

Please enter the DNS name or IP address the client will use to connect with SX-GATE.

Allow direct Internet access

If this option is disabled, there will be no direct Internet access for the client as soon as the VPN connection is established. The client sets its default gateway to the VPN tunnel. So any access to the Internet is routed via VPN and so via SX-GATE's firewall and proxies. When the client disconnects, its default gateway is reset to the original value, restoring direct internet access.

Enable this option and the client keeps its direct Internet connection. Only the relevant IP addresses will be routed via VPN.

Allow direct Internet access

- No

Please read on at [Windows IPsec-L2TP setup](#) (p. 162)

VPN server behind nat router

If this option is set, the required Windows registry key will be set automatically when the connection is created.

Connection-specific DNS suffix

You can optionally assign a connection-specific DNS suffix to the Windows client. So the Windows client can e.g. resolve hosts on the LAN using their plain hostname.

Windows IPsec-L2TP routes***Additional routes (powershell only)***

Here you can specify additional local networks to be routed via the VPN connection. To route a connection to a single host you have to supply its IP.



The routes are set only with the Powershell installation package. With the deprecated CMAK installation package, the routes are not taken into account.

Windows IPSec-L2TP setup

Setup package for Windows IPSec-L2TP (Powershell)

Click this button to download a self-extracting ZIP archive for Windows. In addition to the PKCS#12 file which contains certificates and the private key, the archive includes a powershell script to create the connection in Windows.

Double-clicking the archive in Windows, it will extract itself and starts automatically the installation dialog.



For the connection the secure algorithms AES256-SHA256-DH20 will be used as IKEv1 IKE proposals (phase 1) and AES256-SHA256 as IKEv1 ESP proposals (Phase 2).

Setup package for Windows IPSec-L2TP (CMAK deprecated)

Click this button to download a self-extracting ZIP archive for Windows. In addition to the PKCS#12 file which contains certificates and the private key, the archive includes a certificate import tool and control files for Microsoft's "Connection Manager Administration Kit" (CMAK). CMAK automatically configures the IPSec-L2TP connection in Windows.

Double-clicking the archive in Windows, it will extract itself and then make an attempt to import key and certificates. The user will be prompted for the password which protects the PKCS#12 file. Then, after confirmation, the connection will be configured.



Connections created via CMAK use the obsolete Windows standard SHA-1 for data integrity. In order for Windows to use secure algorithms, this must be adjusted in the Ipsec default settings in the Windows Firewall settings (IKEv1 IKE proposals (phase 1) AES256-SHA1-DH20 und IKEv1 ESP proposals (Phase 2) AES128-SHA1).

Windows IPSec-IKEv2 parameters

Internet IP or servername of SX-GATE

Please enter the DNS name or IP address the client will use to connect with SX-GATE.

Allow direct Internet access

If this option is disabled, there will be no direct Internet access for the client as soon as the VPN connection is established. The client sets its default gateway to the VPN tunnel. So any access to the Internet is routed via VPN and so via SX-GATE's firewall and proxies. When the client disconnects, its default gateway is reset to the original value, restoring direct internet access.

Enable this option and the client keeps its direct Internet connection. Only the relevant IP addresses will be routed via VPN.

Allow direct Internet access

- No

Please read on at [Windows IPsec-IKEv2 setup](#) (p. 163)

Connection-specific DNS suffix

You can optionally assign a connection-specific DNS suffix to the Windows client. So the Windows client can e.g. resolve hosts on the LAN using their plain hostname.

Windows IPsec-IKEv2 routes***Additional routes (powershell only)***

Here you can specify additional local networks to be routed via the VPN connection. To route a connection to a single host you have to supply its IP.



The routes are set only with the Powershell installation package. With the deprecated CMAK installation package, the routes are not taken into account.

Windows IPsec-IKEv2 setup***Setup package for Windows IPsec-IKEv2 (Powershell)***

Click this button to download a self-extracting ZIP archive for Windows. In addition to the PKCS#12 file which contains certificates and the private key, the archive includes a powershell script to create the connection in Windows.

Double-clicking the archive in Windows, it will extract itself and starts automatically the installation dialog.



For the connection the secure algorithms AES256-SHA256-DH20 will be used as IKEv1 IKE proposals (phase 1) and AES256-SHA256 as IKEv1 ESP proposals (Phase 2).

OpenVPN parameters

Internet IP or servername of SX-GATE

Please enter the DNS name or IP address the client will use to connect with SX-GATE.

OpenVPN server interface

Please select the OpenVPN server interface the client is going to connect with. Settings like protocol, port number and encryption parameters in the client configuration will be set accordingly.

OpenVPN setup

Password protected private key embedded in .ovpn file

Download an OpenVPN configuration file for the client here. The private key, its corresponding certificate and the CA certificate are embedded in the file. The private key is encrypted with the password you selected previously.

Unprotected private key embedded in .ovpn file

Similar to the previous option, but with unencrypted private key. So no password is required to establish the VPN connection. We recommend to enable server-side user authentication.



Unauthorized access to the configuration file must be prevented by appropriate measures both, during transport to the client and on the client itself.

Private key in password protected PKCS#12 file

This self-extracting ZIP archive is intended to simplify the OpenVPN configuration in Windows. The archive consists of a PKCS#12 file with the private key, its corresponding certificate and the CA certificate. Also an OpenVPN config file with appropriate settings is included. Double-clicking the archive in Windows will extract the contents to the system-wide OpenVPN config directory.

Whenever the client tries to open a new connection the password has to be entered in order to extract the private key from the PKCS#12 file.

Import of private key into Windows user certificate store

This self-extracting ZIP archive is intended to simplify the OpenVPN configuration in Windows. The archive consists of a PKCS#12 file with the private key, its corresponding certificate and the CA certificate. Also an OpenVPN config file with appropriate settings is included. Double-clicking the archive in Windows will prompt for the import password and install the private key and the certificate into the Windows user certificate store. The .ovpn file is extracted into the system-wide OpenVPN config directory.

The client will be able to start the VPN connection without entering a password. We recommend to enable server-side user authentication.

Password protected private key embedded in .ovpn file

Since OpenVPN 2.6 the Windows client "OpenVPN GUI" supports Start Before Logon (SBL). When configured, an additional icon will show up on the Windows logon screen. Click the icon to establish the VPN connection before logging into Windows. This allows you to directly logon to a Window domain via VPN.



It is necessary to enable the "Pre-Logon Authentication Provider" (PLAP) in the settings of OpenVPN GUI.

The self-extracting ZIP archive provided here contains an OpenVPN configuration file with an embedded encrypted private key. The file will be installed to the system-wide OpenVPN configuration directory "config-auto" on Windows. An additional file is created in this directory with a random password that is used for the internal communication of OpenVPN.

Whenever the client tries to open a new connection the password has to be entered in order to decrypt the private key.

Import of private key into Windows machine certificate store

Since OpenVPN 2.6 the Windows client "OpenVPN GUI" supports Start Before Logon (SBL). When configured, an additional icon will show up on the Windows logon screen. Click the icon to establish the VPN connection before logging into Windows. This allows you to directly logon to a Window domain via VPN.



It is necessary to enable the "Pre-Logon Authentication Provider" (PLAP) in the settings of OpenVPN GUI.

The self-extracting ZIP archive provided here contains a PKCS#12 file with the private key, its corresponding certificate and the CA certificate. Also an OpenVPN config file with appropriate settings is included. You need to install the archive as administrator on Windows. After prompting for the import password the private key and the certificate will be installed into the Windows machine certificate store. The .ovpn file is extracted into the system-wide OpenVPN config directory "config-auto". An additional file is created in this directory with a random password that is used for the internal communication of OpenVPN.

The client will be able to start the VPN connection without entering a password. We recommend to enable server-side user authentication.

iOS IPSec parameters

Only a few parameters can be configured for the profile. Additionally the profile instructs iOS to change its proxy configuration according to the proxy auto configuration file it retrieves from SX-GATE while the VPN is established.

Internet IP or servername of SX-GATE

Please enter the DNS name or IP address the client will use to connect with SX-GATE.

User's XAUTH login

Enter the user login for authentication with SX-GATE. If empty, the user is prompted for it while connecting the VPN.

iOS IPSec profile

iOS profile for IPSec VPN

Click this button to download an iOS IPSec VPN profile. In addition to the settings, the profile contains certificates and a private key in PKCS#12 format.

While installing the profile, the user will be prompted for the password which protects the PKCS#12 file.

Parameters for remote SX-GATE

Internet IP or servername of central SX-GATE

Please enter the DNS name or IP address the remote SX-GATE will use to connect with the local one.

IPSec server connection

Please select the IPSec connection the remote SX-GATE is expected to connect with. This is necessary to supply the remote SX-GATE with the required settings.

Setup for remote SX-GATE

Setup package for remote SX-GATE

This tar archive is intended to simplify the configuration of a VPN to an other SX-GATE. The archive consists of a PKCS#12 file with the private key, its corresponding certificate and the CA certificate. Also a config file with appropriate settings is included. Import this file on the remote SX-GATE.

iOS Exchange parameters

Internet IP or servername of SX-GATE

Please enter the DNS name or IP address the client will use to connect with SX-GATE.

User's Windows login

Enter the user's Windows login including the Windows domain in format "login@domain". If empty, the user is prompted for it while installing the profile.

Users's Exchange email address

Enter the Exchange user's email address. If empty, the user is prompted for it while installing the profile.

iOS Exchange profile***iOS profile for access to Exchange***

Click this button to download an iOS profile for accessing Exchange. In addition to the settings, the profile contains certificates and a private key in PKCS#12 format, used for authenticating the iOS to SX-GATE's reverse proxy.

While installing the profile, the user will be prompted for the password which protects the PKCS#12 file and the password for logging into the Exchange server.

Install in "Keyring"

A table gives you an overview of the available objects. If multiple columns are displayed you can change the sort order by clicking the column title. If there are more than 20 entries, a navigation bar will appear below the bottom right hand corner of the table. You can switch between a grouped view or a pager. The full screen mode allows you to see all entries at the same time. Pick an entry by clicking its title in the left column. A pencil icon or a trashcan in the right column allow you to rename or delete an entry. Add new objects by clicking "New Entry" below the table on the left.

Name of key

Here you have to specify a name for the key. It is only used to identify the key, so you can choose any appropriate name.

Issue local VPN server certificate

With this function you can issue or renew the certificate of SX-GATE's own VPN server. The new certificate will be signed by the SX-GATE CA and is valid for up to 6 years.

Issue new VPN server certificate

On this screen you have to enter the certificate subject.

CN

If SX-GATE has a static Internet IP address or a certain DNS name, you should supply it here. Otherwise choose a name which is rather unambiguous.

Subject alternative names

Most clients prefer this certificate property while verifying that the server certificate belongs to the expected server. Enter all required names and IPs used to address the IPsec server from the Internet.



This property is mandatory if MacOS clients will connect. MacOS clients expect server certificates with a subject alternative name which includes the server address as configured in the MacOS client.

Certificate request

Entering this screen, a certificate request will be generated on SX-GATE. You can sign it now with the CA certificate.

Extended Key Usage: server authentication

It is recommended to enable this option. By default the Windows IPsec client requires the VPN server certificate to include this "Extended Key Usage" value.



Depending on the client and its configuration, a client may refuse to connect if the server certificate does not include this attribute.

Signing certificate

Entering this screen, the certificate will be signed. By pressing the "Finish" button, the new VPN server key will be installed.

12.4.1.3 Custom CAs

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

12.4.1.3-A Certificates.....	169
12.4.1.3-B Usage.....	169

Here you can upload external or local CA certificates, if required by some SX-GATE services to verify certificates. Change into the configuration of the respective services to select which CAs it should use.

12.4.1.3-A Certificates

Export CA certificate / CA bundle

You can download the certificate or certificate bundle here. The file format is PEM.



The export will not contain certificates from "Included CA certificates / bundles".

Import CA certificate or bundle

Here you can upload CA certificates in PEM format. A PEM formatted certificate is base64 encoded, i.e. it's a simple text file. The certificate is surrounded with the boundary lines "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----". Text outside of those boundaries is ignored. Concatenate multiple CA certificates in a single file to upload a "CA bundle".



You should upload root CA certificates only. The administration interface does not check if the upload contains just root or CA certificates.

Included CA certificates / bundles

Use this control to combine multiple CA certificates or bundles.

12.4.1.3-B Usage

This table show in which settings the definition is used.

12.4.2 Keyring

You can manage all the key-pairs used by the various SX-GATE servers in this menu. A key-pair consists of a private key and a corresponding public key. The public key is part of a certificate, i.e. it has been signed by a certificate authority (CA).



For security reasons, private keys are not included with the SX-GATE backups. Use the export function on each key-pair's screen to download and save a password protected copy.

In this menu you can manage key-pairs signed by public CAs as well as key-pairs signed by the SX-GATE CA. There are also simple self-signed certificates like the pre-defined key-pair "DUMMY". It serves as the default certificate for all servers and is also used as a fallback if a key-pair is incomplete, i.e. the private key is missing. Note that you cannot create backups of self-signed certificates.

To select a key-pair for a certain SX-GATE server, please change into the menu of this server.

A table gives you an overview of the available objects. If multiple columns are displayed you can change the sort order by clicking the column title. If there are more than 20 entries, a navigation bar will appear below the bottom right hand corner of the table. You can switch between a grouped view or a pager. The full screen mode allows you to see all entries at the same time. Pick an entry by clicking its title in the left column. A pencil icon or a trashcan in the right column allow you to rename or delete an entry. Add new objects by clicking "New Entry" below the table on the left.

Name of key

Here you have to specify a name for the key. It is only used to identify the key, so you can choose any appropriate name.

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

12.4.2.1-A Current key-pair.....	171
12.4.2.1-B Previous key-pair.....	178
12.4.2.1-C Usage.....	179

Application procedure

Select how to apply for the new certificate.

manual

Select this option to manually submit the certificate signing request (CSR) to the CA, either by file or by copy-and-paste. As soon as the CA has issued the certificate it has to be imported into SX-GATE by file upload or copy-and-paste.

ACME (e.g. Let's Encrypt)

Select this option to automatically issue and renew certificates using the ACME protocol. Currently only HTTP authorization is supported. The SX-GATE firewall must forward inbound HTTP connections to an HTTP port of its reverse proxy that in turn must be configured to handle ACME HTTP authorization.

Managed PKI

This option only make sense if you need a lot of certificates (e.g. when using the SX-GATE S/MIME gateway). Certificates will be issued and renewed automatically.



At the moment we support the CA SwissSign only. We're happy to add further CAs here. We require an interface description and a test account.

12.4.2.1-A Current key-pair

On this tab you can manage the currently active key-pair. Whenever the current key-pair is replaced (e.g. when issuing a new key-pair or restoring the backup of a key-pair), a backup of the old key-pair is kept. If a previous backup exists, it will be overwritten, i.e. only one generation of previous key-pairs is stored. As soon as a backup exists, the tab "Previous key-pair" will become available.



The previous key-pair might be used by the SX-GATE S/MIME gateway.



For security reasons, private keys are not included with the SX-GATE backups. You should therefore backup the key-pair, in particular for purchased certificates.

MPKI profile

Profiles are created in menu "System > Certificate manager > MPKI profiles" and include the credentials for connecting to the CA, the selected certificate product and other parameters.

Manual renewal

The certificate is renewed automatically if automatic renewal has been enabled in the profile. Use this switch to disable automatic renewal for this individual certificate.

Import the issued certificate

This wizard becomes available after you have filed a certificate signing request. As soon as the CA issued the certificate you can import it here.

Select certificate file

Here you can import the certificate you received back from the certificate authority. Both, the PEM and the DER format are supported.

Check certificate

Check the certificate you just uploaded before it's going to be installed.

Please read on at [Install certificate](#)

Select CA certificate file

Now the certificate chain must be added to the certificate. This may include one or more intermediate CAs. The chain ends with the root CA. All certificates must be in PEM or DER format. Please ask your CA for the required certificates.

Check CA certificate

The uploaded certificate is appended to the certificate chain.

Please read on at [Select CA certificate file](#)

Install certificate

The import procedure is complete. The certificate is now ready to be installed.

Delete certificate request

You can cancel a certificate request here.



This will destroy the private key irrevocably.

Export certificate

You can download the certificate here. The certificate is the CA signed public key. The file format is PEM.



This is not a backup function as the private key is not included.

ACME server

If you are using the ACME protocol for automatic certificate updates, the name of the ACME server is shown here.

Configure certificate retrieval via ACME

ACME settings

Select the CA and enter the certificate properties on this screen.

ACME server

Please enter the ACME server here. If the CA provides a test environment, we recommend to use it whenever you issue a certificate for a server name for the first time. There is often a limit on transactions in the production environment which you might hit when running into problems.

Contact email for CA

Some CAs ask for the email address of an administrator when registering for their service.

CN

Issue the certificate to the DNS name which is used to connect with the service from the Internet.



Certificates for IP addresses are not supported via ACME by the CAs we know.

Subject alternative names

Most clients prefer this certificate property while verifying that the server certificate belongs to the expected server. Enter all required names used to address the server.



Wildcard certificates and IP addresses are not supported via ACME by the CAs we know.

Key strength

Old systems like e.g. Windows XP before SP3 might only support keys with max. 2048 bit.

Retrieve / renew certificate via ACME

With this function you will retrieve a certificate from the ACME server, using the previously configured properties.

Check registration

First SX-GATE needs to register itself with the ACME server. Usually you will also have to download, read and accept the CA's terms of service.

Issue new certificate

[Click here](#) to issue a new certificate.



To get a certificate from the local SX-GATE CA, please issue the certificate in menu "System > Certificate manager > CA certificates". Follow the link "Certificates" in the "SX-GATE CA" line. At the end of this process you will have the possibility to store the new key-pair in the "Keyring".

Choose action***Please select what you want to do***

There are different ways to get a new certificate:

Create a certificate request for submission to an external CA

In order to get a certificate from a public certification authority (CA), you need to hand in a certificate signing request (CSR). For this purpose SX-GATE first creates a new RSA key-pair and asks for all the data to be included in the CSR. You can then download the CSR as file or copy it as text and forward it to the CA. An import wizard becomes available where you can upload the certificate, once you get it back from the CA.

Issue a certificate signed by the SX-GATE CA

Certificates issued by the SX-GATE CA are suitable for use in a closed user group like e.g. VPN for your own employees.

Create a new selfsigned certificate

A self-signed certificate can be useful while testing. The certificate will be valid for one year.



This certificate is not signed by the SX-GATE CA.

Please select what you want to do

- Create a certificate request for submission to an external CA
Please read on at [Create a certificate request](#) (p. 175)
- Issue a certificate signed by the SX-GATE CA
Please read on at [Issue a certificate signed by the SX-GATE CA](#) (p. 175)
- Create a new selfsigned certificate
Please read on at [Certificate data](#) (p. 176)

Issue a certificate signed by the SX-GATE CA

Certificates from the local SX-GATE CA are available via menu "CA certificates". From there, follow the link "Certificates" in the "SX-GATE CA" line. Please select 'Install in "Keyring"' at the end of the certificate issue process.

Create a certificate request for submission to an external CA

Create a certificate request

On this screen you have to enter the certificate subject.

CN

Issue the certificate to the address which is normally used to connect with the service from the Internet. Usually this is the Internet DNS name of SX-GATE. You can also issue a wildcard certificate (e.g. *.example.com), however wildcard certificates are usually much more expensive.

Subject alternative names

Most clients prefer this certificate property while verifying that the server certificate belongs to the expected server. Enter all required names and IPs used to address the server. You can also issue a wildcard certificate (e.g. *.example.com).



Some CAs ignore this extension. Often the charge for multidomain and wildcard certificates is considerably higher. Please clarify this with the CA before you submit the certificate request.

Certificate request

Entering this screen, a certificate request will be generated on SX-GATE.

Issue self-signed certificate

Certificate data

A self-signed certificate can be useful while testing.

Issue certificate

The self-signed certificate has been issued.

Update certificate (re-issue)

This function is only rarely needed. No new key-pair will be generated, the old key-pair is still used. The certificate authority just provides an newly signed certificate.



If the old certificate is about to expire, we recommend to generate a new key-pair. Use the wizard "Issue new certificate" to generate a new certificate request.

Select certificate file

Here you can import the new certificate you received from the certificate authority. Both, the PEM and the DER format are supported.

Check certificate

Check the certificate you just uploaded before it's going to be installed.

Please read on at [Install certificate](#)

Select CA certificate file

Now the certificate chain must be added to the certificate. This may include one or more intermediate CAs. The chain ends with the root CA. All certificates must be in PEM or DER format. Please ask your CA for the required certificates.

Check CA certificate

The uploaded certificate is appended to the certificate chain.

Please read on at [Select CA certificate file](#)

Install certificate

The import procedure is complete. The certificate is now ready to be installed.

Configure certificate retrieval through MPKI

Create a certificate request

On this screen you have to enter the certificate subject. Configure default values in the profile.

CN

Issue the certificate to the address which is normally used to connect with the service from the Internet. Usually this is the Internet DNS name of SX-GATE. You can also issue a wildcard certificate (e.g. *.example.com), however wildcard certificates are usually much more expensive. For S/MIME certificates usually the email address or the name of the owner is entered.

Subject alternative names

Most clients prefer this certificate property while verifying that the server certificate belongs to the expected server. Enter all required names used to address the server. You can also issue a wildcard certificate (e.g. *.example.com).



Some CAs ignore this extension. Often the charge for multidomain and wildcard certificates is considerably higher. Please clarify this with the CA before you submit the certificate request.

Revoke certificate

Reason

Please select the reason for revoking

Reason

Please select the reason for revocation.

Import backup of key-pair

You can import a key-pair in PKCS#12 format here.

Select file

Select the PKCS#12 file with the key-pair and enter the password which protects the file.

Check certificate

Check the certificate you just uploaded before it's going to be installed.

Please read on at [Install certificate](#)

Select CA certificate file

Now the certificate chain must be added to the certificate. This may include one or more intermediate CAs. The chain ends with the root CA. All certificates must be in PEM or DER format. Please ask your CA for the required certificates.

Check CA certificate

The uploaded certificate is appended to the certificate chain.

Please read on at [Select CA certificate file](#)

Install certificate

The import procedure is complete. The certificate is now ready to be installed.

Backup key-pair

The key pair can be exported in PKCS#12 format to save a backup. Please note that this export also contains the private key which must be kept secret.



There's no way to restore a purchased certificate without backup.

12.4.2.1-B Previous key-pair

After replacing a key-pair, the previous key-pair is made available on this tab. This backup is primarily intended to protect against accidental loss.



The SX-GATE S/MIME gateway might use the old key-pair to decrypt inbound emails that have been encrypted with the old certificate.



Only one generation of old keys is stored on the device. The previous key-pair is not part of the SX-GATE backups.

Backup the previous key-pair

The key pair can be exported in PKCS#12 format to save a backup. Please note that this export also contains the private key which must be kept secret.



There's no way to restore a purchased certificate without backup.

Swap previous and current key-pair

To re-enable the previous key-pair, you can swap it with the current key-pair.

12.4.2.1-C Usage

This table show in which settings the definition is used.

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

12.4.2.2-A Ed25519 Key.....	179
12.4.2.2-B Previous key-pair.....	179
12.4.2.2-C Usage.....	180

12.4.2.2-A Ed25519 Key

Download public key

You can download the public key here.



This is not a backup function as the private key is not included.

Import backup of private key

You can import a private key in OpenSSH format here.

Install key

The import procedure is complete. The key is now ready to be installed.

Backup private key

The private key can be exported in OpenSSH format to save a backup. Please note that the private key must be kept secret.

12.4.2.2-B Previous key-pair

After replacing a key-pair, the previous key-pair is made available on this tab. This backup is primarily intended to protect against accidental loss.

Backup private key

The private key can be exported in OpenSSH format to save a backup. Please note that the private key must be kept secret.

Swap previous and current key-pair

To re-enable the previous key-pair, you can swap it with the current key-pair.

12.4.2.2-C Usage

This table show in which settings the definition is used.

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

12.4.2.3-A X25519 Key.....	180
12.4.2.3-B Previous key-pair.....	180
12.4.2.3-C Usage.....	181

12.4.2.3-A X25519 Key***Import backup of private key***

You can import a private X25519 key that has been exported from a SX-GATE here. It is using a special encrypted backup format.



It is not possible to import raw unencrypted private X25519 keys as generated by the wireguard command "genkey".

Install key

The import procedure is complete. The key is now ready to be installed.

Backup private key

You can export the private key to save a backup. It will be AES-256 encrypted with a password. Please note that the private key must be kept secret.

12.4.2.3-B Previous key-pair

After replacing a key-pair, the previous key-pair is made available on this tab. This backup is primarily intended to protect against accidental loss.

Backup private key

The private key can be exported in OpenSSH format to save a backup. Please note that the private key must be kept secret.

Swap previous and current key-pair

To re-enable the previous key-pair, you can swap it with the current key-pair.

12.4.2.3-C Usage

This table show in which settings the definition is used.

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

12.4.2.4-A RSA Key.....	181
12.4.2.4-B Previous key-pair.....	182
12.4.2.4-C Usage.....	182

12.4.2.4-A RSA Key**Public key (DKIM format)**

DKIM requires that the public key is published in the DNS of the domain to sign. The name of that DNS entry consists of a selector and the text "_domainkey". The selector is an identifier of your choice that should correspond to a specific DKIM key. The required type of the DNS entry is "TXT". Enter the data displayed here as its value.



Depending on the administration interface of your DNS server it may be necessary to split this very long entry into multiple parts with a maximum of 255 characters each (e.g. dkim._domainkey TXT "Part1" "Part2" ... "PartX").

For example if you decided to use the text "dkim" as selector and want to sign the domain "example.com", the required DNS entry would be "dkim._domainkey.example.com".

The key should be changed regularly. Please do not replace the existing key-pair via "Generate new key". Add a new entry below "Keyring" instead and publish the new public key with a different selector in DNS.



When changing the DKIM key once a year, you could include the year number in the selector.

After publishing the public key in DNS you can enable DKIM for the respective domain in menu "Modules > Mail Server > Domains".

Download public key (SSH format)

You can download the public key here.



This is not a backup function as the private key is not included.

Import backup of private key

You can import a private key in format OpenSSH, PEM or PKCS#8 here.

Install key

The import procedure is complete. The key is now ready to be installed.

Backup private key

The private key can be exported in OpenSSH format to save a backup. Please note that the private key must be kept secret.

12.4.2.4-B Previous key-pair

After replacing a key-pair, the previous key-pair is made available on this tab. This backup is primarily intended to protect against accidental loss.

Backup private key

The private key can be exported in OpenSSH format to save a backup. Please note that the private key must be kept secret.

Swap previous and current key-pair

To re-enable the previous key-pair, you can swap it with the current key-pair.

12.4.2.4-C Usage

This table show in which settings the definition is used.

12.4.3 MPKI profiles

Many CAs offer a "Managed PKI" (MPKI), an interface for automatic certificate purchase. This makes sense for customers requiring many certificates like those using the SX-GATE S/MIME gateway.



If the CA of your choice is not yet supported by SX-GATE, we need an interface description and a test account to make it available.

In this menu you can create profiles that provide all the required settings to order certificates of a specific kind from a specific CA.

A table gives you an overview of the available objects. If multiple columns are displayed you can change the sort order by clicking the column title. If there are more than 20 entries, a navigation bar will appear below the bottom right hand corner of the table. You can switch between a grouped view or a pager. The full screen mode allows you to see all entries at the same time. Pick an entry by clicking its title in the left column. A pencil icon or a trashcan in the right column allow you to rename or delete an entry. Add new objects by clicking "New Entry" below the table on the left.

Profilename

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

12.4.3-A CA settings.....	183
12.4.3-B Default values.....	184
12.4.3-C Usage.....	184

12.4.3-A CA settings

On this tab you select the CA and choose the certificate product.

API selection

If you have access to the test environment, we highly recommend to configure it first, as there are usually no costs involved here. Change to the production environment as soon as everything works as expected.

At the moment we support SwissSign only. We're happy to add further CAs here. We require an interface description and a test account.

Login

Enter the credential you received from the CA to access the MPKI.

Automatic renewal

Enable this option to renew certificates that are about to expire automatically.



In the settings of the individual certificates you can disable the automatic renewal for a specific certificate.



The automatic renewal usually incurs costs.

Renewal

Configure how many days before its expiry a certificate should be renewed if the automatic renewal is enabled.

Selected product

The selected certificate product is displayed here.

Select product

Select the certificate product that should be ordered by this profile.



If you require different certificate products, you will have to add a dedicated profile for each one.

12.4.3-B Default values

On this tab you can set default values for the various fields and properties of the certificates linked to this profile. You can override the values in the individual settings of each certificate.

12.4.3-C Usage

This table show in which settings the definition is used.

12.5 Backup

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

12.5-A Actions.....	185
12.5-B System backup.....	187
12.5-C User backup.....	189
12.5-D Mail backup.....	191
12.5-E CA keys.....	193
12.5-F Keyring backup.....	194

12.5-A Actions

Restore backup

Generally, it is recommended that you backup the current settings before restoring them from a backup file. The currently values will be replaced by the data from the backup.



Mail backups are handled in a special way. Please take notice of the following hints.

A mail backup contains the email folders plus any additional data from the home directories of all users. If the SX-GATE Groupware is installed, it also contains the groupware data such as address books, calendars, mail filters and other settings.

A mail backup can become very large. Uploading the backup may take a long time or it might even be too large to be accepted by the administration web server. Particularly if only a single user's mailbox is to be restored you should consider opening the mail backup file with an archiver which is able to handle ZIP files.



You must upload unmodified .rbu files only. Some archivers will allow you to modify the contents of an archive. Saving the changes might damage the backup file, so that SX-GATE will refuse to accept it.

The mail backup file contains an .rbu file for each user. Upload the respective file to restore the mail backup of one specific user. However it is even possible to open the backup file of an individual user. It contains one file for the home directory with the emails ("folders-<username>.rbu") and possibly one for groupware data ("sogo-<username>.rbu"). Each can be restored by its own.



Extract and upload the backup file with either the home directory and mails or the groupware data to restore only one part of the users mail data.

SX-GATE will restore a user's files only if all of the following conditions apply:

- The user exists on SX-GATE
- The user is member of group "system-mail"

While restoring emails, groupware adressbooks and groupware calendars, SX-GATE makes an effort to merge the data, i.e. deleted entries will be restored from the backup, new elements will be kept. An element which has been moved into an other folder (even if it's the trash folder) won't be restored as it's still present.



It is possible that elements are doubled while merging.



Groupware mail filters, subscriptions and other settings will be overwritten with the data from the backup.



When restoring a mail backup from the 7.0 release series or older, all emails will be taken from the backup. New mails will be lost!

Reset configuration

The default configuration of SX-GATE can be restored with this option.

Reset type

Please select reset type

Please select which parts of SX-GATE you want to reset.



If you proceed, the IP address of SX-GATE will be reset to its default value 192.168.0.254.

Default system configuration only

The reset to this state can be compared to restoring the system backup of a new SX-GATE. Only the system configuration will be affected. Other parts like e.g. the users and their emails, logfiles and statistics will not be deleted.

Delivery state

In contrast to the previous option the system will be reset to the state of its delivery. If you choose this, the users, emails, logfiles and statistics will be deleted, too. The password of the administrator will be reset to the default password.

Show all configuration settings

Press this button to show you all system- and user-settings of SX-GATE. A new browser window with a raw list of all settings will open. Please note that this is not a backup of your system. It is just for documentation.

12.5-B System backup

On this screen you can configure the backup of the system configuration (system backup). The settings of the user administration will not be included in this backup.



For security reasons the backup will not contain the SX-GATE CA keys. Furthermore, if the backup is not encrypted, it will contain no private keys at all. Please refer to the tabs "CA keys" and "Keyring backup" to backup private keys.



Always keep these backup files in a save place. Otherwise they may end up being read in the wrong hands!

Create system backup now

To save the system backup manually, please press this button.

Automatic system backup by

Please select the protocol used for transfer. Except for secure copy and SFTP the backup is transmitted unencrypted. The backup file is only stored encrypted on the target system if you have chosen an encrypted backup. Please make sure the file is protected in case of an unencrypted backup.



Secure copy and SFTP connections are authenticated using SX-GATE's SSH ED25519 or RSA key. Please configure the SSH resp. SFTP server accordingly.

Encryption password

In general an encrypted backup is preferable to an unencrypted backup.



But bear in mind that the backup is worthless if the password for encryption has been lost!



An encrypted system backup also includes the private keys from the keyring, but not the SX-GATE CA keys.

Login

Enter the user name SX-GATE has use to authenticate itself.



When storing the backup on a Windows network share you will usually have to specify the Windows domain name along with the user name. Please use the syntax "Domain/Username". Do not enter a backslash ("\") as you would in Windows.

Path and filename

Enter the directory and filename for the backup. The directory part is optional. However if you enter a directory, it must already exist on the server.

The filename can include variables, so previously created backup file will not be overwritten. The following variables are available:

- %Y: 4 figure year (e.g. 2001)
- %y: 2 figure year (e.g. 01)
- %m: Month (from 01 to 12)
- %d: Day (from 01 to 31)
- %H: Hour (from 00 to 23)
- %M: Minute (from 00 to 59)
- %S: Second (from 00 to 59)
- %U: Week of the year (Value from 00 to 53)
- %w: Day of the week (0 for Sunday to 6 for Saturday)
- %j: Day of the year (from 001 to 366)

If for instance you specify the destination

"backup/%m.%d.rbu"

, the filename will include the current month and day. Thus the backup file will not be overwritten until next year.

Scheduled

Use the automatic backup to make sure that it will not be forgotten. Select when and how often the backup should be created.



Monthly backups will be created on the first day of each month.
Weekly updates will be made on Mondays.



You should check the backups regularly.

Test automatic systembackup

Tries to transfer the current system configuration to the configured location.

12.5-C User backup

On this screen you can configure the backup of menu "System > User administration".



Always keep these backup files in a save place. Otherwise they may end up being read in the wrong hands!

Create user backup now

To save the user backup manually, please press this button.

Automatic user backup by

Please select the protocol used for transfer. Except for secure copy and SFTP the backup is transmitted unencrypted. The backup file is only stored encrypted on the target system if you have chosen an encrypted backup. Please make sure the file is protected in case of an unencrypted backup.



Secure copy and SFTP connections are authenticated using SX-GATE's SSH ED25519 or RSA key. Please configure the SSH resp. SFTP server accordingly.

Login

Enter the user name SX-GATE has use to authenticate itself.



When storing the backup on a Windows network share you will usually have to specify the Windows domain name along with the user name. Please use the syntax "Domain/Username". Do not enter a backslash ("\") as you would in Windows.

Path and filename

Enter the directory and filename for the backup. The directory part is optional. However if you enter a directory, it must already exist on the server.

The filename can include variables, so previously created backup file will not be overwritten. The following variables are available:

- %Y: 4 figure year (e.g. 2001)
- %y: 2 figure year (e.g. 01)
- %m: Month (from 01 to 12)
- %d: Day (from 01 to 31)
- %H: Hour (from 00 to 23)
- %M: Minute (from 00 to 59)
- %S: Second (from 00 to 59)
- %U: Week of the year (Value from 00 to 53)
- %w: Day of the week (0 for Sunday to 6 for Saturday)
- %j: Day of the year (from 001 to 366)

If for instance you specify the destination

"backup/%m.%d.rbu"

, the filename will include the current month and day. Thus the backup file will not be overwritten until next year.

Scheduled

Use the automatic backup to make sure that it will not be forgotten. Select when and how often the backup should be created.



Monthly backups will be created on the first day of each month. Weekly updates will be made on Mondays.



You should check the backups regularly.

Test automatic userbackup

Tries to transfer the current user configuration to the configured location.

12.5-D Mail backup

On this screen you can configure the backup of the inbox, the home directories and the groupware data of all users. In the home directory IMAP and groupware mail folders will be stored. Groupware data includes the settings, address books, calendar entries and filter settings.



Always keep these backup files in a save place. Otherwise they may end up being read in the wrong hands!

Create mail backup now

To save the mail backup manually, please press this button.



This always creates a complete backup including all mail users, regardless of the setting "Create backupfile for each mail user?".

Automatic mail backup by

Please select the protocol used for transfer. Except for secure copy and SFTP the backup is transmitted unencrypted. The backup file is only stored encrypted on the

target system if you have chosen an encrypted backup. Please make sure the file is protected in case of an unencrypted backup.



Secure copy and SFTP connections are authenticated using SX-GATE's SSH ED25519 or RSA key. Please configure the SSH resp. SFTP server accordingly.



It is not advisable to deliver the mailbackup by email, especially if it will be sent to a local user. If the mail stays in the local inbox for a while the size of the mailbackup might increase dramatically!

Login

Enter the user name SX-GATE has use to authenticate itself.



When storing the backup on a Windows network share you will usually have to specify the Windows domain name along with the user name. Please use the syntax "Domain/Username". Do not enter a backslash ("\") as you would in Windows.

Path and filename

Enter the directory and filename for the backup. The directory part is optional. However if you enter a directory, it must already exist on the server.

The filename can include variables, so previously created backup file will not be overwritten. The following variables are available:

- %Y: 4 figure year (e.g. 2001)
- %y: 2 figure year (e.g. 01)
- %m: Month (from 01 to 12)
- %d: Day (from 01 to 31)
- %H: Hour (from 00 to 23)
- %M: Minute (from 00 to 59)
- %S: Second (from 00 to 59)
- %U: Week of the year (Value from 00 to 53)
- %w: Day of the week (0 for Sunday to 6 for Saturday)
- %j: Day of the year (from 001 to 366)

If for instance you specify the destination

"backup/%m.%d.rbu"

, the filename will include the current month and day. Thus the backup file will not be overwritten until next year.

Scheduled

Use the automatic backup to make sure that it will not be forgotten. Select when and how often the backup should be created.



Monthly backups will be created on the first day of each month. Weekly updates will be made on Mondays.



You should check the backups regularly.

Create backupfile for each mail user?

If this option is activated a backupfile for each mail user will be created at the configured destination. The configured filename is prefixed with the user's login name and an underscore.

Test automatic mailbackup

Tries to transfer the current email storage to the configured location.

12.5-E CA keys

Private keys are not part of the regular backups for security reasons. However particularly the CA keys are essential to the functionality. As CA certificates are valid for many years and usually won't change during this period of time, creating a backup once is enough. The backup file is password protected.



Deposit the backup at safe places and remember that the CA is valid for many years. The media should be suitable for longterm storage. Make sure that the password required to re-import the backup file cannot be forgotten.

Backups of CA keys made on this screen must be restored in menu "System > Certificate manager > CA certificates" below "SX-GATE CA".

Backup CA key-pair

The key pair of the SX-GATE CA can be exported in PKCS#12 format to save a backup. Please note that this export also contains the private key which must remain completely secret.

Backup proxy key-pair

The key pair of SX-GATE's proxy CA can be exported in PKCS#12 format to save a backup. Please note that this export also contains the private key which must remain completely secret.

12.5-F Keyring backup

On this screen you can backup the private keys from menu "System > Certificate manager > Keyring".



Always keep these backup files in a save place!

12.6 Update

Bringing in an update normally takes a few minutes and if need be will re-start the system by itself. Please be sure to read the README file instructions on the respective update. After each update, your version of SX-GATE should display a new value. If this isn't the case, please consult technical support. If an automatic update has been planned, you will see a corresponding message on this side. It is then possible to cancel the automatic update here.

SX-GATE update

Here you can update your SX-GATE system.



Please check regularly if new updates are available. Not installing updates which contain security fixes can affect the security of your networks.

Installed release

The currently installed release of SX-GATE is shown here.

Update server

To make the update procedure straightforward, SX-GATE can suggest which updates need to be installed next. Enter the URL where SX-GATE can download updates.

How do you want to update your SX-GATE?

Please select the update method.

interactive (recommended)

Choose this option to get an overview of all available updates first. After confirmation the first one will be installed. Repeat this procedure until all updates have been installed.

scheduled

With this option SX-GATE will also show you a list of available updates. However here you have to specify the time when SX-GATE will automatically start to install updates. The first update due is always installed. All following regular updates are also installed automatically. Processing stops before beta releases, non-free releases and whenever a choice between multiple alternative updates has to be made.

manually by uploading an update file

If you have the update file stored locally in the form of a *.rup file, you can upload this file manually.

How do you want to update your SX-GATE?

- interactive (recommended)
Please read on at [Available updates](#) (p. 196)
- scheduled
Please read on at [Schedule update](#) (p. 196)
- manually by uploading an update file
Please read on at [Select file](#) (p. 197)

View latest update log

This tab allows you to see any message that was produced while installing the previous update. If there were any problems, the log might provide further information.



10 days after the last access, the log will be deleted automatically.

Schedule update

Select day and time when the update should be started. At the specified point in time, SX-GATE will download and install all available updates one by one.



If the given time already has passed, the update will be started right after any required setting has been done.

Available updates

This screen lists the updates available for your SX-GATE.



Please take a look at the information provided in the "README" file.

Confirm update

Press "Finish" to complete the update procedure.

Select file

Please select a valid update file for your SX-GATE.

12.7 Apps

Installed apps

Lists all currently installed apps along with their version number and status. Apps can be started, re-started or stopped. A running app will be started automatically next time the runtime environment is started. A stopped app remains stopped.



Apps are running in separated environments (operating-system-level virtualization). The required runtime environment can be started in menu "System > Services" on tab "System".

Check online for updates and more apps

An Internet connection is required by this function as SX-GATE needs to contact its update server. You will get a list of all available apps with the possibility to update installed apps and install new apps.



Apps have to be updated independant of SX-GATE updates. So please don't forget to check for app updates regularly.

12.8 Management server

In this menu you can enter your SX-GATE and SX-GATE Satellite devices. You will then be able to remotely install updates and see the devices' current status.

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

12.8-A Settings.....	199
12.8-B SX-GATE.....	200
12.8-C SX-GATE Satellite.....	202

12.8-A Settings

Private key of the SSH TCP-Forwarders (port 2222)

To avoid problems caused by NAT routers and to avoid having to configure firewall rules often SSH tunnels are used. With an SSH tunnel the managed SX-GATE will initiate a connection to the SSH TCP-Forwarder service of the management server. Here you configure the SSH key used by the TCP-Forwarder. We recommend to generate a dedicated ed25519 key for this purpose in menu "System > Certificate manager > Keyring".



Do not use the pre-defined key "SSH_ED25519" on a clustered management server, as this key is not synchronized.

Private authorization key of the management server

This key is used to authenticate at the managed SX-GATEs. We recommend to generate a dedicated ed25519 key for this purpose in menu "System > Certificate manager > Keyring".



Do not use the pre-defined key "SSH_ED25519" on a clustered management server, as this key is not synchronized.

Corresponding public key

This public key needs to be configured on the managed SX-GATEs to grant access for the management server.

12.8-B SX-GATE

To manage a remote SX-GATE you need to configure it. Beginning with release 7.1-3.3 you will find the settings in menu "System > Setup" on tab "Management access".



The information is updated every 5 minutes. So after adding a new device, it may take up to 5 minutes until information becomes available.

Manageable SX-GATEs

The following parameters have to be configured to manage a remote device:

Name or group/name

Use for your own purposes. Note that the character '/' serves as a delimiter for grouping entries (e.g. "VIP-customers/London - update at night"). This can be useful if you are managing lots of devices.

Active

You can disable the periodic information retrieval here, e.g. if a system is temporarily unavailable. Note that in case of an SSH tunnel the remote device is still allowed to establish the tunnel.

Address / Connection ID

Depending on the direction of the maintenance connection you need to enter:

Connection from management server to managed SX-GATE

IP address or DNS name of SX-GATE

SSH tunnel from managed SX-GATE to management server

An individual connection ID between 10000 and 20000. The ID corresponds to a TCP port which is opened on the management server. The management server can then connect to the managed SX-GATE via this port.

Public key of managed server

Only required for SSH tunnels (Connection from managed SX-GATE to management server). The required public key is displayed on the managed SX-GATE.

The following information is displayed for a managed device:

Version

The last known version of the remote SX-GATE.

Apps

Number of installed apps.

Status

Displays if there is current data available for this device:

green

Fresh data has been received within the last 10 minutes

red

The data is older than 10 minutes

grey

No data has been retrieved yet

The following actions are available:

Details

An overview of the latest data received, even if it is old data

Administration

Opens a connection to the administration interface of the remote SX-GATE. A tunnel is opened between the remote interface and a random port (> 20000) on the LAN IP of the local management server. If the connection is idle for more than five minutes, it will be closed automatically. Whenever you click this link, a new tunnel is opened.



Everyone who has access to the LAN IP of the management server can connect to the administration interface of the remote device. Use firewall rules to restrict access if necessary.

Open support connection

Open a support connection on the managed SX-GATE

New connection with install package

Using this wizard to setup a new connection, you will be able to download an installation package. With it, configuring the remote SX-GATE becomes as simple as installing this package.



Supports tunneled connections established by the managed SX-GATE only.

Supporttunnel / -keys remove

Select devices

overview:

The following states are possible:

mark

Der SX-GATE is in the list.

request send

The request to remove the support tunnels/keys has been sent to SX-GATE.

done

The request completed successfully on SX-GATE.

failed

The request could not be completed successfully on SX-GATE.

status unknown

The status of the request is unknown.

Manageable Devices with open support tunnel or shared authorization key

The table lists all SX-GATE for which a support tunnel is open or shared authorization key is active. The value -1 means that the number of public keys could not be determined.

12.8-C SX-GATE Satellite

Manageable remote devices

Remote devices must be entered manually here. To be able to connect with a SX-GATE Satellite, it must be reachable with SSH and it must have the SSH certificate of SX-GATE installed. The certificate is installed along with the VPN installation package.



Whenever the SX-GATE hardware is swapped, its SSH key will change. Thus SX-GATE Satellites which received the VPN installation package before the hardware was swapped will become unreachable. A backup feature for the SSH key and the possibility to install an SSH certificate on SX-GATE Satellite without issuing a new VPN installation package will be added soon.

The following information has to entered or will be displayed for each remote device:

IPsec connection

Name of the IPsec connection as configured in menu "Modules > Network > Interfaces".

Management IP

The SX-GATE Satellite IP address SX-GATE is going to connect to with SSH. Usually you will enter the internal IP address of the SX-GATE Satellite here. You could also enter its external IP, however this required a firewall rule on SX-GATE Satellite.

Certificate

The certificate of the IPsec connection from menu "System > Certificate manager > CA certificates". This parameter is optional and will be used by a future extension.

Expiry date

The installed IPsec-certificate on SX-GATE Satellite expires on the specified date.

Version

The detected version

wifi

The availability of the wifi on SX-GATE Satellite.

Status

The status is signaled via traffic lights. There are four possible results:

green

The last update was successful and no errors or warnings were found.

yellow

There is at least one error or warning.

red

The last connection failed.

white

There is no information or the remote device is unknown.

Additional details are displayed as a tooltip when you point the mouse on the traffic light.

Install update

This wizard lets you update multiple remote devices at a time.



Make sure that nobody in the remote office switches off the device during this stage. The device might be damaged irreparably.



Currently updates are supported for SX-GATE Satellite with at least version 3.1.1 only.

Select file

In case an update is running in the background, the latest status of the entire update process is loaded. The information will not be refreshed automatically on this page.

Otherwise, you can select and upload a firmware.

Select devices

After successfully checking the firmware, the details of the firmware and the remote devices that can be updated with this firmware are shown here.



Make sure that nobody in the remote office switches off the device during the update. The device might be damaged irreparably.

Details of the firmware:

The following information regarding the firmware is displayed:

Version

Architecture

32 and 64 bit versions are supported.



To install a 64 bit version, a SX-GATE Satellite with at least version 3.2.0 is required. Furthermore its hardware must support 64 bit.

Suitable for version

Depending on the SX-GATE Satellite version, you will need a specific image:

< 3.1.1

legacy firmware

>= 3.1.1

default firmware

Available remote devices which are suitable for the update:

After successfully checking the firmware, the details of the firmware and the remote devices that can be updated with this firmware are shown here.

Select the remote devices you want to update.



The tables lists only those devices which are suitable for the update.

The remote devices are processed sequentially. If an update process fails, the entire process is aborted. An update process for a remote device consists of three parts:

Upload firmware

The firmware is copied to the remote device. It is checked whether the copy was transferred correctly.



Please bear in mind that the duration of the copy process depends on the available bandwidth

Start of the installation process

The remote installation process is started and takes between 3 and 10 minutes, depending on the hardware and version. During this time, the remote device is not available.



Make sure that nobody in the remote office switches off the device during this stage. The device might be damaged irreparably.

Waiting for the results of the installation.

The installation is considered to have failed if the remote device cannot be reached after 10 minutes or the new firmware has not been installed.

12.9 License

License number (Support IP)

This is the software license number of your device.

Hardware ID

A SX-GATE license key always corresponds to one specific machine. This ID identifies your SX-GATE hardware.

Maximum number of users

When the maximum number of users has been added, you will not be able to add any further users. If required, please purchase additional user licenses.

Activate license key

Here you install the different SX-GATE licenses.

SX-GATE license key

Enter license key

Please enter the license key

Here you can find the license key of your SX-GATE. Among others this key controls the number of users and the available options. If for instance you purchase additional users, you will receive a new license key which must be entered here.



A SX-GATE license key consists of exactly 29 characters. When entering the new key, please take care of ambiguous characters (e.g. O or 0). If you received the new key via email, use "Copy" and "Paste" to enter it.

12.10 Shutdown / Reboot

Please choose

If you have to restart or switch off SX-GATE, please select the respective option.

reboot SX-GATE

This option will re-start the system. Confirm by clicking on "Finish" . It may take up to 5 minutes before SX-GATE is in operation again.

power off SX-GATE

If this option is selected, the system will be shut down and switched off. After confirmation with "Finish", this can take up to 2 minutes.

13 Wizards

For the basic configuration of your SX-GATE you should make use of the wizards offered in mainmenu "Wizards". Step by step you setup the main functionalities like networking or the mail system in a fast and easy way.

13.1 LAN integration

IP address of SX-GATE

SX-GATE requires a unique, fixed IP address in your internal network. Do not allocate an address which is already in use by an other device in your LAN (Local Area Network). If in doubt, please ask the person in charge of your network.

You cannot use an arbitrary IP address range for your LAN. According to Internet standard RFC 1918, local networks (called private subnets) should use IP addresses starting with 10., 172.16 through 172.31 or 192.168. All other IP address ranges are either reserved or already assigned to companies and organisations. So, please do not use network addresses outside the private subnet ranges. If you decide to use e.g. 192.168.0.0 with netmask 255.255.255.0, you can assign 254 IP addresses from the range 192.168.0.1 through 192.168.0.254 to computers in your LAN.

You might have to change the IP configuration of all those servers and workstations in your LAN which require direct access to the Internet. The IP address of SX-GATE has to be configured as gateway and as name server (DNS) on these computers. Please make sure that the IP address of SX-GATE is the only entry configured there and remove any additional entries. Internet access with a web browser and the email communication should make use of the SX-GATE web proxy and mail functions. There's no need to configure gateway and DNS on a workstation if these services are sufficient. However be aware that you cannot use the hostname of SX-GATE if you want to address it from a workstation without appropriate DNS setup. You have to address SX-GATE by its IP instead.

Using a DHCP server simplifies the IP configuration of the workstations. The IP addresses for gateway (router) and name server (DNS) will be configured on the DHCP server only. The workstations can then be configured to receive the IP configuration automatically from the DHCP server. Later in this wizard you will be asked if you plan to use SX-GATE as your local DHCP server.

LAN IP address of SX-GATE

In your local network, SX-GATE can be addressed by the IP you enter here. The IP must fit to the network you configured on the other computers in your LAN.

LAN netmask

Enter the netmask fitting to your local network into this field. All computers in this network must have the same netmask configured.

Name of SX-GATE

Assign the FQDN (fully qualified domain name) of SX-GATE. The FQDN consists of the hostname and the corresponding domain. Particularly the domain is used as default for many configuration options on SX-GATE.

Specify e.g. "gateway" as hostname and "example.com" as domain. Now SX-GATE is accessible with the Internet browser in the internal LAN using the address

"https://gateway.example.com"

- presumed the DNS of the workstation is configured accordingly.

Hostname of SX-GATE

Enter the hostname of SX-GATE here. It may contain only the letters "a" through "z", digits and dashes.

Domain

Insert the domainname for SX-GATE here. If your company already reserved or connected an Internet domain you should use this one. Otherwise enter a name which is guaranteed not used in the Internet (e.g. "company.internal") to avoid domain conflicts.



The domain mentioned here has nothing to do with a Windows NT domain.

Intranet IP addresses**Internal IP networks**

Some services of SX-GATE have to differentiate whether the origin of a request is the Internet or the internal LAN. Here you can specify which networks are to be attributed to the LAN. The SX-GATE mail server for example offers specific functions only for client from the local networks stated here. Other services like the web proxy refuse access to IP addresses that are outside of the address ranges as stated here.

This setting does not interact with the firewall policy in any way.

SX-GATE DHCP server

Activate DHCP server

The SX-GATE DHCP service can centrally control and automate the IP address allocation and the IP configuration of the workstations in your local network. SX-GATE can carry out this function in your LAN if the DHCP service is not already offered by another server.

If a DHCP server already exists in your LAN, the SX-GATE DHCP server can be configured as a secondary DHCP server. In this way the DHCP service is still available in your local network even when the primary DHCP server is offline.

Activate DHCP server

- yes
Please read on at [Backup DHCP server](#) (p. 210)
- no
Please read on at [Save the changes](#) (p. 211)
- as relay
Please read on at [Save the changes](#) (p. 211)

Backup DHCP server

Use SX-GATE as a secondary DHCP server

Activate this option if you want to use SX-GATE as secondary DHCP-server.



If you unnecessarily configure the DHCP server as a secondary, the start up time of workstations will be longer. If more than one primary DHCP server is active, the server that replies faster will assign the IP configuration. Depending on the behaviour of the servers, disruptions or interferences may occur.

In contrast to a primary DHCP server, SX-GATE as secondary will not reply immediately when a device asks for an IP address. SX-GATE will only reply when a few seconds have passed and the device continues to demand the IP address. In this case SX-GATE assumes that the primary DHCP server is not available and will thus assign an IP address.



Please make sure that the IP address ranges assigned by the primary and the secondary DHCP servers do not overlap. As the primary server is not aware of the existence of a secondary, overlapping may result in a conflict.

DHCP IP address pool

Address ranges of DHCP IP pool

Here you can specify the IP address ranges which will be assigned dynamically to network devices. Make sure that the ranges do not include addresses which have been assigned statically to a network device.



The address ranges you specify here must be part of the same IP subnet as the IP you assigned to SX-GATE at the beginning of this wizard.



The address ranges will automatically fit the SX-GATE IP if you use a special syntax. Simply set the network part of the address to "0". If e.g. the network matching SX-GATE's IP is "192.168.0.0/24", the entry "0.0.0.100-0.0.0.199" is in fact "192.168.0.100-192.168.0.199".

You should allocate fixed addresses to all network devices offering services in your local network (e.g. servers, network printers, routers and switches). This ensures that these services are always available at the same IP address. Using the DHCP service is mainly recommended for the configuration of workstations or mobile computers. These are added, exchanged or removed more frequently.

Make sure that you specify enough dynamically assignable IP addresses. If all addresses are assigned, any additional network device won't be able to connect to your local IP network.

Save the changes

Yet no changes have been made to the system configuration of SX-GATE. Press "Finish" to apply the changes you made or "Cancel" to dismiss them.



If you altered the IP address of SX-GATE, it will no longer respond to the old address after you pressed the "Finish" button. However after a few seconds SX-GATE will be available at the new address. In case the new IP address is part of an other IP subnet you might have to re-configure your workstation before you can contact SX-GATE at the new IP address.

13.2 Internet access

Type of Internet connection

What type of Internet connection do you have

There are various types of Internet connection. The wizard will help you if you are connected to one of the following:

DSL dial-up link with PPP-over-Ethernet/PPPoE (via DSL modem or router in modem mode)

This is a DSL link which is established using a DSL modem. SX-GATE talks to the modem using the PPP-over-Ethernet protocol and controls the link.

Via Router (enter SX-GATE's static Internet IP)

SX-GATE is situated behind an upstream router which in turn is connected with the Internet using any technology.

If you insert the SX-GATE between an existing router and its LAN, please make sure that you configure an IP network between router and SX-GATE which is different from the IP network used in the LAN. You will probably have to re-configure the router. As an alternative you can use the bridge mode.



Never configure IP addresses from the LAN IP network for the connection to the router.

Internet IP via DHCP (cable modem or router)

With this option SX-GATE will be assigned an Internet IP via DHCP. This method is typically used to connect with a cable Internet link. In this case SX-GATE is connected to a cable modem.

It is also possible that an upstream router assigns an IP via DHCP. However we recommend to manually configure a static IP instead.

SX-GATE as a bridge between router and LAN (transparent firewall; recommended for simple networks only)

Connects router and LAN with a bridge.



Choose this option only for simple networks which don't require routing (i.e. no VPN, no internal routers, no additional interfaces which are not part of the bridge). Otherwise the firewall configuration will quickly become complex and thus error-prone.

SX-GATE as a server in LAN or DMZ (network connectivity via eth0 only)

If SX-GATE is not used as a router and Internet gateway but as a server (e.g. proxy, mail or VPN server), this setting should be the right choice. SX-GATE must be connected to the Internet router via LAN interface eth0.

What type of Internet connection do you have

- <Please select>
Please read on at [Type of Internet connection](#) (p. 213)
- DSL dial-up link with PPP-over-Ethernet/PPPoE (via DSL modem or router in modem mode)
Please read on at [ADSL parameters](#) (p. 214)
- Via Router (enter SX-GATE's static Internet IP)
Please read on at [Internet IP address](#) (p. 214)
- Internet IP via DHCP (cable modem or router)
Please read on at [Automatic IP via DHCP](#) (p. 216)
- SX-GATE as a bridge between router and LAN (transparent firewall; recommended for simple networks only)
Please read on at [IP configuration of bridge](#) (p. 216)
- SX-GATE as a server in LAN or DMZ (network connectivity via eth0 only)
Please read on at [IP configuration](#) (p. 216)

ADSL parameters

Please insert username (login) and password required for the dial-in connection to your provider here. If you received different credentials (e.g. also for email and webhosting), please supply the credentials for DSL dial-up. The correct VLAN configuration is crucial. It depends on the provider and the modem.

VLAN ID

Enter a VLAN ID for DSL Internet connections using VLAN. Then tagged VLAN packets are used to connect with the DSL modem. Please ask your provider for the correct VLAN ID.

Local IP address

You can either accept a dynamic IP assigned by the peer or specify an IP address.

Please read on at [Use automatic DNS](#)

Internet IP address

Use the second network card of SX-GATE (eth1) to establish the Internet connection via router. This network card may not be used for any other purpose.

Connect the ethernet port of the external router directly with SX-GATE. Alternatively, you can connect SX-GATE and the router via a dedicated switch. You may connect only those devices to the switch which have to be part of the transfer network between SX-GATE and the router.



Please note that the ip addresses entered here may not be part of the address range configured for your LAN. If you use for instance the subnet 192.168.0.0 with a netmask of 255.255.255.0 for your LAN, the addresses entered here may not begin with 192.168.0 as well.



Any device connected to the transfer network between SX-GATE and the router will not be protected by the SX-GATE firewall towards the Internet. Put these devices into a Demilitarized Zone (DMZ) instead. You can configure a DMZ with SX-GATE.

Internet IP address of SX-GATE

Enter the external IP address of SX-GATE here. If you received a range of IP addresses from your provider choose one address. Note that the first and the last IP address of an IP subnet are reserved. The first address (network address) always ends with an even number while the last address (broadcast address) ends with an odd number. Please check if the address range the provider gave you includes these reserved addresses or not. Of course you may not assign the same IP address to SX-GATE which is used by the router.



The IP address of the SX-GATE external interface must not be part of the IP range used for your LAN. In no case you may use the LAN IP of SX-GATE also as its external IP.

IP address of Internet router (gateway)

Enter the (internal) IP address of the router here. Check the information you received from the provider. It might have been named "gateway".

Netmask of transfer network

Please enter here the corresponding network mask. If the netmask that you have received from your provider is 255.255.255.252, there is no way that you can connect any more devices to the transfer network. Although it is possible to link other devices (e.g. web server, mail server, ...) to the transfer network when using different network masks this is not recommended. Usually these devices can be addressed directly

from the Internet and are unprotected. We recommend to put these devices into a Demilitarized Zone (DMZ) which can be configured with SX-GATE.

Please read on at [DNS server of ISP](#)

Automatic IP via DHCP

In this mode the IP configuration is done automatically.

Please read on at [Use automatic DNS](#)

IP configuration of bridge

IP address of the router

Enter the (internal) IP address of the router here. Check the information you received from the provider. It might have been named "gateway".

Please read on at [DNS server of ISP](#)

IP configuration

IP address of the Internet router

Enter the (internal) IP address of the router here. Check the information you received from the provider. It might have been named "gateway".

Please read on at [DNS server of ISP](#)

Use automatic DNS

Use automatically assigned DNS servers

Enable this option to use the name servers your provider assigned to SX-GATE to resolve host names.

Use automatically assigned DNS servers

- yes (recommended)

Please read on at [Use upstream proxy server](#) (p. 217)

- no

Please read on at [DNS server of ISP](#) (p. 217)

DNS server of ISP

Forward DNS queries to name servers

Enter the IP addresses of your provider's name servers (DNS) here. DNS is required to map the name of a web server or the domain of a mail address to the IP address of the corresponding web- or mail server. You can receive these addresses from your provider. If multiple servers are available they will be asked in order of their speed of response.



Please specify only those DNS servers that may be used from your Internet access point. If none of the configured DNS servers are accessible then most of the Internet services will fail.

If you don't know which name server to use, you can make use of the so-called "root servers". This operation mode will be activated if you don't specify any DNS server. You should be aware that the response time may be significantly longer in this case, however.

Use upstream proxy server

Use the proxy server of your ISP

The web proxy of SX-GATE can forward requests to an upstream proxy server. Otherwise the web proxy of SX-GATE will always connect directly to the requested destination address.



In some cases it may be mandatory to use the proxy due to a regulation.

Use the proxy server of your ISP

- yes
Please read on at [Upstream proxy server](#) (p. 218)
- no
Please read on at [Use SMTP relay server](#) (p. 218)

Upstream proxy server

Hostname or ip address of proxy server

Ask the operator for the name or IP of the proxy server.

Port

You have to specify the portnumber of the proxy server. You should have received it along with its address. Typically one of the numbers 80, 3128 or 8080 is used.

Force use of ISP proxy

If SX-GATE is situated behind a firewall, which does not allow direct communication with the Internet, it may be necessary to handle all requests using the proxy server. Please activate the option in this case.

Otherwise SX-GATE assumes a caching proxy used to speed up the Internet connection. In this case the SX-GATE web proxy optimises the forwarding of requests. SX-GATE will forward only those requests to the upstream proxy which might be cached there. For requests that may not be cached anyway, a direct connection to the target web server will be established instead. As an example files may not be cached if user authentication is necessary to download them. Also encrypted (https) connections may not be cached.

Use SMTP relay server

Send outgoing emails via mail relay server of ISP

Outgoing emails can either be sent directly to the email server of the recipient or via the mail relay server of your provider. The job of a relay server is to accept emails from mail clients or other mail servers and forward them to the mail server of the recipient or maybe an other relay server.

Use a relay server for Internet links with a dynamic IP. If you have a static IP you may consider direct delivery, however you must make sure that a suitable DNS reverse lookup entry has been configured for the IP.

Send outgoing emails via mail relay server of ISP

- yes
Please read on at [SMTP relay server](#) (p. 219)
- via Microsoft 365 using OAUTH2
Please read on at [Microsoft 365 OAUTH2](#) (p. 219)
- no
Please read on at [Enable NTP timeserver](#) (p. 221)

SMTP relay server

It is highly recommended to use the relay server offered by your Internet access provider. Usually no user authentication is necessary in this case, so leave the text fields for the credential empty.

Hostname or IP address or relay server

Enter the name or the IP address of the relay server of your provider. All email traffic destined for users in the Internet will then be forwarded to this server. The provider relay will then assure that the mail reaches the mail server of the recipient. If the relay server encounters problems when forwarding the mail, it will either retry the delivery or notify the sender that the mail was undeliverable.

SMTP-Auth login

If the provider operating the relay server and the provider operating your Internet connection are different providers, you usually have to authenticate when using the relay server. With authentication the provider prevents abuse of the relay server by SPAM mail senders. The standardised authentication method is called SMTP-Auth.

If in doubt, ask your provider if you have to authenticate when using his relay server, if the relay server supports SMTP-Auth and which credentials you have to use to login.



According to the SMTP-Auth standard, SMTP-Auth is a "hop to hop" authentication. This implies that only the direct communication partner (SX-GATE in this case) will authenticate at the relay server. For this reason, SX-GATE will always use the same login and password with SMTP-Auth. It is not possible to use different credentials depending on the actual sender of the email.

SMTP-Auth password

Enter the SMTP-Auth password here.

Please read on at [Enable NTP timeserver](#)

Microsoft 365 OAUTH2

For sending outbound emails via a Microsoft 365 account using the OAuth2 authentication scheme, SX-GATE uses the "client credentials flow". You need to create an application with an application password for SX-GATE in Entra ID (formerly Azure Active Directory). SMTP Authentication permission has to be granted to the application. SX-GATE uses a single user account for sending mails, so all senders have to grant "SendAs" permission to this user. With its application ID and password, SX-GATE will

then be able to get a short-lived access token, which in turn allows sending mails via the configured user account.

The steps in detail:

Register application

Login to Microsoft Azure with an administrator account (<https://portal.azure.com>).

Select "Microsoft Entra ID", then "Manage > App registrations".

Click "New registration" and assign a name of your choice. Leave the other settings unchanged and click "Register".

In the menu on the left, click "Certificates & secrets" and then "Client secrets". Issue a new application password by clicking "New client secret" and "Add".

Copy the generated password in column "Value" immediately by clicking the copy icon behind the password. It will no longer be possible to copy the password at a later point in time. Paste the password into the SX-GATE mail server's oauth2 configuration or temporarily store it in a safe place to paste it later into SX-GATE.

Now click "Manage > API permissions" in the menu on the left, then "Add a permission". Select "APIs my organization uses" and type "Office" into the search field. Select "Office 365 Exchange Online" and click "Application permissions". Open the section "SMTP" and check "SMTP.SendAsApp". Close the window with "Add permissions". Finally click "Grant admin consent for DOMAINNAME".

Now click "Overview" in the menu on the left and copy the values "Application (client) ID" and "Directory (tenant) ID" into the oauth2 configuration of the SX-GATE mail server or store the values to configure SX-GATE later.

Leave the App registration by clicking "Home" in the upper left corner.

Select "Microsoft Entra ID" again, but this time choose "Manage > Enterprise Applications". Copy the "Object ID" of the application you just registered for later use. The "Application ID" is also displayed here again. You will need both values in a moment when configuring Exchange.

Grant access in Exchange

SX-GATE uses just one single account for sending mails. After you decided, which account to use, you should check in "Microsoft 365 admin center" (<https://admin.microsoft.com>), if "Authenticated SMTP" has been granted for this account. Click on the account below "Users > Active Users", then "Mail" and check the permissions below "Email apps".

Now step through all other users and groups and grant "SendAs" permission for the account used to send mails.

Configure credentials in SX-GATE

If you haven't done so already, paste the values you copied earlier into the OAuth2 configuration of the SX-GATE mail client.

Enter the account you picked for sending mails as "SMTP-Auth login". It is not necessary to enter the corresponding password, as SX-GATE can login with its application password.

Hostname or IP address or relay server

For Microsoft 365 you will usually enter smtp.office365.com here.

Tenant

Enter your Entra ID tenant name or ID.

OAuth2 client ID

Enter the client ID you have registered in Entra ID for the SX-GATE mail server.

Secret OAuth2 client key

Enter the application password you have generated in the Azure Active Directory for the SX-GATE mail server.



The Azure AD application password has a limited validity period. Please remember to issue a new application password in time and copy it to SX-GATE.

Enable NTP timeserver***Synchronize system time with timeservers and publish it locally***

Use this setting to enable the NTP time server on your SX-GATE. SX-GATE will then synchronize its system time with public Internet time servers. Furthermore other systems may then use SX-GATE as their time server.

Synchronize system time with timeservers and publish it locally

- yes
Please read on at [NTP timeservers](#) (p. 221)
- no
Please read on at [Save the changes](#) (p. 221)

NTP timeservers***Hostnames or IP addresses of time servers***

Configure the time servers SX-GATE will use to synchronize its system time here.

Save the changes

Yet no changes have been made to the system configuration of SX-GATE. Press "Finish" to apply the changes you made or "Cancel" to dismiss them.

13.3 Proxy configuration

Browser setup

Browser setup method?

Either enter the browser proxy settings manually or have make the browser use Web-Proxy Auto-Discovery (WPAD) to automatically detect the browser settings. If DHCP is enabled on the workstations, the DHCP based WPAD method can be used. However only few browsers support this. The DNS based WPAD approach is often the better choice. However SX-GATE's intranet HTTP server must be running for this.

manually or centralized

Select this option if you want to configure the browsers all manually, if you want to configure a central configuration file (Proxy autoconf URL) or if you want to use Active Directory group policies.

automatically (WPAD)

By selecting this option you can configure WPAD support in SX-GATE. This allows browsers to automatically detect proxy parameters, provided this is enabled in the browser settings. Note that it is still possible to configure browsers manually (see previous option), even if WPAD is on.

Browser setup method?

- manually or centralized
Please read on at [Manual or centralized browser configuration](#) (p. 222)
- automatically (WPAD)
Please read on at [Web-Proxy Auto-Discovery \(WPAD\)](#) (p. 223)

Manual or centralized browser configuration

Manual browser configuration

Open the browser's proxy settings dialogue. Set the proxy to SX-GATE's IP, port "8080". Use these values for all protocols except "SOCKS". At least for the administrator's PC it is advisable to connect to the SX-GATE administration directly and not via proxy. So please add SX-GATE's IP to the proxy bypass list.

Centralized browser configuration

In both, the browser's proxy settings and the Active Directory group policies, you can enter the address of a proxy autoconf file. SX-GATE's administration webserver provides a suitable file. Fill in the following URL if you want to use it: "http://<SX-GATE's LAN IP>:8000/proxy.pac".

Please read on at [Web proxy access](#)

Web-Proxy Auto-Discovery (WPAD)

Most browsers are able to automatically detect the web proxy configuration using Web-Proxy Auto-Discovery (WPAD). The browser needs to download a config file from a web server. Publishing via DHCP is one of the methods WPAD specifies to determine the URL of this config file. Yet only Microsoft Internet Explorer supports this distribution method, provided that DHCP is enabled. An alternative DNS based solution is supported by all major browsers and does not require DHCP.



Make sure that automatic proxy detection is enabled in the browsers.

Enable WPAD via DHCP

Yet only Microsoft's Internet Explorer supports the DHCP based approach. It's also required, that the workstation itself uses SX-GATE as its DHCP server.



If a third-party DHCP server is used, the WPAD URL has to be deployed on that server. Enter the URL "http://<SX-GATE's LAN IP>:8000/proxy.pac" if you want to use SX-GATE's predefined Proxy Autoconf file.

Enable WPAD via DNS

Here you can enable a DNS based method. The browser tries to download the file "wpad.dat" from a server named "wpad.<LOCAL DOMAIN>".

Specify the network domain configured on your workstations here. SX-GATE will then set up appropriate DNS entries in its name server and instruct the intranet web server to redirect requests for "wpad.dat" to

"http://<SX-GATE's LAN-IP>:8000/proxy.pac"

. This is a predefined config file which instructs the browsers to use SX-GATE as web proxy.



If the workstations are in different subdomains (e.g. "sales.example.com" and "management.example.com"), enter the domain part they have in common ("example.com").

Web proxy access

SX-GATE's web proxy will provide secured browser access to the Internet. In addition to HTTP and HTTPS, the proxy also supports browser access to FTP servers. The web proxy can not be used by true FTP clients. For these, SX-GATE provides an FTP proxy which can be enabled later on in this wizard.

Access for browsers with configured web proxy

The proxy should be configured in the browsers whenever possible. Only then proxy authentication is an option. Users will also be able to access HTTP servers running on non-standard ports without a hassle.

Proxy authentication

Please select if and how users have to authenticate for using the proxy.

without user authentication

This mode grants proxy access without authentication. However it will not be possible to configure user specific settings.

manual user authentication

Select this option if you want the users to authenticate themselves by typing a login and password before they get Internet access. Add the required accounts in the user administration. The users have to become members of group "system-proxy" to be accepted by the proxy.

automatic user authentication (NTLM)

Here the user's current Windows domain authentication is used to automatically authorize proxy access. The users will not be prompted for a login and password, unless the browser doesn't support this authentication method. In this case the credentials of an authorized Windows user have to be supplied.



With NTLM authentication, the SX-GATE group "system-proxy" is not considered for authorization. So it is not necessary to create user accounts for this purpose.

Proxy authentication

- without user authentication
Please read on at [Web proxy filters](#) (p. 226)
- manual user authentication
Please read on at [Web proxy filters](#) (p. 226)
- Proxy authentication by LDAP server
Please read on at [Web proxy filters](#) (p. 226)
- Proxy authentication by Windows (obsolete)
Please read on at [Web proxy filters](#) (p. 226)

Access for browsers without proxy configuration (transparent proxy)

It is not always possible or desired to configure the proxy settings of browsers. With the following options, SX-GATE's web proxy and firewall will be configured to redirect HTTP and HTTPS connections with the standard destination ports 80 and 443 to the web proxy. The wizard will modify the firewall settings of ethernet interface "eth0" only. The proxy can be used by browsers with and without proxy configuration at the same time.



For transparent connections the proxy will never require authentication.



For browsers without proxy configuration some particularities have to be considered. In the network configuration of the respective workstation SX-GATE has to be configured as default gateway. Otherwise transparent access will not work. DNS is required, too. The transparent FTP proxy has to be enabled later on in this wizard if FTP access is required. Internet access with HTTP and HTTPS to non-standard ports will not be possible by default. The firewall policy would have to be modified for this.

Windows settings

ActiveDirectory server IP

Please enter the IP address of the ActiveDirectory server. If you want to use the NT4 compatibility mode, enter the NetBIOS name of your local Windows domain instead.



The NetBIOS domain name is for instance displayed below "Network Places" where it might be labeled "Workgroup". A NetBIOS domain name usually contains no dots (e.g. "EXAMPLE"). In contrast an active directory domain name is actually an Internet domain name. As such it contains at least one dot (e.g. "example.com").

Authorized users

Select which users are authorized to use the proxy.

Join Windows domain

SX-GATE needs a machine trust account in the Windows domain to be able to perform NTLM authentication. Please enter the credentials of a Windows administrator to create the account.



Once the account is created, login and password are no longer required. They will not be stored on SX-GATE.

Administrator login

Please enter the login name of a Windows administrator. If you have already created a machine trust account for SX-GATE it is not necessary to provide the credentials again. Leave the field blank. On the next screen SX-GATE will check if the account is still valid.

Web proxy filters

URL filter

For access restrictions, a categorized database of internet addresses comes along with SX-GATE. Custom address lists can be defined, too. Furthermore it is possible to deny access to certain types of files based on its names. Enable the filter with this switch.



Turn to menu "Definitions > URL filter lists" to compile lists. Then assign the lists to individual IP addresses or user groups in menu "Modules > Web proxy > URL filter".

Content filter

With this option enabled, files which are downloaded via the SX-GATE web proxy will be screened.



By default only virus scanning is enabled. For performance reasons some content types will not be scanned by default.



For virus scanning a functional virus scanner has to be installed on SX-GATE. The virusscanner licenses are not included with SX-GATE and must be purchased separately.

FTP-Proxy

Enable FTP proxy?

SX-GATE provides this proxy for access to internet FTP servers.

yes

If this option has been selected, the FTP proxy can be used by true FTP clients but not by web browsers.



Use SX-GATE's web proxy on port 8080 for non-transparent browser access to web servers.

In the settings of the FTP client, SX-GATE has to be configured as proxy with port 2121. Common names for the proxy type to select are "USER with no login" or "USER user@host:port". If it is not possible to configure a proxy type in the FTP client, the proxy can still be used. Regardless of the actual destination a connection to port 2121 of SX-GATE has to be established (e.g. "ftp 192.168.0.254 2121"). As login you have to enter the login on the remote server followed by an "@" character and the address of the destination (e.g. "login@ftp.example.com").



To use the proxy it must be configured in the FTP client or the connection must be established via port 2121 of SX-GATE.

yes, as transparent proxy

The firewall policy of ethernet interface "eth0" will be changed when selecting this option. Connections to port 21 will be redirected to the FTP proxy. Both, FTP clients and web browsers will then be able to use the proxy although the proxy has not been configured.



In the network configuration of the respective workstation SX-GATE has to be configured as default gateway. Otherwise transparent access will not work. Usually DNS is required, too.

Enable FTP proxy?

- no

Please read on at [Save the changes](#) (p. 230)

FTP proxy filter

FTP proxy virusscan

To scan for viruses in files downloaded via the FTP proxy, this option has to be enabled.



This option is without effect if no functional virus scanner is installed on SX-GATE. The virusscanner licenses are not included with SX-GATE and must be purchased separately.

FTP destinations

FTP proxy will accept connections to

Determine the accounts and FTP servers to which connections will be accepted.

specific FTP servers and accounts

Select this option to restrict FTP access on the following screen.

any FTP servers and accounts

With this setting access to any FTP server is granted. This includes anonymous as well as authenticated access.

FTP proxy will accept connections to

- any FTP servers and accounts

Please read on at [Save the changes](#) (p. 230)

FTP proxy destinations

Destinations accepted by the FTP proxy

Use this control to specify the accepted target FTP servers and its corresponding accounts. If the list is empty, the proxy will deny access to any server.

Account

Enter the login for the target FTP server here. Select "ftp (anonymous)" to grant access for anonymous FTP. Select the option above and enter the login to grant access to a specific account only. If you leave the input field empty, the FTP proxy will accept connections to any account on the FTP server.

Destination server

Fill in the name or the IP address of the target FTP server here. Do not enter anything in order to accept access to any FTP server.

Some typical example rules which may be combined to satisfy your requirements.

Anonymous access to any FTP server

Select "ftp (anonymous)" and press "Add". The rule "ftp@*" will be added.



This rule will grant access to publicly available contents but will deny access to protected areas (e.g. maintenance of private homepages).

Access to any account on a specific FTP server

Enter the server name (e.g. ftp.example.com) as "Destination server", select the topmost option "Account" but leave the input field empty. Clicking on "Add", the new entry "*@ftp.example.com" will appear.

Access to a single account on a specific FTP server

Specify the account and the server in the respective input fields and click "Add". The created rule will look like e.g. "webmaster@www.example.com".

Save the changes

Yet no changes have been made to the system configuration of SX-GATE. Press "Finish" to apply the changes you made or "Cancel" to dismiss them.

13.4 Email configuration

Configuration of the email services

Which service do you want to configure?

To configure all important aspects of the SX-GATE mail system you should begin with the option "local and internal domains". At the end of this topic you will have the possibility to continue with the other options. Especially for the start-up configuration, this ensures that you adjusted all important settings. Of course you can pick a specific option as well and modify the corresponding settings only.



The mail relay server of your provider depends on your Internet connection. Therefore this setting is configured in the wizard "Wizards > Internet access".

Select "local and internal domains" to configure the local email domains. Emails for these domains can either be forwarded to an other mail server in your LAN or they can be delivered to mailboxes on SX-GATE. You can also activate some security mechanisms like the mail virusscanner.

Security and filter mechanisms like the mail virusscanner will be activated in "mail filters".

Receiving emails from the Internet is configured with "mail reception". If SX-GATE has to poll POP servers in the Internet for incoming mails, you can specify the corresponding mailboxes here. ETRN or direct delivery by SMTP however requires changes in the firewall configuration which can be made here as well.



Finishing this wizard will activate the mail system of SX-GATE. So first you should make sure that all local user mailboxes are in place before you start to receive Internet email. Of course you can as well skip this step for now and configure "mail reception" later.

The timing of email delivery and retrieval can be adjusted with "polling and delivery schedule". You can optimise the corresponding parameters depending on the type of your Internet connection.

Which service do you want to configure?

- local and internal domains
Please read on at [Domains](#) (p. 232)
- mail filters
Please read on at [Activate SPAM filter](#) (p. 236)
- mail reception
Please read on at [Mail reception](#) (p. 241)
- polling and delivery schedule
Please read on at [Queue parameters](#) (p. 249)

Domains

SX-GATE can be responsible for multiple local and/or internal domains.

A table gives you an overview of the available objects. If multiple columns are displayed you can change the sort order by clicking the column title. If there are more than 20 entries, a navigation bar will appear below the bottom right hand corner of the table. You can switch between a grouped view or a pager. The full screen mode allows you to see all entries at the same time. Pick an entry by clicking its title in the left column. A pencil icon or a trashcan in the right column allow you to rename or delete an entry. Add new objects by clicking "New Entry" below the table on the left.

Email domain

Please enter an email domain. Mails to this domain are either going to be delivered to a local mailbox on SX-GATE or forwarded to an internal mail server.

Domain type

Deliver mail to

Select "to SX-GATE mailbox" if you want SX-GATE to be your local mail-server. Emails to all the domains that you can specify later in this wizard will then be delivered to mailboxes on SX-GATE. Users can access their emails using the SX-GATE groupware or with any mail client supporting the POP3 or the IMAP4 protocol.



To create a user mailbox on SX-GATE you have to add a user at "System > User administration > Users" and assign him to group "system-mail".

In case you already operate a mail server in your LAN and you want to keep on using it, SX-GATE can forward all emails addressed to specific domains to this internal mail server. The email communication with the Internet will benefit from the security features of SX-GATE without having to relinquish the present system. Please select "to internal mail server" to configure this scenario.

Deliver mail to

- to SX-GATE mailbox
Please read on at [Users](#) (p. 233)
- to internal mail server
Please read on at [Verify recipient](#) (p. 233)

Users

Users with mail accounts

With this control you can assign members to SX-GATE's "system-mail" group. For each member, an email account is available on SX-GATE, which consists of a mailbox and an associated mail address. Users can access their mails with POP3, IMAP4 or with the SX-GATE groupware.



To create additional users you have to change into the user administration after completing this wizard. Create the required users there and assign them to group "system-mail".

Verify recipient

Verify recipient addresses in advance

When this option is enabled, SX-GATE will contact the internal mail server for every email it receives to verify if it is willing to accept a message for the given recipients. This is checked before the actual message body is transmitted to SX-GATE, so mails to non-existent recipients will be rejected before wasting bandwidth.



This feature applies to all recipient domains SX-GATE forwards to an internal mail server.



Address verification also applies to mails SX-GATE retrieves from a POP or IMAP server. If the internal mail server refuses delivery, the mail is usually silently discarded.

using SMTP

This is the most simple approach which works with almost all mail servers. For each inbound mail SX-GATE opens an SMTP connection to the internal mail server and The received sender and recipient addresses are forwarded to it. Depending on the replies of the internal mail server, the sender is then either allowed to continue with the transmission of the email or the mail is rejected.



With this method you can even make use of any capability your internal mail server offers to reject sender addresses.



Make sure that the internal mail server immediately rejects unknown recipient addresses. The following paragraph describes how to enable this in Microsoft Exchange.

In Microsoft Exchange you will have to enable recipient filtering first. Install the Antispam Agents by searching and starting the script "Install-AntispamAgents" that you will find in a subfolder below the Exchange program folder. Since Exchange 2013 an additional HubTransport connector of type "Internet" is also required. Configure the connector to grant anonymous access. We recommend to allow access from SX-GATE's IP only. If the Windows firewall is enabled, you will also have to add a rule there to grant access to the new connector. Finally enter the port number of the new connector on SX-GATE on the next screen.

using LDAP (Active Directory)

The requested recipient addresses will be looked up in an Active Directory (attribute "proxyAddresses"). The necessary parameters for LDAP access have to be configured on the next screen.

Verify recipient addresses in advance

- disabled
Please read on at [Internal mail server](#) (p. 236)
- using SMTP
Please read on at [Verify recipients using SMTP callout](#) (p. 235)
- using LDAP (Active Directory)
Please read on at [Verify recipients using LDAP](#) (p. 235)

Verify recipients using SMTP callout

SMTP port for verification

Address verification can use a different port than the actual mail delivery.

Please read on at [Internal mail server](#)

Verify recipients using LDAP

Active Directory server

Enter the IP address of the Active Directory server which keeps the user information. Usually this is the IP of the domain controller.

LDAP searchbase

Specify the LDAP path used by SX-GATE when binding to the Active Directory. All relevant users and groups must be situated below this path in the LDAP hierarchy.

The simplest searchbase is the name of the Active Directory server (e.g. ad.example.com). But you can also enter any Distinguished Name (DN) like for example "CN=users,DC=ad,DC=example,DC=com" or "OU=internet-users,DC=ad,DC=example,DC=com".

Login for searching in Active Directory

Leave this field empty if an anonymous search is allowed in the Active-Directory or else specify the login of a user which has the required permissions (Bind DN). If the user is a member of Active Directory container "users", entering the user name (e.g. "searchuser") is sufficient. Otherwise you have to specify the complete DN here (e.g. "CN=searchuser,OU=it,DC=ad,DC=example,DC=com").



In Microsoft's SBS you have to use a DN like e.g. "cn=searchuser,OU=SBSUsers,OU=Users,OU=MyBusiness,DC=example,DC=com".

Password

If authentication is required by the Active Directory, the password goes in here.

use SSL encryption

Enabling this option will encrypt all communication between SX-GATE and Active Directory. The Active Directory Server will only accept SSL connections when a suitable certificate has been installed in the Windows Certificate Store.

Please read on at [Internal mail server](#)

Internal mail server***Forward mails to server***

Please enter the address of your internal mail server. All mails with a recipient address in the currently selected domain will not be forwarded to the Internet but delivered directly to the internal SMTP mail server. For this, please set up the corresponding user accounts and mail addresses on your internal mail server.



To avoid mail loops, the internal mail server must recognise the domain as a local domain. It must not attempt to send these emails back to the Internet.

Activate SPAM filter***SPAM filtering configuration***

A SPAM mail is an unsolicited email, usually with dubious origin. SX-GATE's SPAM filter identifies these mails and makes them easily recognizable or even discards or refuses to accept such mails.



Your selection here does not directly affect SX-GATE's configuration, only which screens you will be shown next.

SPAM filtering configuration

- configure common SPAM filter
Please read on at [Common SPAM filter](#) (p. 237)
- individual SPAM filtering per SX-GATE user mailbox
Please read on at [Individual SPAM filter](#) (p. 237)
- skip SPAM filter configuration
Please read on at [Activate virus scanner](#) (p. 240)

Individual SPAM filter

Individual SPAM filtering per SX-GATE user mailbox must be configured in the user administration by clicking on each account separately.

Please read on at [SPAM filter settings](#)

Common SPAM filter

To activate the SPAM filter you have to enable at least one of the thresholds. Here you activate the SPAM filter in relay mode. In this mode it examines every inbound email while passing the SX-GATE mail server. It is not possible to assign different thresholds to different users, as the mail users are not defined on SX-GATE but on the internal mail server.

The SPAM mail filter of SX-GATE classifies emails by identifying typical phrases and other attributes indicating an unsolicited email. SX-GATE contains a database of checks to perform and all matches result in a score which in turn allows filtering emails. Characteristics indicating a SPAM mail will add a value to the score while other characteristics indicating that it's not a SPAM mail will subtract a certain value. The higher the final score, the more likely it's a SPAM mail.



Emails exceeding the size of 1MB will not be classified to save system resources. However this is not a drawback, as a SPAM mail is usually very small.

A few headers will be added to each email examined by the SPAM mail filter. The header "X-Spam-Status" shows the final score (hits=...) and give the name of the matches (tests=...). This allows the recipient of the mail to check the score of any mail. The header "X-Spam-Level" will contain one "x" per scored point (e.g. "X-Spam-Level: xxx" for a score between 3.0 and 3.99). This header allows automatic sorting in the user's mail client.



Most mail clients will display only the most important headers by default. Usually the full header information is available after selecting a specific menu option.

Tag an email as SPAM when it is scored more than

If the score exceeds the threshold for tagging an email as SPAM, the subject of the mail is prefixed by the text "***** SPAM *****". Furthermore the email will contain

a brief summary of the tests leading to this score. The original email is added as an attachment.

Delivering the original email as attachment is supposed to achieve that selecting the email in the mail client will not trigger any unwanted actions. Depending on the mail client program used, the mere selection of an HTML formatted email may for example trigger the download of images from the Internet as the mail client tries to show a preview of the mail. So the sender of a SPAM mail is unnoticeably informed that the SPAM mail was opened. This will increase the value of this email address for SPAM mail senders and in turn more and more SPAM will be sent to this address.

Refuse to accept mails when score exceeds

Exceeding this threshold, SX-GATE's mail server will refuse to accept the email. The sending system in charge of a proper reaction like e.g. notifying the sender or an administrator. If you want to be sure that no requested email gets lost, you should not enable this option. Activate the threshold "Tag an email as SPAM when it is scored more than" instead and make use of the features offered by the mail client programs to sort emails based on header lines.



Emails which have been retrieved from a POP server by SX-GATE's mail client will be silently discarded if the mail server refuses delivery due to the SPAM filter. There will be no notification and it is not possible to undelete the email. The email is lost irrecoverable!



To avoid loss of important emails you should be very carefully when activating this option. You should select a value which is rather to high than to low. Please note that automatically deleting email may be subject to legal constraints or might even be prohibited by law.

SPAM filter settings

In addition to the builtin rules database the SX-GATE SPAM filter can query several Internet realtime lists. These have a notable impact on the detection ratio.



The settings on this screen apply to the global relay SPAM filter as well as to the users' personal SPAM filter. The latter must be enabled individually in the user administration of SX-GATE.



Do not activate these features when your internet connection is a rather expensive dial-up link. Depending on the actual configuration even an internal email might trigger an Internet connection. Thus the dial-up link will be online frequently which results in high expenses.

An other extremely useful extension is the Bayes filter. When enabled, the SPAM filter keeps adapting to its environment by learning the typical vocabulary used in regular emails and at the same time recognizing topics of current SPAM waves.

DNS based lists

Several blacklists are available in the Internet, which contain mail servers known to be the origin of SPAM mails. Another form of blacklists contains web server addresses that are advertised by SPAM mails (URI: URI Black Lists). Links in the message body are checked against these URI Black Lists. Finally there are also whitelists with friendly mail servers.

When analyzing an email, some of these lists can be queried. Each single hit will be rated with a rather moderate value. However when multiple lists indicate potential SPAM, it will have considerable impact on the SPAM score. The reliability of the lists depends on how the entries have been collected. Choose which level of quality will be considered.

few

Select this option if you want to include only verified SPAM sources. Particularly automatically collected lists will not be considered. URI Black Lists are active.

medium

In addition to verified SPAM sources this level will also include addresses collected automatically by SPAM traps.

many

If you choose this option, emails from known dynamic IP addresses and Korean and Chinese relay servers will be scored, too.

Enable Razor2 distributed spam filter network

This feature will calculate a fuzzy checksum of some parts of an email and send it to Razor2 servers in the Internet (TCP port 2703). Razor2 provides a database with the checksums of known SPAM. In case of a match, the SPAM score of the mail is increased. The amount depends on the reputation of those, who reported the SPAM mail to the Razor2 system.

Enable Bayes filter

If enabled, the SPAM filter autonomically learns additional characteristics of unsolicited mail (SPAM) and requested mail (HAM) while processing inbound emails. Only mails with a score of more than 10 or 0 and less are considered respectively.



At least 200 SPAM mails and 200 HAM mails have to be learned before the Bayes filter is taken into account.

Activate virus scanner

Virusscan all emails

Activate this option to check every emails passing the SX-GATE mail server for viruses. This applies to both, incoming and outgoing emails.



This function can only be used if a virus scanner has already been installed on SX-GATE. The virus scanner licenses are not included with SX-GATE and must be obtained separately.

The delivery of an email will be stopped if it contains a virus. The mail will be moved to a quarantine directory and the local administrator will be notified by mail. Depending on the type of the detected virus also the sender of the infected email will be notified (e.g. for macro viruses or the EICAR virusscanner testfile). Only the administrator can access the quarantine directory. If there was no access to a quarantined email for 10 days it will be deleted automatically.

Activate attachment filter

Attachment filter

Email attachments can be filtered by SX-GATE based on the filename extension. We recommend to enable the attachment filter as it can enhance the virus protection, even if you are already using virusscanners. Usually a virusscanner can detect a virus only if its signature is already known. Filtering attachments with filename extensions often used by viruses can defang a virus which is yet unknown to the virusscanner. You could also activate this component to enforce local policies which deny sending or receiving emails in certain file formats.

incoming and outgoing mails

While inbound emails are usually quarantined, outbound emails with unwanted attachments will always be rejected.

Attachment filter

- <disabled>
Please read on at [Save the changes](#) (p. 241)
- incoming mails only
Please read on at [Dangerous attachments](#) (p. 241)
- incoming and outgoing mails
Please read on at [Dangerous attachments](#) (p. 241)

Dangerous attachments

Filter attachments with these file extension or MIME types

If the filename of an attachment matches one of the extensions listed here or if the "Content-Type" header of an attachment matches a MIME type from the list, the attachment will be objected. The email will either be rejected, retained as a whole or the unwanted attachments will be replaced with a warning message before the modified email is delivered to its recipients.

The administrator or any user who is allowed to access menu "Monitoring > Mail server" can retrieve quarantined attachments or forward retained emails. They will be deleted automatically after the "Storage time" configured in menu "Modules > Mail Server > SPAM/Virus/Malware" on tab "MIME filter" has been reached.

You can specify an extension as ext, .ext or *.ext. All three formats are equivalent. The comparison is case-insensitive.

You may also add MIME types like e.g. "application/zip" to the list. An asterisk serves as a placeholder (e.g. "application/*").

Save the changes

Yet no changes have been made to the system configuration of SX-GATE. Press "Finish" to apply the changes you made or "Cancel" to dismiss them.

Mail reception

How does SX-GATE receive emails from the Internet

The common way to retrieve incoming emails is by collecting them from a POP server. If SX-GATE is connected to the Internet using a dial-up line with fixed IP address, the ETRN protocol might be used as well. On a leased line, SX-GATE can be addressed

anytime by any mail server in the Internet. In these cases you might receive incoming emails directly with the SMTP protocol. If in doubt, please ask your provider how you receive incoming emails.

How does SX-GATE receive emails from the Internet

- by polling a POP or ETRN server
Please read on at [Servers](#) (p. 243)
- direct SMTP delivery
Please read on at [Firewall access for SMTP](#) (p. 242)

Firewall access for SMTP

SMTP access to SX-GATE on interface ...

Accepting SMTP connections from the Internet usually requires a modification of the firewall policy. If no modification is necessary, an appropriate message will be shown. Else you can define firewall rules here. If there are no rules in the list, no inbound SMTP connections will be accepted.



This wizard will check and configure the firewall policy of the current Internet interface only. Depending on the firewall configuration of other interfaces, it might be necessary to change the firewall policy of these interfaces as well.

Here you can define firewall rules granting access to the SMTP server either only for specific IP addresses or for any Internet IP address.

If DNS lists the Internet IP address of SX-GATE as Mail-Exchanger for your domain, any mail server in the Internet will send email for your domain directly to SX-GATE. Hence you should choose "*" (any)" as "Internet source IP" and add the firewall rule. This will grant SMTP access independent of the source IP. If you are not sure about the actual DNS entry, you can check it by sending a suitable DNS query. If in doubt, please ask your provider.

If the only way you receive emails is by ETRN, the source of every incoming SMTP connection will be the IP address of the ETRN server. Also if every emails for you domain will be delivered to the mail server of your provider first, which then forwards the mail to SX-GATE, the source IP of every incoming SMTP connection will always be the same - namely the IP address of the provider's SMTP server. In these cases you should specify the appropriate IP address and select the corresponding option when adding a firewall rule. This will ensure that only those servers can establish a SMTP connection to SX-GATE who really have to.

Save the changes

Yet no changes have been made to the system configuration of SX-GATE. Press "Finish" to apply the changes you made or "Cancel" to dismiss them.

Servers

SX-GATE can poll mails from multiple POP3, IMAP4 or ETRN servers.

A table gives you an overview of the available objects. If multiple columns are displayed you can change the sort order by clicking the column title. If there are more than 20 entries, a navigation bar will appear below the bottom right hand corner of the table. You can switch between a grouped view or a pager. The full screen mode allows you to see all entries at the same time. Pick an entry by clicking its title in the left column. A pencil icon or a trashcan in the right column allow you to rename or delete an entry. Add new objects by clicking "New Entry" below the table on the left.

Poll a POP or ETRN Server

Enter the hostname or the IP address of the new POP or ETRN server here. Ask your provider if you do not know what to enter.

Server type

Protocol used to access this server

Please select the protocol used to access this server. Ask your provider for the correct setting.

The most commonly used way to retrieve emails is by using the POP3 protocol. With POP3, emails are kept in mailboxes that can be accessed with a username and a password. You can retrieve emails from a mailbox at the provider and deliver it to a specific local user or group (single-drop). An other possibility is to retrieve the emails from a mailbox and have SX-GATE deliver it to the recipient deduced from the headers of the mail (multi-drop).

APOP is similar to POP3, except for a different way to authenticate.

IMAP may be used instead of POP3 if the POP server uses very short connection idle timeouts.

To retrieve mail from Microsoft 365 mailboxes with POP3 or IMAP, a special authentication method is required. Select one of the OAUTH2 options in this case.

ETRN is a command of the ESMTP protocol. It might be used if SX-GATE is connected to the Internet with a dial-up line using a fixed IP address. The mail server of the provider tries to forward incoming emails directly to this fixed IP address. If SX-GATE is

unavailable, as e.g. the dial-up line is offline, the mail server of the provider keeps the mail in a queue. Just after the dial-up line connects again, SX-GATE used the ETRN command to trigger a new delivery attempt of all waiting mails.

Protocol used to access this server

- POP3
Please read on at [Single-drop accounts](#) (p. 246)
- Microsoft 365 POP3 (OAUTH2)
Please read on at [OAuth2](#) (p. 244)
- APOP
Please read on at [Single-drop accounts](#) (p. 246)
- IMAP
Please read on at [Single-drop accounts](#) (p. 246)
- Microsoft 365 IMAP (OAUTH2)
Please read on at [OAuth2](#) (p. 244)
- ETRN (ESMTP)
Please read on at [ETRN domains](#) (p. 248)

OAuth2

In order to retrieve mails from a Microsoft 365 account, it is necessary to use the OAuth2 authentication scheme. SX-GATE uses the "client credentials flow", i.e. comparable to a user account, an application with an application password is created for the SX-GATE mail client in Entra ID (formerly Azure Active Directory). POP3 or IMAP4 access permissions are granted to the application. Finally, using the Exchange Management Shell, the application has to be granted access to the required mailboxes. With its application ID and password, SX-GATE will then be able to get a short-lived access token, which in turn grants access to all of the configured mailboxes.

The steps in detail:

Register application

Login to Microsoft Azure with an administrator account (<https://portal.azure.com>).

Select "Microsoft Entra ID", then "Manage > App registrations".

Click "New registration" and assign a name of your choice. Leave the other settings unchanged and click "Register".

In the menu on the left, click "Certificates & secrets" and then "Client secrets". Issue a new application password by clicking "New client secret" and "Add".

Copy the generated password in column "Value" immediately by clicking the copy icon behind the password. It will no longer be possible to copy the password at a later point in time. Paste the password into the SX-GATE mail client's oauth2 configuration or temporarily store it in a safe place to paste it later into SX-GATE.

Now click "Manage > API permissions" in the menu on the left, then "Add a permission". Select "APIs my organization uses" and type "Office" into the search field. Select "Office 365 Exchange Online" and click "Application permissions". Open the sections "IMAP" and/or "POP" and check the respective "AccessAsApp"

permission. Close the window with "Add permissions". Finally click "Grant admin consent for DOMAINNAME".

Now click "Overview" in the menu on the left and copy the values "Application (client) ID" and "Directory (tenant) ID" into the oauth2 configuration of the SX-GATE mail client or store the values to configure SX-GATE later.

Leave the App registration by clicking "Home" in the upper left corner.

Select "Microsoft Entra ID" again, but this time choose "Manage > Enterprise Applications". Copy the "Object ID" of the application you just registered for later use. The "Application ID" is also displayed here again. You will need both values in a moment when configuring Exchange.

Grant access in Exchange

First you should check in the "Microsoft 365 admin center" (<https://admin.microsoft.com>), if POP3 or IMAP4 access has been granted for the required users. Click each user below "Users > Active Users", then "Mail" and check the permissions below "Email apps".

Now connect with the Exchange Management-Shell. Open the Powershell and if necessary, install the ExchangeOnlineManagement module. You might have to import the module with "Import-Module ExchangeOnlineManagement".

Open the connection with "Connect-ExchangeOnline -UserPrincipalName ADMINUSER". To connect via proxy, store the proxy settings in a variable beforehand, e.g. with "\$proxyoptions = New-PSSessionOption -ProxyAccessType ieconfig". Then append the option "-PSSessionOption \$proxyoptions" to the connect command.

Register the application once using the command "New-ServicePrincipal -AppId APPLICATION_ID -ServiceId OBJECT_ID". Replace APPLICATION_ID and OBJECT_ID with the values you copied earlier.

If the application has already been registered, the command "Get-ServicePrincipal" will show you its "Object ID" (here it is called "ServiceId").

Now grant access for this ID to each user mailbox SX-GATE has to connect with: "Add-MailboxPermission -Identity USER -User OBJECT_ID -AccessRights FullAccess". Replace USER with the user's email address.

Configure credentials in SX-GATE

If you haven't done so already, paste the values you copied earlier into the OAuth2 configuration of the SX-GATE mail client.

While adding the individual user mailboxes, SX-GATE will not ask for the users' passwords, as SX-GATE can login to all the users' mailboxes with its application password.

Tenant

Enter your Entra ID tenant name or ID.

OAuth2 client ID

Enter the client ID you have registered in Entra ID for the SX-GATE mail client.

Secret OAuth2 client key

Enter the application password you have generated in the Azure Active Directory for the SX-GATE mail client.



The Azure AD application password has a limited validity period. Please remember to issue a new application password in time and copy it to SX-GATE.

Single-drop accounts***Mirrored mailboxes (single-drop)***

Subscribe for a new mailbox of the POP server or delete a subscription by clicking on the "Add" or "Remove" button respectively.



This list will show single-drop accounts only. Multi-drop accounts are not visible here. You can change the multi-drop settings later in this wizard.

You have to specify a username and a password to be able to access a mailbox on a POP server. Ask your provider for the required values.

For each mailbox you have to specify the local recipient as well as the corresponding local domain. All emails retrieved from the POP mailbox at the provider will be delivered to this address by SMTP, hence the name single-drop. However this address does not have to be the address of a user. Of course you can address a mail distribution list (group) as well.

Configure multi-drop mailbox***Configure multi-drop mailbox***

The disadvantage of single-drop mailboxes is the double administration expense of the accounts. These must be created locally on SX-GATE as well as with the provider. Multi-drop mailboxes might simplify administration.

Most providers support POP3 multi-drop accounts. In a multi-drop mailbox emails addressed to a whole domain (or even multiple domains) are collected. It is usually possible to mix single-drop and multi-drop account for a domain. Emails addressed to specific users are kept in single-drop accounts, whereas emails to other recipients are delivered to the multi-drop account.

It may make sense to treat a multi-drop account like a single-drop account when retrieving mails. All mails from the multi-drop account at the provider will then be delivered locally to a specific account or to a specific group. Typically for this scenario, a single-drop account exists for every employee on the mail server of the provider and a multi-drop account exists for all unknown addresses. The contents of the multi-drop account is then delivered to a certain local user or distributor (e.g. info).

If SX-GATE retrieves emails in multi-drop mode, an attempt will be made to re-construct the original recipient from the contents of each email. If this is possible, the mail will be delivered locally to the recognised recipient. Introducing a new mail address or distributor requires no intervention from the provider - the account will be managed purely on a local basis.



It is not always possible to reconstruct the actual mail recipient. In some cases the recipient of an email is transmitted in the SMTP envelope only! Especially the following cases may pose problems:

- Mails that were sent as blind carbon copies (Bcc).
- Mails addressed to multiple recipients without specifying the recipients one-by-one but rather through a distribution list (particularly relevant with mailing lists).
- Certain provider mail servers which do not always leave the required information in mails.

If the recipient of an email from a multi-drop account cannot be reconstructed, the mail will always be delivered to the administrator.

If you encounter problems with the multi-drop account, you should combine both multi-drop and single-drop. Newly set-up addresses can then be put into operation instantly by using the multi-drop accounts. If problems occur create a single-drop account with your provider for the problematic users.

Configure multi-drop mailbox

- yes
Please read on at [Multi-drop accounts](#) (p. 248)
- no
Please read on at [Save the changes](#) (p. 243)

Multi-drop accounts

Multi-drop mailboxes

Subscribe for a new mailbox of the POP server or delete a subscription by clicking on the "Add" or "Remove" button respectively. This list will show multi-drop accounts only.

You have to specify a username and a password to be able to access a mailbox on a POP server. Ask your provider for the required values.

For each mailbox you have to specify the corresponding local domain. When retrieving emails from the mailboxes listed here, an attempt will be made to reconstruct the original recipient from the contents of the email. The email will then be delivered to the recognised recipient. If SX-GATE was not able to deduce the original recipient, the email will be delivered to the administrator instead.

Although it is possible to specify multiple multi-drop mailboxes per POP server, this usually doesn't make sense. In most cases only one multi-drop mailbox exists at the provider.

Multi-drop domains

To deduce the recipient search in email for these domains

To reconstruct the original recipient of an email, SX-GATE has to know how the relevant addresses look like. Therefore SX-GATE searches in certain email headers for email addresses ending with one of the domains entered here. The domain part of a matching email address will be replaced by the target domain specified along with the mailbox. The email will then be delivered to this address. If no matches were found, the mail will be delivered to the administrator.



Not specifying the domains to search for anywhere will cause all emails to be delivered to the administrator.

Please read on at [Save the changes](#)

ETRN domains

Call ETRN for the following domains

SX-GATE will submit an ETRN call for every domain listed here. The mail server of the provider will then retry the delivery of queued emails for these domains.

Please read on at [Firewall access for SMTP](#)

Queue parameters

Retry delivery of deferred emails

The delivery of an email will be deferred if the target mail-server is temporarily unavailable or an error occurs during transmission. Here you have to specify, the period of time after which SX-GATE will re-attempt to deliver queued mails.



If the available datarate of your Internet connection is rather low, you should choose a rather long period. Otherwise repeatedly failing emails could use up datarate considerably. Moreover a long interval is advisable if your Internet connection is charged by data volume.

Scheduled mail retrieval

Schedule for polling POP/ETRN servers

Here you can compile the schedule for the retrieval of emails from the configured POP or ETRN servers. If you synchronised mail retrieval with new connections of the dial-up Internet connection, it is not necessary to define a schedule.



If no POP or ETRN server has been defined or no mailboxes and domains have been specified along with the POP or ETRN server, there will be no activity at the specified polling times.

13.5 IPsec VPN

Configure IPsec VPN

What do you want to configure?

Setup L2TP-IPsec server for client connections

With this wizard you can prepare SX-GATE's VPN server for connections from L2TP IPsec clients. This will configure the interfaces "l2tp0" and "ipsec0". The corresponding VPN connection will be called "L2TP".

Connect to a central SX-GATE

If this SX-GATE is located in a branch office, you can install the IPsec setup package which has been issued by the central SX-GATE here. Interface "ipsec0" will be configured.

What do you want to configure?

- Setup L2TP-IPsec server for client connections
Please read on at [Configure L2TP IPsec VPN](#) (p. 250)
- Connect to a central SX-GATE
Please read on at [Select file](#) (p. 254)

Configure L2TP IPsec VPN

Some general information on L2TP IPsec

L2TP is the acronym for "Layer Two Tunneling Protocol". It is used to provide remote access to a certain network, typically the LAN. Although the L2TP client has no direct physical connection to the LAN, an unused LAN IP address is assigned to it. For all other devices in the LAN, the L2TP client seems to be a physical member of the LAN. Thus there's no need to change the routing configuration of any LAN device.

SX-GATE provides an L2TP server which authenticates any incoming connection with a username and a password. Besides authentication, the L2TP server will also assign an IP to the L2TP client and will reconfigure the network interface so that data packets for the L2TP client are directed to SX-GATE. While running, the L2TP server extracts the payload received via the L2TP channel and wraps L2TP around data packets sent from the LAN to the client.

For privacy, the L2TP connection is protected by an IPsec VPN tunnel. Just like the L2TP connection, the VPN tunnel is established between SX-GATE and the L2TP IPsec client. Besides the possibility of using the stronger certificate based authentication, VPN will encrypt every L2TP packet and ensure the authenticity of all data packets.

Recapitulating, when an L2TP client communicates with a device inside the LAN, between the client and SX-GATE the payload is embedded in L2TP which in turn is embedded in IPsec packets. Any routers in-between will only "see" the IPsec VPN.

Notes regarding this wizard

VPN connections can be configured in various different ways. Not all of them can be covered by this wizard. This wizard configures a typical L2TP IPsec connection. In individual cases it will be necessary to make some modifications in other configuration menus of SX-GATE.



Please read the information provided on the different screens carefully. Things you have to do outside this wizard will be stated there.

This wizard will always change the VPN connection named "L2TP" within interface "ipsec0". If necessary these will be created. When creating interface "ipsec0", it will be set on top of the current Internet interface as determined by the default route.

Certificate based authentication is preferred, using certificates of a certain trusted Certificate Authority (CA). If the latter hasn't been determined yet, SX-GATE's builtin CA is used. If needed, the SX-GATE CA and the key for SX-GATE's VPN server will be initialized, first.

Please read on at [Issue new VPN server certificate](#)

Please read on at [Trusted VPN CA](#)

Please read on at [L2TP IP addresses](#)

Issue new VPN server certificate

On this screen you have to enter the certificate subject.

CN

If SX-GATE has a static Internet IP address or a certain DNS name, you should supply it here. Otherwise choose a name which is rather unambiguous.

Subject alternative names

Most clients prefer this certificate property while verifying that the server certificate belongs to the expected server. Enter all required names and IPs used to address the IPsec server from the Internet.



This property is mandatory if MacOS clients will connect. MacOS clients expect server certificates with a subject alternative name which includes the server address as configured in the MacOS client.

Certificate request

Entering this screen, a certificate request will be generated on SX-GATE. You can sign it now with the CA certificate.

Extended Key Usage: server authentication

It is recommended to enable this option. By default the Windows IPsec client requires the VPN server certificate to include this "Extended Key Usage" value.



Depending on the client and its configuration, a client may refuse to connect if the server certificate does not include this attribute.

Signing certificate

Entering this screen, the certificate will be signed. By pressing the "Finish" button, the new VPN server key will be installed.

Trusted VPN CA

To authenticate an IPsec VPN connection, SX-GATE verifies whether the certificate presented by the peer has been issued by the trusted Certificate Authority (CA). Currently the trusted CA is not SX-GATE's builtin CA. This is perfectly all right if an external CA issues certificates for you. Otherwise you have the possibility to replace it by SX-GATE's CA.



When changing the trusted CA, other VPN connections might no longer work.

Although it is basically possible to have more than one trusted CA, on SX-GATE you can specify only one to keep it more simple. If anyhow the certificates of the peers have been issued by different CAs you have to make a decision which of them is to be the trusted CA. For all other connections you have to stick to the other authentication mode which requires the import of the peers' public keys. The respective configuration is not

supported by this wizard. Please change to the "Modules" menu instead. There you can also set an external trusted CA.



CA based authentication requires that the SX-GATE VPN server certificate has been issued by the trusted CA, too.

Please read on at [L2TP IP addresses](#)

L2TP IP addresses

IP addresses assigned to L2TP clients

Insert the IP addresses which SX-GATE will assign to the peers. The IPs must not be in use elsewhere. If possible, you should enter IPs from the network the L2TP client wants to connect with. This network has to be directly connected to SX-GATE.



The number of IP addresses specified here determines the maximum number of concurrent L2TP connections.

You can either add single IPs or whole blocks of addresses. A block of addresses is specified by a network address with its corresponding netmask. If for example the LAN network is 192.168.0.0/24, the entry 192.168.0.160/27 will add the 32 IP addresses from the range 192.168.0.160 to 192.168.0.191.



The address ranges must not include network or broadcast addresses of a local ethernet, except for the network and broadcast addresses of a class C network (*.0 and *.255). The system will exclude these automatically.



Entering an invalid netmask can cause havoc. In the example above, the entry 192.168.0.160/255.255.255.0 (netmask 255.255.255.0 instead of 255.255.255.224) would add 254 addresses from the range 192.168.0.1 to 192.168.0.254 which is identically equal to the LAN address range.

DNS

Assign DNS server

With this setting you will determine which name server the client will use. For a Windows network one would typically enter the IP of the Windows server.

Users

Users with RAS access

When connecting to the L2TP server, the clients have to authenticate themselves with login and password. Only members of the SX-GATE group "system-ras" are able to do so. This control shows you to which users this right has been granted and which users are not able to connect. To add or remove several users at a time you can select multiple entries from the respective list. Hold down the CTRL key while selecting a user to accomplish this.



To create additional users you have to change into the user administration after completing this wizard. Create the required users there and assign them to group "system-ras".

Save the changes

Yet no changes have been made to the system configuration of SX-GATE. Press "Finish" to apply the changes you made or "Cancel" to dismiss them.

Select file

Please select the setup archive. It contains a file with the required configuration parameters and a password protected PKCS#12 file with an RSA key-pair. You will have to enter the password to open the PKCS#12 file.

Check certificate

Check the certificate you just uploaded before it's going to be installed.

Please read on at [Imported VPN server certificate](#)

Select CA certificate file

Now the certificate chain must be added to the certificate. This may include one or more intermediate CAs. The chain ends with the root CA. All certificates must be in PEM or DER format. Please ask your CA for the required certificates.

Check CA certificate

The uploaded certificate is appended to the certificate chain.

Please read on at [Select CA certificate file](#)

Imported VPN server certificate

The key-pair has been imported

Check CA certificate

The trusted VPN server CA should usually be the same CA which issued the VPN server certificate. If the CA certificate is included in the uploaded PKCS#12 file it may be imported along with the server certificate.



If you change the trusted CA, connections which need to be authenticated with the old CA can no longer be established.

A table gives you an overview of the available objects. If multiple columns are displayed you can change the sort order by clicking the column title. If there are more than 20 entries, a navigation bar will appear below the bottom right hand corner of the table. You can switch between a grouped view or a pager. The full screen mode allows you to see all entries at the same time. Pick an entry by clicking its title in the left column. A pencil icon or a trashcan in the right column allow you to rename or delete an entry.

Check VPN connection

Especially when configuring a SX-GATE in a branch office, uploading a setup archive comes in handy. After confirmation of this screen an IPsec connection to the central SX-GATE is configured, according to the data found in the archive. The connection uses interface ipsec0 and is named after the peer's internet address as stated in the setup archive. If necessary the ipsec0 interface will be created, the IPsec service will be started and other configuration option will be changed as required.



If an IPsec connection with the same name exists, it will be replaced.

13.6 Support access

Select access method

How can technical support access SX-GATE?

There are several different ways to grant access:

Via Internet (outgoing)

This method also grants Secure Shell access to your SX-GATE via Internet. In contrast to the previous option, your SX-GATE will establish an outbound connection which can be used by technical support to connect back to the device (reverse tunnel). This will only be possible as long as the outbound connection exists. If SX-GATE is situated behind a NAT device or an other firewall, the reverse tunnel might be the only option to grant access for technical support.

Via Internet (incoming)

With this option the wizard will help you to modify the firewall policy of SX-GATE so that technical support can connect via Internet using Secure Shell. Furthermore the wizard allows you to disable or delete the relevant firewall rules.

How can technical support access SX-GATE?

- Via Internet (outgoing)
Please read on at [Connect](#) (p. 258)
- Via Internet (incoming)
Please read on at [Firewall access for Secure Shell](#) (p. 257)

Firewall access for Secure Shell

SSH access to SX-GATE on interface ...

Technical support uses Secure Shell connections to access SX-GATE. Hence the firewall policy has to accept incoming connections to the corresponding TCP port 22 (ssh). If full access is granted anyway, an appropriate message will be shown. Otherwise you can insert or delete the required rules here. If there are no rules in the list, no inbound SSH connections will be accepted.



If SX-GATE is protected by one or more upstream firewalls, the policy of these firewalls will have to allow incoming Secure Shell connections, too.

Please ask technical support for their IP address and the correct port range to insert.

Save the changes

Yet no changes have been made to the system configuration of SX-GATE. Press "Finish" to apply the changes you made or "Cancel" to dismiss them.

Connect

Please select

Technical support will give you the name of their server system. As soon as SX-GATE connects to this server, technical support can connect back to SX-GATE. If you close the connections all active sessions will be terminated and technical support will no longer be able to establish a new connection.

14 Modules

The mainmenu "Modules" provides a module based view on the SX-GATE functions. Extensive know-how is expected in this area. For the basic overall configuration of the system you should make use of the wizard style setup offered in the mainmenu "Wizards".

14.1 Network

14.1.1 Settings

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

14.1.1-A General.....	259
14.1.1-B IPsec Parameters.....	261
14.1.1-C VPN Certificate.....	261
14.1.1-D Trusted VPN CA.....	262

14.1.1-A General

IPv6

This setting enables or disables SX-GATE's IPv6 support.

Router mode

Select this option if SX-GATE should advertise itself as an IPv6 router in your network.

Host mode

If SX-GATE is used as e.g. proxy or mail relay server in a DMZ, this option should be used.

Default route using interface

Here you can specify which interface is used to connect to the Internet. All IP packets with destination addresses that have no other routing information will be sent via the selected interface.



You can use this setting to switch between two Internet connections (e.g. leased line connection via eth1, ADSL dial-up via adsl0). Please note however, that switching the connection might require other parameters to be changed accordingly (e.g. name server, the provider's proxy or the provider's mail relay).

Cluster with shared Internet access

Enable for a mutually exclusive use of the Internet connection by master and backup node. This is required if e.g. only one ADSL line or - when connecting via an upstream router - only one valid Internet IP is available. While in backup state, the backup node will access the Internet through the master. In case of a failover the backup node will take over the Internet connection.



The master node must grant unlimited Internet access for the backup in this case. On the backup node, please add a firewall forwarding rule to the firewall configuration of the internet interface. Choose protocol "*" and enter the backup IP as configured in the cluster configuration as source IP. Finally sync the new rule to the master.

fallback on failure

When this option is activated, the system will switch automatically to the configured interface, whenever the Internet connection is interrupted. An ADSL connection is considered broken if the PPP connection is down. For other interface types "ping" is used to check if the servers from a customizable list of addresses are reachable. Depending on the nature of the problem, it can take a few minutes until fallback is triggered.

During fallback SX-GATE keeps testing the broken link. When it's online again, it automatically switches back.



With a manual ADSL or network restart you can force the system back to the default link.

When using an ADSL interface as fallback, the corresponding service must be running and the interface must be configured ready to use.

The settings for DNS, mail relay and proxy server of the ISP will not be altered by the fallback. Especially if your ADSL line and the backup line are operated by different providers, you have to make sure that these services are available in both configurations.

Fallback mail notification

Notifications about a fallback will be sent to this email address.

Alive check using ping to

SX-GATE checks the connection by regularly pinging the addresses from this list. You can select IP objects, too, however only IP addresses will be used and networks will be ignored.



Please do not use DNS-based IP objects with frequently changing IPs. Each IP change would trigger a restart of the networking subsystem.

14.1.1-B IPsec Parameters***MTU of ipsec interfaces***

When extending IP packets with the IPsec headers, often the maximum allowed packet size on the link to the remote IPsec server is exceeded. So these packets need to be fragmented. This in turn may cause problems with some Internet routers, especially those which have been configured to discard fragmented packets.

If e.g. the transmission of data packets of more than 1500 byte fails, while packets with less than say 1200 byte are delivered ok, it indicates an MTU problem. Even the negotiation phase of A IPsec connection can be affected. If you don't get a connection but find complaints about duplicate packets in the IPsec log, the MTU might cause this, too.

Reduce the MTU (Maximum Transmit Unit) in this case. With this parameter you can control the maximum size of data packets before they are passed on to the encryption stage. Choose a value which is low enough, so that no in transit fragmentation of the encrypted packets is necessary. Note however, that a lower MTU reduces the throughput.

Non-unique IDs

When disabled, a new connection will terminate an existing connection with the same ID. This is important for dial-up clients with dynamic IP addresses as it will clean up broken connections which might otherwise prevent new connections in the worst case. You should enable this option only if there really are multiple peers using the same ID.

14.1.1-C VPN Certificate

To authenticate VPN connections using X.509 certificates, SX-GATE requires a key-pair with certificate of its own.



Both, IPsec and OpenVPN based VPNs use this certificate.

To prepare a new SX-GATE for IPsec client connections or to configure the VPN server of a SX-GATE in a branch office using a setup archive, please change to menu "Wizards > IPsec VPN".

Otherwise, the certificate administration takes place in menu "System > Certificate manager". In submenu "CA certificates" you can initialize the "SX-GATE CA" and issue certificates yourself by clicking "Certificates". In submenu "Keyring" you can import key-pairs you received from other certification authorities.

If you don't use the VPN server of SX-GATE or if you authenticate VPN connections by preshared keys only, this screen is not effective.

Select key/certificate

Please select one of the keys managed in menu "System > Certificate manager > Keyring".

Export public key

If the VPN peer requires the public key of the SX-GATE VPN server certificate, it can be downloaded here.



Please assure that it is really the public key of the VPN server which is requested. Perhaps the public key of the CA which issued the SX-GATE certificate is required instead.

14.1.1-D Trusted VPN CA

Certificate based authentication usually implies checking if the presented certificate has been issued by a trusted certification authority (Root-CA). Here you can specify the CA trusted by SX-GATE's VPN server. You can use the local SX-GATE CA or upload the public key of a CA.

Although it is basically possible to have more than one trusted CA, on SX-GATE you can specify only one to keep things simple. If anyhow the certificates of the peers have been issued by different CAs, you have to make a decision which of them is to be the trusted CA.



In the IPsec configuration it is possible to import a peer's public key. So it is still possible to authenticate it, even though its certificate has been issued by a different CA. For OpenVPN based connections you may use certificates of different CAs if SX-GATE is the client.

If you don't use the VPN server of SX-GATE or if you authenticate VPN connections by preshared keys or specific public keys only, this area is not effective.

Delete second trusted CA certificate

After all peers were migrated to the new CA, you can delete the old CA here.

Set a new trusted CA

Here you can specify, which CA will be the trusted CA for the SX-GATE VPN server. You can copy the public key of the local SX-GATE CA, import the public key of a CA in PEM format or extract it from a PKCS#12 file.

Issue local VPN server certificate

With this function you can issue or renew the certificate of SX-GATE's own VPN server. The new certificate will be signed by the SX-GATE CA and is valid for up to 6 years.

Issue new VPN server certificate

On this screen you have to enter the certificate subject.

CN

If SX-GATE has a static Internet IP address or a certain DNS name, you should supply it here. Otherwise choose a name which is rather unambiguous.

Subject alternative names

Most clients prefer this certificate property while verifying that the server certificate belongs to the expected server. Enter all required names and IPs used to address the IPsec server from the Internet.



This property is mandatory if MacOS clients will connect. MacOS clients expect server certificates with a subject alternative name which includes the server address as configured in the MacOS client.

Certificate request

Entering this screen, a certificate request will be generated on SX-GATE. You can sign it now with the CA certificate.

Extended Key Usage: server authentication

It is recommended to enable this option. By default the Windows IPsec client requires the VPN server certificate to include this "Extended Key Usage" value.



Depending on the client and its configuration, a client may refuse to connect if the server certificate does not include this attribute.

Signing certificate

Entering this screen, the certificate will be signed. By pressing the "Finish" button, the new VPN server key will be installed.

Delete trusted CA certificate

You can terminate the trust relationship with the specified CA here. After the trusted CA key has been deleted, VPN connections will no longer be accepted if the presented X.509 certificate was issued by the formerly trusted CA. As an exception, a connection will still be accepted if the public key of the peer was imported into SX-GATE for authentication purposes.

Import certificate revocation list

Here you can install the recent certificate revocation list (CRL) of the trusted CA. A CRL offer the possibility to invalidate a certificate already before it expires. This is useful if for example an employee leaves the company and VPN access has to be denied. You can copy the CRL of the local SX-GATE CA or import a CRL file in PEM format.



The CRL must have been issued by the trusted CA. Otherwise it is not considered.

Copy local CA revocation list to VPN server

If SX-GATE's VPN server uses certificates issued by its own CA, you can transfer the current certificate revocation list (CRL) into the VPN server here. A CRL offers the possibility to invalidate a certificate before it expires. This is useful if for example an employee leaves the company and VPN access has to be denied.

Delete certificate revocation list

Here you can delete the certificate revocation list. Formerly invalidated certificates will then be accepted again.

14.1.2 Interfaces

A table gives you an overview of the available objects. If multiple columns are displayed you can change the sort order by clicking the column title. If there are more than 20 entries, a navigation bar will appear below the bottom right hand corner of the table. You can switch between a grouped view or a pager. The full screen mode allows you to see all entries at the same time. Pick an entry by clicking its title in the left column. A pencil icon or a trashcan in the right column allow you to rename or delete an entry. Add new objects by clicking "New Entry" below the table on the left.

Interface type

To create a new interface, please select the type of interface first.

ADSL/Mobile broadband (adsl)

An ADSL interfaces uses one of the system's Ethernet adapters. After adding the interface you can specify which Ethernet adapter you want to use. For a mobile broadband connection an USB modem is required which is available from your SX-GATE dealer.

Ethernet (eth)

The Ethernet adapters of SX-GATE are numbered consecutively starting with 0. Thus the interface eth2 refers to the third Ethernet adapter.

VLAN 802.1Q (vlan)

VLAN interfaces are logical network interfaces, which tag frames according to the IEEE 802.1Q standard. A VLAN interface must be assigned to an ethernet adapter. The interface number of the created VLAN corresponds to its VLAN tag. Acceptable values are 1 through 4094.



Packets routed via a VLAN interface will get tagged accordingly. Vice versa the interface receives only packets with the appropriate tag.



If a regular ethernet interface has been configured for the ethernet adapter, too, the regular ethernet interface will send and receive untagged packets. Delete the interface or configure the VLAN switch accordingly to avoid this.

WLAN (wlan)

To use an installed WLAN adapter please create the WLAN interface with number 0. It is possible to run up to seven additional SSIDs on the same WLAN adapter

and the same channel. Create WLAN interfaces with a numbers greater than 0 for additional SSIDs.

Wireguard (wg)

Each interface of this type will create a Wireguard instance with an individual setup. Usually a single instance is sufficient, as it can handle multiple connections. However multiple interfaces are useful to group connections (e.g. clients vs. other VPN servers) or if different firewall settings are required (e.g. own employees / own branch offices vs. external employees / other companies).

OpenVPN Client (ovpnc)

This interface type is required if SX-GATE is to connect to a OpenVPN server. Each interface can handle only one connection. Create multiple interfaces if you need to connect to multiple servers.

OpenVPN Server (ovpns)

Each interface of this type will create an OpenVPN server instance with an individual setup. Usually a single server instance is sufficient, as it can handle multiple clients. However multiple interfaces are useful to group connections (e.g. clients vs. other VPN servers) or if different firewall settings are required (e.g. own employees / own branch offices vs. external employees / other companies).

IPSec VPN (ipsec)

Interfaces of this type are logical interfaces. An ipsec interface has to be associated with an other interface. This will add VPN functionality to this host interface. Enter a single digit interface number. Only ipsec0 supports host interfaces with a dynamic IP address. The host interface must provide the Internet connection (defaultroute) in this case.

Interface number

Please specify the interface number here. There may be certain limitations depending on the interface type as stated above.

Firewall trustlevel

Specify the firewall base policy of the new interface.

14.1.2.1 ADSL/Mobile broadband (adsl)

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

14.1.2.1-A ADSL/PPPoE.....	268
14.1.2.1-B ADSL/PPTP.....	269
14.1.2.1-C Mobile broadband.....	270
14.1.2.1-D IP addresses.....	272
14.1.2.1-E Routing.....	273
14.1.2.1-F Bandwidth management / QoS.....	273
14.1.2.1-G Priorities.....	276
14.1.2.1-H Dynamic DNS.....	277
14.1.2.1-I Limits.....	279
14.1.2.1-J Ethernet.....	280

Connection type

Please select the correct ADSL type here.

ADSL/PPPoE

Connect SX-GATE to a DSL router in bridge mode or a DSL modem if the DSL line is using PPP-over-Ethernet (PPPoE).

ADSL/PPTP

A DSL modem with integrated PPTP-to-PPPoA Relay is required to connect SX-GATE with a PPP-over-ATM (PPPoA) line. In this case SX-GATE talks PPTP to the modem.

Mobile broadband

If a certified USB stick with a valid SIM card is attached to SX-GATE, you can establish an Internet connection with LTE/UMTS/GPRS.

IPv4 mode

If IPv6 is enabled, you need to choose the kind of IPv4 connectivity.

Dual-Stack

Select this option if the provider assigns both, an IPv4 and an IPv6 address. The IPv4 address may be an internal IP address according to RFC-1918 which is then translated by the provider (Carrier-Grade NAT).

Dual-Stack Lite (DS-Lite)

With DS-Lite your Internet connection is IPv6 only. IPv4 packets are tunneled via the IPv6 connection to a specific gateway of your provider. This is where the IPv4 packet will get its final sender address (Carrier-grade NAT) and enter the IPv4 Internet.

IPv6 mode

manual IP

If this option is selected, all IPv6 parameters have to be configured manually. Router advertisements will be ignored.

automatic IP (SLAAC/DHCPv6)

Choose this option and SX-GATE will automatically determine its IPv6 configuration based on the router advertisements it receives.

14.1.2.1-A ADSL/PPPoE

Description

This input serves for documentation purposes only.

Login

Insert the login here that SX-GATE uses to sign on to the peer.

Password

Enter the password here that is used when the peer asks SX-GATE to authenticate.

Connected to network card

Select the name of the network card which is connected with the ADSL modem. We recommend to use a dedicated network card for the ADSL connection, i.e. one that does not show up in the tree menu below "Network".

VDSL via VLAN

Enter a VLAN ID for VDSL Internet connections using VLAN. Then tagged VLAN packets are used to connect with the DSL modem. Please ask your provider for the correct VLAN ID.

Use new driver

The new driver supports higher speeds. Enable this option for speeds beyond 200 Mbit/s.

Idle hangup

Here you can determine when the DSL dial-up connection has to be established and disconnected.

The dial-up connection can be established automatically whenever data has to be transmitted to the Internet. It will be disconnected when no data has been transmitted for a configurable period of time.

Alternatively you can decide to keep the connection permanently online. Anytime the link is disconnected it will be reestablished immediately.



Some Internet access providers will disconnect the line when no data has been transmitted for a certain period of time or when the connection is already online for quite a long time (e.g. 24 hours).



You should not keep the connection online permanently if the link is charged by a connection time based rate.

Hangup at

Some providers disconnect an ADSL dial-up link automatically after it has been online for 24 hours without interruption. During working hours this might be bothering. You can enter a time at which SX-GATE will always hangup so disconnection can take place e.g. at night-time.

Leave the input field empty if a scheduled hangup is not required.

14.1.2.1-B ADSL/PPTP**Description**

This input serves for documentation purposes only.

Login

Insert the login here that SX-GATE uses to sign on to the peer.

Password

Enter the password here that is used when the peer asks SX-GATE to authenticate.

Modem IP

This setting is only required for PPPoA connections. SX-GATE opens a PPTP connection to the address you fill in here.



The default IP of many modems is 10.0.0.138.



In addition to the adsl interface there must be an eth interface with an IP address in the same subnet as the modem.

Idle hangup

Here you can determine when the DSL dial-up connection has to be established and disconnected.

The dial-up connection can be established automatically whenever data has to be transmitted to the Internet. It will be disconnected when no data has been transmitted for a configurable period of time.

Alternatively you can decide to keep the connection permanently online. Anytime the link is disconnected it will be reestablished immediately.



Some Internet access providers will disconnect the line when no data has been transmitted for a certain period of time or when the connection is already online for quite a long time (e.g. 24 hours).



You should not keep the connection online permanently if the link is charged by a connection time based rate.

Hangup at

Some providers disconnect an ADSL dial-up link automatically after it has been online for 24 hours without interruption. During working hours this might be bothering. You can enter a time at which SX-GATE will always hangup so disconnection can take place e.g. at night-time.

Leave the input field empty if a scheduled hangup is not required.

14.1.2.1-C Mobile broadband

Description

This input serves for documentation purposes only.

Preferred mode

In some situations, better throughput rates can be achieved by using for example UMTS instead of LTE. This setting can be used to force the specified mode.

Login

Insert the login here that SX-GATE uses to sign on to the peer.



For mobile broadband connections it is not always necessary to enter credentials. It depends on the provider.

Password

Enter the password here that is used when the peer asks SX-GATE to authenticate.

APN

Please ask your UMTS provider for the Access Point Name.

PIN

If your SIM card is protected by a PIN number, please fill it in here. Leave this field empty if your SIM card is not protected.

Dial-up Phone Number

Enter the dial-up phone number as required for your provider. Most providers use *99#, however numbers like e.g. *99***1# are commonly used, too.

Idle hangup

Here you can determine when the DSL dial-up connection has to be established and disconnected.

The dial-up connection can be established automatically whenever data has to be transmitted to the Internet. It will be disconnected when no data has been transmitted for a configurable period of time.

Alternatively you can decide to keep the connection permanently online. Anytime the link is disconnected it will be reestablished immediately.



Some Internet access providers will disconnect the line when no data has been transmitted for a certain period of time or when the connection is already online for quite a long time (e.g. 24 hours).



You should not keep the connection online permanently if the link is charged by a connection time based rate.

Hangup at

Some providers disconnect an ADSL dial-up link automatically after it has been online for 24 hours without interruption. During working hours this might be bothering. You can enter a time at which SX-GATE will always hangup so disconnection can take place e.g. at night-time.

Leave the input field empty if a scheduled hangup is not required.

14.1.2.1-D IP addresses

IPv4 address

You can either accept a dynamic IP assigned by the peer or specify an IP address.

DS-Lite Address-Family-Transition-Router (AFTR)

In dual stack light Internet links IPv4 packets are tunneled via IPv6. The tunnel endpoint on the provider side is a special router. If its address isn't advertised with DHCP you can enter the address here.

IPv6 address

Enter an IPv6 address for this interface.

Prefix length

The IPv6 prefix length is the equivalent to IPv4 netmasks. The typical prefix length is 64, but your provider might have told you a higher value.

IPv6 privacy extension (RFC3041)

A dynamic IPv6 address derived with SLAAC is based on the hardware address of the network card. So it can be tracked worldwide easily. Enable this option and SX-GATE will add a temporary random address which is preferred.

IPv6 prefix delegation

Enable this option to ask your provider for an additional IPv6 network prefix, which is then made available for internal networks by SX-GATE.

As soon as SX-GATE receives such a prefix, an entry is created in menu "Definitions > IP objects" which will be named after the interface (e.g. "ipv6_prefix_adsl0" for "adsl0"). Subdivide the prefix by adding entries of type "IPv6 prefix" or "IPv6 address" and make

them refer to the prefix you received. You can use these objects in various configuration options.

Additional IPv6 addresses (aliases)

You can specify additional IPv6 addresses for the select network interface.

14.1.2.1-E Routing

Policy Routing

On this tab you can configure static routing entries. You can add conventional routes, considering only the packet's destination, but also extended rules which include source addresses, protocol and port numbers (policy based routing).

Static routes must be added for networks behind the peer. Specify the network address and the netmask of this remote network - this will automatically instruct the SX-GATE firewall to accept the network on this interface.

Rules for specific protocols or sources come into play if multiple internet links are available. One could for instance direct web traffic via an ADSL link while all the other traffic like emails and VPN uses an SDSL line.

The evaluation order is not based on the order in the list. The priority depends on how specific a rule is, taking in account the rules configured across all devices. Routes with all three parameters defined (i.e. protocol, source and destination) will be considered first. Rules with a destination take precedence over rules with protocol. These in turn have a higher priority than rules with a source. Within source and destination, rules are sorted by descending netmasks. The evaluation order of overlapping protocol specifications is not defined.

14.1.2.1-F Bandwidth management / QoS

For bandwidth management you have to fill in the available bandwidth. Uplink and downlink may be different (ADSL). Leave empty to disable bandwidth management on this interface. If you enter only one value, either for uplink or for downlink, bandwidth management will apply to packets in that direction only.



Specifying a wrong bandwidth can cause severe connection problems, especially if the actual bandwidth is lower than the configured one. Please ask your provider if you are uncertain.

Outbound bandwidth (uplink)

Enter the uplink bandwidth. For asymmetric connections this is usually the lower value. Bandwidth management will then process all outbound packets on this interface. The direction of the corresponding connection (inbound or outbound) doesn't matter.

Inbound bandwidth (downlink)

Enter the downlink bandwidth. For asymmetric connections this is usually the higher value. Bandwidth management will then process all inbound packets on this interface. The direction of the corresponding connection (inbound or outbound) doesn't matter. Leave empty if you don't need inbound bandwidth management.

Inbound bandwidth management is a contradiction in terms. Priority driven re-ordering of data packets waiting to be transmitted usually has to be done on the sending side of the (Internet) link. Only there it can be done in a reliable way. After all the packet has already been transmitted on the receiver side. However Internet connectivity with provider guaranteed Quality of Service / bandwidth management is often very expensive, so inbound bandwidth management is an option despite of its limitations.



Inbound bandwidth management reduces the available bandwidth by up to 20%. It requires that an adequate amount of the inbound data volume is covered by TCP connections.

Quality of Service (QoS) for Voice over IP (VoIP)

For VoIP the latency time, i.e. the time it takes for a voice packet to travel from sender to recipient, is very important. Hence SX-GATE's traffic shaper optimizes delivery of VoIP data packets with a special quality-of-service module.



In order to be recognized as VoIP packet, a data packet needs to be tagged according to Diffserv-Code-Point Expedited-Forwarding (DSCP EF).

The amount of bandwidth a single call requires depends on the codec that is used. The codec defines the compression of a VoIP call. The more compression is applied the less bandwidth is consumed, however also the quality decreases. The following table shows the net bandwidth required by commonly used codecs. Some codecs are used at different bandwidths. In this case the maximum bandwidth is given.

Codec	max. bandwidth (bit/s)
G.711	64000
G.722	64000

Codec	max. bandwidth (bit/s)
G.722.1	32000
G.723.1	6400
G.726	40000
G.728	16000
G.729	8000
GSM	13000
iLBC	15200

Max. number of concurrent calls

Enter the expected maximum number of simultaneous calls on this interface. It is used to calculate the overall bandwidth that needs to be reserved for VoIP traffic. The value "0" will disable this feature.



The total bandwidth of the link must not be exceeded.

Bitrate of the codec used

Enter the net bandwidth of the codec to be used. Take the codec with the largest bandwidth if different codecs are in use.



When calculating the total required bandwidth the system will automatically take the IP overhead into account. Lower bandwidth consumption causes more overhead.

Max. number of calls via IPSec

Enter the expected maximum number of simultaneous calls over VPN on this interface. It is used to calculate the overall bandwidth that needs to be reserved for VoIP traffic. The value "0" will disable this feature.



Wenn enabled, VoIP data packets will be expedited. This applies to the plain packet as well as to the VPN packet after encryption.



The total bandwidth of the link must not be exceeded.

Bitrate of the codec used in IPSec

Enter the net bandwidth of the codec to be used. Take the codec with the largest bandwidth if different codecs are in use.



When calculating the total required bandwidth the system will automatically take the IP and the IPSec overhead into account. Lower bandwidth consumption causes more overhead.

14.1.2.1-G Priorities

Use this feature to determine the priority of outgoing data packets. A proportional minimum bandwidth is assigned to each priority class. Unused bandwidth of a class will be used by classes with lower priority.

From a technical point of view the rules overwrite the ToS/DSCP field of matching IP packets. If a local application already takes care of this field, a rule would not be necessary for outbound packets. For inbound packets however the ToS/DSCP field is often modified in transit. So inbound traffic shaping usually requires rules.



Some ISPs will charge you for IP packets with certain ToS/DSCP values. Please check the ISPs terms of service.

The minimum bandwidth is assigned as follows: The bandwidth required for VoIP according to the configuration is reserved and subtracted from the total available bandwidth. Of the remaining bandwidth, 10% goes to empty TCP ACK packets, 50% to packets with high priority and 20% to packets with normal and low priority respectively.



Inbound traffic shaping treats all non-TCP packets as high priority.

Priorization of connections

Use this list to assign a higher or lower priority to specific data packets. If more than one rule matches, the priority of the topmost rule will be used.

The following inputs are available:

Protocol

Selects the IP protocol and port signature. With inbound bandwidth management, only TCP protocols will actually be processed.



Protocols are defined in menu "Definitions > Protocols".

Local IP/network

Viewed from the perspective of the selected interface, you can enter a local address here. This corresponds to the source IP of outbound packets (before SNAT) and the destination IP of inbound packets (before DNAT).



When SNAT or DNAT is involved, restricting a priority rule to specific local IPs usually requires two rules to catch both, in- and outbound packets: For inbound packets you would enter a SX-GATE IP, for outbound packets the internal IP (of the LAN client or the server addressed with DNAT).

Direction

Decide in which direction the port signature of the selected protocol has to be applied. Let's take the HTTP protocol as an example. The arrow "-->" means the HTTP port 80 is on the external side. So outbound bandwidth management will process packets to port 80, inbound bandwidth management packets from port 80. With "-->" you will get the opposite: Packets to port 80 are processed by inbound, packets from port 80 by outbound bandwidth management. The double arrow "<-->" combines both directions.

External IP/network

Viewed from the perspective of the selected interface, you can enter a remote address here. This corresponds to the destination IP of outbound packets and the source IP of inbound packets.

Priority

Select the priority for matching packets.

14.1.2.1-H Dynamic DNS

With dynamic DNS it is possible to address a device which it is connected to the Internet with a dynamic IP address. So with dynamic DNS you can access the services offered by SX-GATE despite of its dynamic IP address. Dynamic DNS uses ordinary hostnames (fully qualified domain names, FQDN) to address a device. Dynamic DNS is offered by many different providers. Some offer this service for free, others charge for it.



It takes a few seconds or even minutes until a new IP address becomes available via dynamic DNS.

If SX-GATE gets a dynamic IP address itself (ADSL interface with dynamic IP or Ethernet interface with IP address assigned via DHCP), please configure dynamic DNS in settings of the respective interface of menu "Modules > Network > Interfaces". SX-GATE will then update its dynamic DNS record once a new dial-up connection is established or when the IP changes.

If SX-GATE is situated behind a NAT router and it's the NAT router that actually gets the dynamic IP, the NAT router must forward inbound connections to SX-GATE (DNAT, portforwarding, exposed host). You should configure dynamic DNS in the NAT router, as only the NAT router knows its current dynamic IP. Only if this is not possible you may consider to configure dynamic DNS in SX-GATE menu "Modules > DNS > Settings". SX-GATE will then try to figure out the current dynamic IP of the NAT router at regular intervals, using an Internet based service.

Protocol

Unfortunately there's no standard protocol for updating dynamic DNS records. SX-GATE offers a bunch of different protocols. Please consult your dynamic DNS provider, which protocol is used and if SX-GATE supports it.

Update server of the DNS provider

Here you have to specify the server which accepts and processes the IP address update messages. This server may be different to the webserver of the dynamic DNS provider.

Update URL

Here you have to specify the update URL (aka "direct URL") for updating the dynamic IP address. The URL may have the placeholders <host>, <ipaddr>, <username> and <password> that will be substituted by the dynamic DNS name, the IP address, the username and the password, i.e.: `http://dynupdate.exampledyndns.com/nic/update?hostname=<domain>&myip=<ipaddr>`

Dynamic DNS hostname of SX-GATE

Usually the providers allow you to manage multiple dynamic DNS names with a single user account. Therefore you have to supply SX-GATE's complete dynamic DNS name here (including the domain).

Login

No dynamic DNS updates without authentication. Please enter the login for the corresponding account here.

Password

Finally you have to specify the password for the dynamic DNS account.

Update now

Check live if DynDNS update is working.

14.1.2.1-I Limits

If SX-GATE is connected to the Internet with a ADSL dial-up line you can define upper limits for the online time and the number of connections. These settings apply to SX-GATE's current default route interface.



If the Internet connections is charged depending on the time spent online or the number of connections, in your own self-interest you should define reasonable limits here. This is the only way to protect yourself from high costs caused e.g. by a misconfigured system or application.

For each of the following values you can define two limits. When the first limit is reached, an email notification will be sent to the administrator. Also when the second threshold is exceeded an email will be generated. In addition the interface will be disabled.



To enable a stopped interface you have to restart the corresponding service.

Leave the input fields blank for all those limits you don't want to define.

The current statistics of the connection are displayed, too.



The counters will start to increase as soon as the IP connection has been established completely. If the ADSL connection succeeds, but the login at the provider fails, the ADSL connection will not be detected.

Email warning after connection time

These limits will apply to the total time of the current connection.

Email warning after total connection time

These limits will apply to the total time of all connections. Use the switch "Reset totals" to control how often the sum will be reset.

Email warning after total number of dial-ups

These limits will apply to the total number of all connections. Use the switch "Reset totals" to control how often the sum will be reset.

Reset totals

The totals will be reset in the interval specified here.



A stopped interface will not be restarted automatically when the totals are reset.

Reset totals now

You can reset the totals anytime by pressing this button.



Also this command will not restart a disabled interface. You have to restart the corresponding service at "System > Services".

14.1.2.1-J Ethernet

If autonegotiation of network link parameters fails you can switch to manual configuration.



Not all network card drivers support a manual configuration.

Speed

Please select the required network device speed.

Duplex

Please select the required duplex mode.

14.1.2.2 Ethernet (eth)

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

14.1.2.2-A Settings.....	283
14.1.2.2-B IP addresses.....	285
14.1.2.2-C IPv6 router advertisement.....	287
14.1.2.2-D Routing.....	289
14.1.2.2-E Bandwidth management / QoS.....	290
14.1.2.2-F Priorities.....	292
14.1.2.2-G Dynamic DNS.....	294
14.1.2.2-H Packet monitor.....	295
14.1.2.2-I Server addresses.....	295
14.1.2.2-J Additional rulesets.....	295

Interface mode

Select how the network adapter should be used.

standalone network

In this mode the network adapter will get its own IP configuration.

additional link aggregation port

Select this option if the network adapter should join a group of adapters for link aggregation.



To create a new link aggregation adapter group, please select option "standalone network" and enable link aggregation there.

additional Bridge port

With this option you can connect the network adapter with a bridge.



To create a new bridge, please select option "standalone network" and enable bridging there.

IDS packet monitor

Select this special mode and the Intrusion Detection System (IDS) will monitor the network interface, which has to be connected to the monitor port of a switch.



The IDS operates in a passive mode, i.e. it logs but does not intercept malicious packets. In active mode the IDS runs as part of the firewall on the Internet interfaces.

IPv4 mode

Select the kind of IPv4 connectivity.



For SX-GATE's primary network interface (eth0) a static IP is mandatory. So this setting is not available for eth0.

automatic IP (DHCP)

For example if a cable modem is used to connect SX-GATE with the Internet, the IP address might be assigned dynamically by DHCP. Select the corresponding option in this case.

Dual-Stack Lite (DS-Lite)

This option is only available if IPv6 is enabled and the interface is not configured as a bridge. With DS-Lite your Internet connection is IPv6 only. IPv4 packets are tunneled via the IPv6 connection to a specific gateway of your provider. This is where the IPv4 packet will get its final sender address (Carrier-grade NAT) and enter the IPv4 Internet.

IPv6 mode

Select the kind of IPv6 connectivity.

manual IP

If this option is selected, all IPv6 parameters have to be configured manually. Router advertisements will be ignored.

automatic IP (SLAAC/DHCPv6)

Choose this option and SX-GATE will automatically determine its IPv6 configuration based on the router advertisements it receives.

14.1.2.2-A Settings

Description

This input serves for documentation purposes only.

Link aggregation of network adapters

Multiple network cards can be aggregated for high availability or increased throughput.



After enabling this option only one network adapter is part of the "aggregation". To add adapters, please create "eth" interfaces as appropriate or select an existing "eth" interface. Then change the setting "Interface mode" to "additional link aggregation port" and add the interface to the bundle.

active/passive

In this mode only one of the aggregated network adapters will be active. When the link is lost it will failover to an other adapter.

Connect the aggregated network adapters with different network switches for high availability. No special features or configuration is required in the switches.

Dynamic Link aggregation IEEE 802.3ad/802.1AX

This mode increases the throughput. It provides only limited high availability, as all network adapters have to be connected with the same switch. For high availability you would need a so called virtual switch, which consists of multiple physical switches.



The distribution of outbound packets is based on the MAC addresses. So this mode is not suitable if most data is sent to the same peer (e.g. a router or gateway).

Connect the aggregated network adapters with a switch that supports Link Aggregation. The switch ports must be configured accordingly. All of the aggregated adapters must connect with the same speed and full duplex.

Load balancing by MAC

This setting is almost identical to the previous one. However the restriction that all network adapters have to connect with the same speed does not apply. Please note that the switch ports have to be grouped together. The vendors use different terms for this (e.g. EtherChannel or Trunking).

Load balancing by packet

Outbound packets will be distributed in turn to the available network adapters. So this mode is the only one where already a single connection can benefit from load balancing.

Select this option if most data is sent to the same peer (e.g. a router or gateway) which is either directly connected (without switch) or via independant, parallel switches. The peer must support this and has to be configured accordingly. This will increase the throughput and provide high availability.

You could use this mode also when you connect all network adapters with a port group (EtherChannel, Trunk) on a single switch. But you need to be aware that packets will often be re-ordered when they arrive at a peer. With TCP this will cause frequent re-transmissions. Due to the connection with a single switch, only limited high availability is provided.

Add to link aggregation

Please select the link aggregation this interface should become a part of.

Bridge

Much like a switch, a bridge connects multiple network segments to one large network. With SX-GATE you can even restrict communication with firewall rules. So you can e.g. configure SX-GATE as a stealth firewall between the LAN and an Internet router.



It is not possible to configure DS-Lite on a bridge interface.

Please note that for connections routed from outside into the bridge the actual target bridge port is unknown by the time it is filtered in the firewall. So firewall forwarding rules, rules for outbound connections (source is a SX-GATE service) and SNAT rules for routed connections always have to be configured for the bridge as a whole and not for each bridge port individually. Even a separate target zone has to be selected for the bridge as a whole.

In contrast you can configure rules for intra bridge traffic, i.e. traffic which passes from one bridge port to another, by port. The same applies to DNAT rules and rules for inbound connections (destination is a SX-GATE service). For each port an individual firewall zone is selected. As source zone it is even available outside of the bridge, whenever a connection is routed from the bridge to an interface outside of the bridge.

Spanning tree protocol

If you have connected multiple switches and bridges in with redundant links, you must enable the Spanning Tree Protocol (STP) on all switches and bridges. Using STP the devices will make sure that no loops occur within the network topology and will react to link failures.

Route known destinations

When enabled, some packets won't pass the bridge but will be routed by SX-GATE instead. It affects packets to destination IPs which are configured on other SX-GATE interfaces, VPNs or for which a static route exists.



Enabling this option makes sense only if SX-GATE is used as a transparent firewall between client devices and a router which is the standard gateway of these clients.



Firewall rules for these connections have to be configured in submenu "Policies" and not in submenu "Bridge".

Add to bridge

Please select the bridge this network adapter should be connected with.

Network card parameters

If autonegotiation of network link parameters fails you can switch to manual configuration.



Not all network card drivers support a manual configuration.

Speed

Please select the required network device speed.

Duplex

Please select the required duplex mode.

14.1.2.2-B IP addresses

IPv4 address

Specify the IPv4 address that the corresponding SX-GATE interface should use as its own address. The IP address of the interface eth0 must be changed at "System > Setup".



The IP address assigned here may not be part of an IP subnet which has already been assigned to an other interface.

IPv4 netmask

Here you have to specify the netmask corresponding to the IP address.

IPv4 default gateway

Simplifying things, a default gateway is a router linking to the Internet. If such a router is connected to this interface you have to enter its IP address here. In "Modules > Network > Settings" you can select which interface is to be used to connect to the Internet. Selecting this interface, SX-GATE will setup a default router via the gateway specified here.

Additional IPv4 addresses (aliases) / Cluster IP addresses

You can specify additional IP addresses for the select network interface. You can add addresses belonging to the same IP subnet as the primary address. This is useful for example to bind multiple Internet IP addresses to SX-GATE and then use firewall rules to redirect connections to different internal addresses. However you may also add addresses of different networks if multiple IP subnets share the same physical Ethernet.

DS-Lite Address-Family-Transition-Router (AFTR)

In dual stack light Internet links IPv4 packets are tunneled via IPv6. The tunnel endpoint on the provider side is a special router. If its address isn't advertised with DHCP you can enter the address here.

IPv6 address

Enter an IPv6 address for this interface. If the address is based on a delegated prefix, please add an entry of type "IPv6 address" in menu "Definitions > IP objects" which refers to the prefix.

IPv6 prefix length

The IPv6 prefix length is the equivalent to IPv4 netmasks. The typical prefix length is 64.



With prefix lengths greater than 64 some IPv6 features like e.g. SLAAC no longer work. Use large prefixes only when you understand the implications.

IPv6 default gateway

If a router is attached to the current interface which provides Internet connectivity, you can enter its IP address here.



You can either enter a global address or a link local address (fe80:...).

IPv6 privacy extension (RFC3041)

A dynamic IPv6 address derived with SLAAC is based on the hardware address of the network card. So it can be tracked worldwide easily. Enable this option and SX-GATE will add a temporary random address which is preferred.

IPv6 prefix delegation

Enable this option to ask your provider for an additional IPv6 network prefix, which is then made available for internal networks by SX-GATE.

As soon as SX-GATE receives such a prefix, an entry is created in menu "Definitions > IP objects" which will be named after the interface (e.g. "ipv6_prefix_eth1" for "eth1"). Subdivide the prefix by adding entries of type "IPv6 prefix" or "IPv6 address" and make them refer to the prefix you received. You can use these objects in various configuration options.

Additional IPv6 addresses (aliases) / Cluster IP addresses

You can specify additional IPv6 addresses for the select network interface. These addresses may belong to the same IP subnet as the primary address or may belong to different networks (e.g. a ULA address).

14.1.2.2-C IPv6 router advertisement

Router advertisement (RA) is used to automatically configure IPv6 on network devices. Routers providing Internet connectivity announce their IP through RA and also the prefix length of the local network is determined by RA.



RA is even required when DHCPv6 is used to assign IP addresses. Neither the router IP nor the prefix length can be assigned with DHCPv6.

Router Advertisement

by unicast to individual clients

Select this option if you don't want to provide IPv6 connectivity for the whole network. Router advertisements will be sent to a list of manually configured clients.

enabled

Select this option and router advertisements will be sent to all network devices by multicast.

Router preference

The preference value can influence which router a client selects if it has multiple routers to choose from.



Some devices ignore this option or must be configured to consider it.

Send router advertisements to

If you decided that router advertisements should be sent by unicast to individual clients only, you have to configure the clients' link local addresses here. Link local addresses always start with "fe80:".

Prefixes for stateless address autoconfiguration

Add IPv6 prefixes clients may use for stateless automatic address configuration.

The prefix may be based on a dynamic prefix SX-GATE requested from your provider. Therefore you can also select from the list of prefixes defined in menu "Definitions > IP objects" when adding a new entry. In said menu you can also add entries of type "IPv6 prefix" yourself to e.g. subdivide the prefix SX-GATE received.

DHCPv6

This setting tells device if a DHCPv6 server is available or not.

no IP assignment, other information only (O flag)

Select this option if DHCP is used to provide information like the DNS server IPs only.

yes (M flag and O flag)

To use DHCPv6 to assign IPv6 addresses to devices, you must select this option.

DNS 1 (RDNSS)

The name server IPs can be announced with the RA extension RDNSS. As many devices don't support this extension yet, you should consider to use DHCPv6 for this purpose, too.

DNS suffix (DNSSL)

The DNS suffix for resolving host names without domain can be configured with RA. But this extension is also not widely supported yet.

Published routes

You can use router advertisements to announce routes to individual IPv6 prefixes.



Some devices ignore this option or must be configured to consider it.

14.1.2.2-D Routing

Policy Routing

On this tab you can configure static routing entries. You can add conventional routes, considering only the packet's destination, but also extended rules which include source addresses, protocol and port numbers (policy based routing).

Static routes must be added, if there are other networks which are not directly connected to the network card but can be addressed via a router. Specify the network address and the netmask of this remote network - this will automatically instruct the SX-GATE firewall to accept the network on this interface. Enter the IP address of the router as gateway.



The router's IP address must always be part of the same IP network as the IP of SX-GATE. The remote network in contrast must address a different network.



Use the special value 0.0.0.0 if the gateway IP is assigned with DHCP.

Rules for specific protocols or sources come into play if multiple internet links are available. One could for instance direct web traffic via an ADSL link while all the other traffic like emails and VPN uses an SDSL line.

The evaluation order is not based on the order in the list. The priority depends on how specific a rule is, taking in account the rules configured across all devices. Routes with all three parameters defined (i.e. protocol, source and destination) will be considered first. Rules with a destination take precedence over rules with protocol. These in turn have a higher priority than rules with a source. Within source and destination, rules are sorted by descending netmasks. The evaluation order of overlapping protocol specifications is not defined.

14.1.2.2-E Bandwidth management / QoS

For bandwidth management you have to fill in the available bandwidth. Uplink and downlink may be different (ADSL). Leave empty to disable bandwidth management on this interface. If you enter only one value, either for uplink or for downlink, bandwidth management will apply to packets in that direction only.



Specifying a wrong bandwidth can cause severe connection problems, especially if the actual bandwidth is lower than the configured one. Please ask your provider if you are uncertain.

Outbound bandwidth (uplink)

Enter the uplink bandwidth. For asymmetric connections this is usually the lower value. Bandwidth management will then process all outbound packets on this interface. The direction of the corresponding connection (inbound or outbound) doesn't matter.

Inbound bandwidth (downlink)

Enter the downlink bandwidth. For asymmetric connections this is usually the higher value. Bandwidth management will then process all inbound packets on this interface. The direction of the corresponding connection (inbound or outbound) doesn't matter. Leave empty if you don't need inbound bandwidth management.

Inbound bandwidth management is a contradiction in terms. Priority driven re-ordering of data packets waiting to be transmitted usually has to be done on the sending side of the (Internet) link. Only there it can be done in a reliable way. After all the packet has already been transmitted on the receiver side. However Internet connectivity with provider guaranteed Quality of Service / bandwidth management is often very expensive, so inbound bandwidth management is an option despite of its limitations.



Inbound bandwidth management reduces the available bandwidth by up to 20%. It requires that an adequate amount of the inbound data volume is covered by TCP connections.

Quality of Service (QoS) for Voice over IP (VoIP)

For VoIP the latency time, i.e. the time it takes for a voice packet to travel from sender to recipient, is very important. Hence SX-GATE's traffic shaper optimizes delivery of VoIP data packets with a special quality-of-service module.



In order to be recognized as VoIP packet, a data packet needs to be tagged according to Diffserv-Code-Point Expedited-Forwarding (DSCP EF).

The amount of bandwidth a single call requires depends on the codec that is used. The codec defines the compression of a VoIP call. The more compression is applied the less bandwidth is consumed, however also the quality decreases. The following table shows the net bandwidth required by commonly used codecs. Some codecs are used at different bandwidths. In this case the maximum bandwidth is given.

Codec	max. bandwidth (bit/s)
G.711	64000
G.722	64000
G.722.1	32000
G.723.1	6400
G.726	40000
G.728	16000
G.729	8000
GSM	13000
iLBC	15200

Max. number of concurrent calls

Enter the expected maximum number of simultaneous calls on this interface. It is used to calculate the overall bandwidth that needs to be reserved for VoIP traffic. The value "0" will disable this feature.



The total bandwidth of the link must not be exceeded.

Bitrate of the codec used

Enter the net bandwidth of the codec to be used. Take the codec with the largest bandwidth if different codecs are in use.



When calculating the total required bandwidth the system will automatically take the IP overhead into account. Lower bandwidth consumption causes more overhead.

Max. number of calls via IPSec

Enter the expected maximum number of simultaneous calls over VPN on this interface. It is used to calculate the overall bandwidth that needs to be reserved for VoIP traffic. The value "0" will disable this feature.



Wenn enabled, VoIP data packets will be expedited. This applies to the plain packet as well as to the VPN packet after encryption.



The total bandwidth of the link must not be exceeded.

Bitrate of the codec used in IPSec

Enter the net bandwidth of the codec to be used. Take the codec with the largest bandwidth if different codecs are in use.



When calculating the total required bandwidth the system will automatically take the IP and the IPSec overhead into account. Lower bandwidth consumption causes more overhead.

14.1.2.2-F Priorities

Use this feature to determine the priority of outgoing data packets. A proportional minimum bandwidth is assigned to each priority class. Unused bandwidth of a class will be used by classes with lower priority.

From a technical point of view the rules overwrite the ToS/DSCP field of matching IP packets. If a local application already takes care of this field, a rule would not be necessary for outbound packets. For inbound packets however the ToS/DSCP field is often modified in transit. So inbound traffic shaping usually requires rules.



Some ISPs will charge you for IP packets with certain ToS/DSCP values. Please check the ISPs terms of service.

The minimum bandwidth is assigned as follows: The bandwidth required for VoIP according to the configuration is reserved and subtracted from the total available bandwidth. Of the remaining bandwidth, 10% goes to empty TCP ACK packets, 50% to packets with high priority and 20% to packets with normal and low priority respectively.



Inbound traffic shaping treats all non-TCP packets as high priority.

Priorization of connections

Use this list to assign a higher or lower priority to specific data packets. If more than one rule matches, the priority of the topmost rule will be used.

The following inputs are available:

Protocol

Selects the IP protocol and port signature. With inbound bandwidth management, only TCP protocols will actually be processed.



Protocols are defined in menu "Definitions > Protocols".

Local IP/network

Viewed from the perspective of the selected interface, you can enter a local address here. This corresponds to the source IP of outbound packets (before SNAT) and the destination IP of inbound packets (before DNAT).



When SNAT or DNAT is involved, restricting a priority rule to specific local IPs usually requires two rules to catch both, in- and outbound packets: For inbound packets you would enter a SX-GATE IP, for outbound packets the internal IP (of the LAN client or the server addressed with DNAT).

Direction

Decide in which direction the port signature of the selected protocol has to be applied. Let's take the HTTP protocol as an example. The arrow "-->" means the HTTP port 80 is on the external side. So outbound bandwidth management will process packets to port 80, inbound bandwidth management packets from port 80. With "-->" you will get the opposite: Packets to port 80 are processed by

inbound, packets from port 80 by outbound bandwidth management. The double arrow "↔" combines both directions.

External IP/network

Viewed from the perspective of the selected interface, you can enter a remote address here. This corresponds to the destination IP of outbound packets and the source IP of inbound packets.

Priority

Select the priority for matching packets.

14.1.2.2-G Dynamic DNS

With dynamic DNS it is possible to address a device which it is connected to the Internet with a dynamic IP address. So with dynamic DNS you can access the services offered by SX-GATE despite of its dynamic IP address. Dynamic DNS uses ordinary hostnames (fully qualified domain names, FQDN) to address a device. Dynamic DNS is offered by many different providers. Some offer this service for free, others charge for it.



It takes a few seconds or even minutes until a new IP address becomes available via dynamic DNS.

If SX-GATE gets a dynamic IP address itself (ADSL interface with dynamic IP or Ethernet interface with IP address assigned via DHCP), please configure dynamic DNS in settings of the respective interface of menu "Modules > Network > Interfaces". SX-GATE will then update its dynamic DNS record once a new dial-up connection is established or when the IP changes.

If SX-GATE is situated behind a NAT router and it's the NAT router that actually get's the dynamic IP, the NAT router must forward inbound connections to SX-GATE (DNAT, portforwarding, exposed host). You should configure dynamic DNS in the NAT router, as only the NAT router knows its current dynamic IP. Only if this is not possible you may consider to configure dynamic DNS in SX-GATE menu "Modules > DNS > Settings". SX-GATE will then try to figure out the current dynamic IP of the NAT router at regular intervals, using an Internet based service.

Protocol

Unfortunately there's no standard protocol for updating dynamic DNS records. SX-GATE offers a bunch of different protocols. Please consult your dynamic DNS provider, which protocol is used and if SX-GATE supports it.

Update server of the DNS provider

Here you have to specify the server which accepts and processes the IP address update messages. This server may be different to the webserver of the dynamic DNS provider.

Update URL

Here you have to specify the update URL (aka "direct URL") for updating the dynamic IP address. The URL may have the placeholders <host>, <ipaddr>, <username> and <password> that will be substituted by the dynamic DNS name, the IP address, the username and the password, i.e.: `http://dynupdate.exampledyndns.com/nic/update?hostname=<domain>&myip=<ipaddr>`

Dynamic DNS hostname of SX-GATE

Usually the providers allow you to manage multiple dynamic DNS names with a single user account. Therefore you have to supply SX-GATE's complete dynamic DNS name here (including the domain).

Login

No dynamic DNS updates without authentication. Please enter the login for the corresponding account here.

Password

Finally you have to specify the password for the dynamic DNS account.

Update now

`ref link="#main_modules#sm_devices#tr_dyndns_checkdd"/>`

14.1.2.2-H Packet monitor

Local networks

Some IDS rules distinguish between internal and external IP addresses. Here you configure which addresses are considered to be internal.

14.1.2.2-I Server addresses

Some IDS rules are tailor-made for specific server protocols. Enter the IP addresses of systems offering the respective services. If no addresses are provided, the IDS expects that this service is available from all internal addresses, which might have a negative impact on the system's performance.

14.1.2.2-J Additional rulesets

Some important rulesets are always enabled. The rulesets on this tab may be added as appropriate.

Web server attacks

Enables specific rules to detect attacks against web and FTP servers.

Mail server attacks

Enables specific rules to detect attacks against SMTP, IMAP4 and POP3 servers.

Internet server attacks

Enables specific rules to detect attacks against other typical internet services like DNS or SIP (VoIP).

LAN server attacks

Enables specific rules to detect attacks against services usually active in LAN networks. This includes Windows protocols, UNIX RPC and SQL servers.



The majority of rules apply only to access from outside the local networks.

Extended browser surveillance

This ruleset monitors web browsers. It alerts if it detects attacks or vulnerable software components.

Non-business activities

Logs activities which are usually not related to normal business operations. This includes e.g. online games, chat and the use of peer-to-peer software.

Connections with Tor network

This switch enables a list of IP addresses that belong to the Tor anonymization network.

14.1.2.3 VLAN 802.1Q (vlan)

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

14.1.2.3-A Settings.....	298
14.1.2.3-B IP addresses.....	299
14.1.2.3-C IPv6 router advertisement.....	301
14.1.2.3-D Routing.....	302
14.1.2.3-E Bandwidth management / QoS.....	303
14.1.2.3-F Priorities.....	306
14.1.2.3-G Dynamic DNS.....	307

Interface mode

Select how the VLAN interface should be used.

standalone VLAN

In this mode the VLAN interface will get its own IP configuration.

additional Bridge port

With this option you can connect the VLAN interface with a bridge.



To create a new bridge, please select option "standalone VLAN" and enable bridging there.

IPv4 mode

Select the kind of IPv4 connectivity.

automatic IP (DHCP)

For example if a cable modem is used to connect SX-GATE with the Internet, the IP address might be assigned dynamically by DHCP. Select the corresponding option in this case.

Dual-Stack Lite (DS-Lite)

This option is only available if IPv6 is enabled and the interface is not configured as a bridge. With DS-Lite your Internet connection is IPv6 only. IPv4 packets are tunneled via the IPv6 connection to a specific gateway of your provider. This is where the IPv4 packet will get its final sender address (Carrier-grade NAT) and enter the IPv4 Internet.

IPv6 mode

Select the kind of IPv6 connectivity.

manual IP

If this option is selected, all IPv6 parameters have to be configured manually. Router advertisements will be ignored.

automatic IP (SLAAC/DHCPv6)

Choose this option and SX-GATE will automatically determine its IPv6 configuration based on the router advertisements it receives.

14.1.2.3-A Settings

Description

This input serves for documentation purposes only.

Connected to network card

Select the name of the network card to which the VLAN device will be bound.

Bridge

Much like a switch, a bridge connects multiple network segments to one large network. With SX-GATE you can even restrict communication with firewall rules. So you can e.g. configure SX-GATE as a stealth firewall between the LAN and an Internet router.

Please note that for connections routed from outside into the bridge the actual target bridge port is unknown by the time it is filtered in the firewall. So firewall forwarding rules, rules for outbound connections (source is a SX-GATE service) and SNAT rules for routed connections always have to be configured for the bridge as a whole and not for each bridge port individually. Even a separate target zone has to be selected for the bridge as a whole.

In contrast you can configure rules for intra bridge traffic, i.e. traffic which passes from one bridge port to another, by port. The same applies to DNAT rules and rules for inbound connections (destination is a SX-GATE service). For each port an individual firewall zone is selected. As source zone it is even available outside of the bridge, whenever a connection is routed from the bridge to an interface outside of the bridge.

Spanning tree protocol

If you have connected multiple switches and bridges in with redundant links, you must enable the Spanning Tree Protocol (STP) on all switches and bridges. Using STP the devices will make sure that no loops occur within the network topology and will react to link failures.

Route known destinations

When enabled, some packets won't pass the bridge but will be routed by SX-GATE instead. It affects packets to destination IPs which are configured on other SX-GATE interfaces, VPNs or for which a static route exists.



Enabling this option makes sense only if SX-GATE is used as a transparent firewall between client devices and a router which is the standard gateway of these clients.



Firewall rules for these connections have to be configured in submenu "Policies" and not in submenu "Bridge".

Add to bridge

Please select the bridge this VLAN interface should be connected with.

14.1.2.3-B IP addresses

IPv4 address

Specify the IPv4 address that the corresponding SX-GATE interface should use as its own address.



The IP address assigned here may not be part of an IP subnet which has already been assigned to an other interface.

IPv4 netmask

Here you have to specify the netmask corresponding to the IP address.

IPv4 default gateway

Simplifying things, a default gateway is a router linking to the Internet. If such a router is connected to this interface you have to enter its IP address here. In "Modules > Network > Settings" you can select which interface is to be used to connect to the Internet. Selecting this interface, SX-GATE will setup a default router via the gateway specified here.

Additional IPv4 addresses (aliases) / Cluster IP addresses

You can specify additional IP addresses for the select network interface. You can add addresses belonging to the same IP subnet as the primary address. This is useful

for example to bind multiple Internet IP addresses to SX-GATE and then use firewall rules to redirect connections to different internal addresses. However you may also add addresses of different networks if multiple IP subnets share the same physical Ethernet.

DS-Lite Address-Family-Transition-Router (AFTR)

In dual stack light Internet links IPv4 packets are tunneled via IPv6. The tunnel endpoint on the provider side is a special router. If its address isn't advertised with DHCP you can enter the address here.

IPv6 address

Enter an IPv6 address for this interface. If the address is based on a delegated prefix, please add an entry of type "IPv6 address" in menu "Definitions > IP objects" which refers to the prefix.

IPv6 prefix length

The IPv6 prefix length is the equivalent to IPv4 netmasks. The typical prefix length is 64.



With prefix lengths greater than 64 some IPv6 features like e.g. SLAAC no longer work. Use large prefixes only when you understand the implications.

IPv6 default gateway

If a router is attached to the current interface which provides Internet connectivity, you can enter its IP address here.



You can either enter a global address or a link local address (fe80:...).

IPv6 privacy extension (RFC3041)

A dynamic IPv6 address derived with SLAAC is based on the hardware address of the network card. So it can be tracked worldwide easily. Enable this option and SX-GATE will add a temporary random address which is preferred.

IPv6 prefix delegation

Enable this option to ask your provider for an additional IPv6 network prefix, which is then made available for internal networks by SX-GATE.

As soon as SX-GATE receives such a prefix, an entry is created in menu "Definitions > IP objects" which will be named after the interface (e.g. "ipv6_prefix_eth1" for "eth1"). Subdivide the prefix by adding entries of type "IPv6 prefix" or "IPv6 address" and make

them refer to the prefix you received. You can use these objects in various configuration options.

Additional IPv6 addresses (aliases) / Cluster IP addresses

You can specify additional IPv6 addresses for the select network interface. These addresses may belong to the same IP subnet as the primary address or may belong to different networks (e.g. a ULA address).

14.1.2.3-C IPv6 router advertisement

Router advertisement (RA) is used to automatically configure IPv6 on network devices. Routers providing Internet connectivity announce their IP through RA and also the prefix length of the local network is determined by RA.



RA is even required when DHCPv6 is used to assign IP addresses. Neither the router IP nor the prefix length can be assigned with DHCPv6.

Router Advertisement

by unicast to individual clients

Select this option if you don't want to provide IPv6 connectivity for the whole network. Router advertisements will be sent to a list of manually configured clients.

enabled

Select this option and router advertisements will be sent to all network devices by multicast.

Router preference

The preference value can influence which router a client selects if it has multiple routers to choose from.



Some devices ignore this option or must be configured to consider it.

Send router advertisements to

If you decided that router advertisements should be sent by unicast to individual clients only, you have to configure the clients' link local addresses here. Link local addresses always start with "fe80:".

Prefixes for stateless address autoconfiguration

Add IPv6 prefixes clients may use for stateless automatic address configuration.

The prefix may be based on a dynamic prefix SX-GATE requested from your provider. Therefore you can also select from the list of prefixes defined in menu "Definitions > IP objects" when adding a new entry. In said menu you can also add entries of type "IPv6 prefix" yourself to e.g. subdivide the prefix SX-GATE received.

DHCPv6

This setting tells device if a DHCPv6 server is available or not.

no IP assignment, other information only (O flag)

Select this option if DHCP is used to provide information like the DNS server IPs only.

yes (M flag and O flag)

To use DHCPv6 to assign IPv6 addresses to devices, you must select this option.

DNS 1 (RDNSS)

The name server IPs can be announced with the RA extension RDNSS. As many devices don't support this extension yet, you should consider to use DHCPv6 for this purpose, too.

DNS suffix (DNSSL)

The DNS suffix for resolving host names without domain can be configured with RA. But this extension is also not widely supported yet.

Published routes

You can use router advertisements to announce routes to individual IPv6 prefixes.



Some devices ignore this option or must be configured to consider it.

14.1.2.3-D Routing

Policy Routing

On this tab you can configure static routing entries. You can add conventional routes, considering only the packet's destination, but also extended rules which include source addresses, protocol and port numbers (policy based routing).

Static routes must be added, if there are other networks which are not directly connected to the network card but can be addressed via a router. Specify the network address and the netmask of this remote network - this will automatically instruct the SX-GATE firewall to accept the network on this interface. Enter the IP address of the router as gateway.



The router's IP address must always be part of the same IP network as the IP of SX-GATE. The remote network in contrast must address a different network.

Rules for specific protocols or sources come into play if multiple internet links are available. One could for instance direct web traffic via an ADSL link while all the other traffic like emails and VPN uses an SDSL line.

The evaluation order is not based on the order in the list. The priority depends on how specific a rule is, taking in account the rules configured across all devices. Rules with all three parameters defined (i.e. protocol, source and destination) will be considered first. Rules with a destination take precedence over rules with protocol. These in turn have a higher priority than rules with a source. Within source and destination, rules are sorted by descending netmasks. The evaluation order of overlapping protocol specifications is not defined.

14.1.2.3-E Bandwidth management / QoS

For bandwidth management you have to fill in the available bandwidth. Uplink and downlink may be different (ADSL). Leave empty to disable bandwidth management on this interface. If you enter only one value, either for uplink or for downlink, bandwidth management will apply to packets in that direction only.



Specifying a wrong bandwidth can cause severe connection problems, especially if the actual bandwidth is lower than the configured one. Please ask your provider if you are uncertain.

Outbound bandwidth (uplink)

Enter the uplink bandwidth. For asymmetric connections this is usually the lower value. Bandwidth management will then process all outbound packets on this interface. The direction of the corresponding connection (inbound or outbound) doesn't matter.

Inbound bandwidth (downlink)

Enter the downlink bandwidth. For asymmetric connections this is usually the higher value. Bandwidth management will then process all inbound packets on this interface.

The direction of the corresponding connection (inbound or outbound) doesn't matter. Leave empty if you don't need inbound bandwidth management.

Inbound bandwidth management is a contradiction in terms. Priority driven re-ordering of data packets waiting to be transmitted usually has to be done on the sending side of the (Internet) link. Only there it can be done in a reliable way. After all the packet has already been transmitted on the receiver side. However Internet connectivity with provider guaranteed Quality of Service / bandwidth management is often very expensive, so inbound bandwidth management is an option despite of its limitations.



Inbound bandwidth management reduces the available bandwidth by up to 20%. It requires that an adequate amount of the inbound data volume is covered by TCP connections.

Quality of Service (QoS) for Voice over IP (VoIP)

For VoIP the latency time, i.e. the time it takes for a voice packet to travel from sender to recipient, is very important. Hence SX-GATE's traffic shaper optimizes delivery of VoIP data packets with a special quality-of-service module.



In order to be recognized as VoIP packet, a data packet needs to be tagged according to Diffserv-Code-Point Expedited-Forwarding (DSCP EF).

The amount of bandwidth a single call requires depends on the codec that is used. The codec defines the compression of a VoIP call. The more compression is applied the less bandwidth is consumed, however also the quality decreases. The following table shows the net bandwidth required by commonly used codecs. Some codecs are used at different bandwidths. In this case the maximum bandwidth is given.

Codec	max. bandwidth (bit/s)
G.711	64000
G.722	64000
G.722.1	32000
G.723.1	6400
G.726	40000
G.728	16000
G.729	8000

Codec	max. bandwidth (bit/s)
GSM	13000
iLBC	15200

Max. number of concurrent calls

Enter the expected maximum number of simultaneous calls on this interface. It is used to calculate the overall bandwidth that needs to be reserved for VoIP traffic. The value "0" will disable this feature.



The total bandwidth of the link must not be exceeded.

Bitrate of the codec used

Enter the net bandwidth of the codec to be used. Take the codec with the largest bandwidth if different codecs are in use.



When calculating the total required bandwidth the system will automatically take the IP overhead into account. Lower bandwidth consumption causes more overhead.

Max. number of calls via IPSec

Enter the expected maximum number of simultaneous calls over VPN on this interface. It is used to calculate the overall bandwidth that needs to be reserved for VoIP traffic. The value "0" will disable this feature.



Wenn enabled, VoIP data packets will be expedited. This applies to the plain packet as well as to the VPN packet after encryption.



The total bandwidth of the link must not be exceeded.

Bitrate of the codec used in IPSec

Enter the net bandwidth of the codec to be used. Take the codec with the largest bandwidth if different codecs are in use.



When calculating the total required bandwidth the system will automatically take the IP and the IPSec overhead into account. Lower bandwidth consumption causes more overhead.

14.1.2.3-F Priorities

Use this feature to determine the priority of outgoing data packets. A proportional minimum bandwidth is assigned to each priority class. Unused bandwidth of a class will be used by classes with lower priority.

From a technical point of view the rules overwrite the ToS/DSCP field of matching IP packets. If a local application already takes care of this field, a rule would not be necessary for outbound packets. For inbound packets however the ToS/DSCP field is often modified in transit. So inbound traffic shaping usually requires rules.



Some ISPs will charge you for IP packets with certain ToS/DSCP values. Please check the ISPs terms of service.

The minimum bandwidth is assigned as follows: The bandwidth required for VoIP according to the configuration is reserved and subtracted from the total available bandwidth. Of the remaining bandwidth, 10% goes to empty TCP ACK packets, 50% to packets with high priority and 20% to packets with normal and low priority respectively.



Inbound traffic shaping treats all non-TCP packets as high priority.

Priorization of connections

Use this list to assign a higher or lower priority to specific data packets. If more than one rule matches, the priority of the topmost rule will be used.

The following inputs are available:

Protocol

Selects the IP protocol and port signature. With inbound bandwidth management, only TCP protocols will actually be processed.



Protocols are defined in menu "Definitions > Protocols".

Local IP/network

Viewed from the perspective of the selected interface, you can enter a local address here. This corresponds to the source IP of outbound packets (before SNAT) and the destination IP of inbound packets (before DNAT).



When SNAT or DNAT is involved, restricting a priority rule to specific local IPs usually requires two rules to catch both, in- and outbound packets: For inbound packets you would enter a SX-GATE IP, for outbound packets the internal IP (of the LAN client or the server addressed with DNAT).

Direction

Decide in which direction the port signature of the selected protocol has to be applied. Let's take the HTTP protocol as an example. The arrow "-->" means the HTTP port 80 is on the external side. So outbound bandwidth management will process packets to port 80, inbound bandwidth management packets from port 80. With "-->" you will get the opposite: Packets to port 80 are processed by inbound, packets from port 80 by outbound bandwidth management. The double arrow "<-->" combines both directions.

External IP/network

Viewed from the perspective of the selected interface, you can enter a remote address here. This corresponds to the destination IP of outbound packets and the source IP of inbound packets.

Priority

Select the priority for matching packets.

14.1.2.3-G Dynamic DNS

With dynamic DNS it is possible to address a device which it is connected to the Internet with a dynamic IP address. So with dynamic DNS you can access the services offered by SX-GATE despite of its dynamic IP address. Dynamic DNS uses ordinary hostnames (fully qualified domain names, FQDN) to address a device. Dynamic DNS is offered by many different providers. Some offer this service for free, others charge for it.



It takes a few seconds or even minutes until a new IP address becomes available via dynamic DNS.

If SX-GATE gets a dynamic IP address itself (ADSL interface with dynamic IP or Ethernet interface with IP address assigned via DHCP), please configure dynamic DNS in settings of the respective interface of menu "Modules > Network > Interfaces". SX-GATE will then update its dynamic DNS record once a new dial-up connection is established or when the IP changes.

If SX-GATE is situated behind a NAT router and it's the NAT router that actually get's the dynamic IP, the NAT router must forward inbound connections to SX-GATE (DNAT, portforwarding, exposed host). You should configure dynamic DNS in the NAT router, as only the NAT router knows its current dynamic IP. Only if this is not possible you may consider to configure dynamic DNS in SX-GATE menu "Modules > DNS > Settings". SX-GATE will then try to figure out the current dynamic IP of the NAT router at regular intervals, using an Internet based service.

Protocol

Unfortunately there's no standard protocol for updating dynamic DNS records. SX-GATE offers a bunch of different protocols. Please consult your dynamic DNS provider, which protocol is used and if SX-GATE supports it.

Update server of the DNS provider

Here you have to specify the server which accepts and processes the IP address update messages. This server may be different to the webserver of the dynamic DNS provider.

Update URL

Here you have to specify the update URL (aka "direct URL") for updating the dynamic IP address. The URL may have the placeholders <host>, <ipaddr>, <username> and <password> that will be substituted by the dynamic DNS name, the IP address, the username and the password, i.e.: `http://dynupdate.exampledyndns.com/nic/update?hostname=<domain>&myip=<ipaddr>`

Dynamic DNS hostname of SX-GATE

Usually the providers allow you to manage multiple dynamic DNS names with a single user account. Therefore you you have to supply SX-GATE's complete dynamic DNS name here (including the domain).

Login

No dynamic DNS updates without authentication. Please enter the login for the corresponding account here.

Password

Finally you have to specify the password for the dynamic DNS account.

Update now

`ref link="#main_modules#sm_devices#tr_dyndns_checkdd"/>`

14.1.2.4 WLAN (wlan)

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

14.1.2.4-A Settings.....	309
14.1.2.4-B IP addresses.....	312
14.1.2.4-C IPv6 router advertisement.....	313
14.1.2.4-D Authentication.....	315
14.1.2.4-E MAC filter.....	316

Interface mode

Select how the WLAN interface should be used.

standalone WLAN

In this mode the WLAN interface will get its own IP configuration.

additional Bridge port

With this option you can connect the WLAN interface with a bridge.



To create a new bridge, please select option "standalone WLAN" and enable bridging there.

IPv6 mode

Select the kind of IPv6 connectivity.

manual IP

If this option is selected, all IPv6 parameters have to be configured manually. Router advertisements will be ignored.

14.1.2.4-A Settings

Description

This input serves for documentation purposes only.

Countrycode

Here you can see the country code the WLAN adapter is configured for. It controls the allowed channels and the transmit power.



When operating a WLAN adapter with the wrong country code setting it may use parameters which are prohibited in your country. Please contact your SX-GATE dealer if this setting is incorrect.

SSID

Please enter the name of your WLAN.

Hide SSID

When enabled, the name of the WLAN is not announced. Clients need to know the name in order to connect with the WLAN.



Tools are available which make it easy for an attacker to find the hidden WLAN.

Disable client isolation

Client isolation is a security mechanism that prevents WLAN users in the same networking from being able to communicate with one another. This is particularly important for guest networks, or networks where users bring their own devices.

When this option is enabled, WLAN users have direct unprotected access to one another.

Radio frequency band

Please select the requested frequency band.

Channel (2.4 GHz)

The channel may be selected automatically or you can configure a specific channel.



The available channels depend on the selected country code.

Channel (5 GHz)

Only very few channels are available for static channel selection as most channels in the 5 GHz band may collide with radar sites. We recommend to use the automatic channel selection, combined with radar detection and Dynamic Frequency Selection (DFS) to enable the full range of 5 GHz channels.



The available channels depend on the selected country code.

Radar detection / DFS

Activate radar detection and Dynamic Frequency Selection (DFS) according to IEEE 802.11h to enable channels 52-64 and 100-140 in the 5 GHz frequency band.



The actually available channels depend on the selected country code.

IEEE 802.11n

You can enable IEEE 802.11n mode here which gives you higher throughput by using multiple parallel data streams via multiple antennas.

20 MHz channels

With this setting the usual channel width of 20 MHz will be used.

40 MHz channels

To get an even higher throughput you can extend the bandwidth per channel to 40 MHz.



When operating in the 2.4 GHz band this will use about half of the available frequencies which makes it difficult to run without overlapping other WLAN in your area.

Bridge

Much like a switch, a bridge connects multiple network segments to one large network. With SX-GATE you can even restrict communication with firewall rules. So you can e.g. configure SX-GATE as a stealth firewall between the LAN and an Internet router.

Please note that for connections routed from outside into the bridge the actual target bridge port is unknown by the time it is filtered in the firewall. So firewall forwarding rules, rules for outbound connections (source is a SX-GATE service) and SNAT rules for routed connections always have to be configured for the bridge as a whole and not for each bridge port individually. Even a separate target zone has to be selected for the bridge as a whole.

In contrast you can configure rules for intra bridge traffic, i.e. traffic which passes from one bridge port to another, by port. The same applies to DNAT rules and rules for inbound connections (destination is a SX-GATE service). For each port an individual

firewall zone is selected. As source zone it is even available outside of the bridge, whenever a connection is routed from the bridge to an interface outside of the bridge.

Spanning tree protocol

If you have connected multiple switches and bridges in with redundant links, you must enable the Spanning Tree Protocol (STP) on all switches and bridges. Using STP the devices will make sure that no loops occur within the network topology and will react to link failures.

Route known destinations

When enabled, some packets won't pass the bridge but will be routed by SX-GATE instead. It affects packets to destination IPs which are configured on other SX-GATE interfaces, VPNs or for which a static route exists.



Enabling this option makes sense only if SX-GATE is used as a transparent firewall between client devices and a router which is the standard gateway of these clients.



Firewall rules for these connections have to be configured in submenu "Policies" and not in submenu "Bridge".

Add to bridge

Please select the bridge this WLAN interface should be connected with.

14.1.2.4-B IP addresses

IPv4 address

Specify the IPv4 address that the corresponding SX-GATE interface should use as its own address.



The IP address assigned here may not be part of an IP subnet which has already been assigned to an other interface.

IPv4 netmask

Here you have to specify the netmask corresponding to the IP address.

Additional IPv4 addresses (aliases) / Cluster IP addresses

You can specify additional IP addresses for the select WLAN interface. You can add addresses belonging to the same IP subnet as the primary address. However you may also add addresses of different networks if multiple IP subnets share the same WLAN.

IPv6 address

Enter an IPv6 address for this interface. If the address is based on a delegated prefix, please add an entry of type "IPv6 address" in menu "Definitions > IP objects" which refers to the prefix.

IPv6 prefix length

The IPv6 prefix length is the equivalent to IPv4 netmasks. The typical prefix length is 64.



With prefix lengths greater than 64 some IPv6 features like e.g. SLAAC no longer work. Use large prefixes only when you understand the implications.

Additional IPv6 addresses (aliases) / Cluster IP addresses

You can specify additional IPv6 addresses for the select WLAN interface. These addresses may belong to the same IP subnet as the primary address or may belong to different networks (e.g. a ULA address).

14.1.2.4-C IPv6 router advertisement

Router advertisement (RA) is used to automatically configure IPv6 on network devices. Routers providing Internet connectivity announce their IP through RA and also the prefix length of the local network is determined by RA.



RA is even required when DHCPv6 is used to assign IP addresses. Neither the router IP nor the prefix length can be assigned with DHCPv6.

Router Advertisement

by unicast to individual clients

Select this option if you don't want to provide IPv6 connectivity for the whole network. Router advertisements will be sent to a list of manually configured clients.

enabled

Select this option and router advertisements will be sent to all network devices by multicast.

Router preference

The preference value can influence which router a client selects if it has multiple routers to choose from.



Some devices ignore this option or must be configured to consider it.

Send router advertisements to

If you decided that router advertisements should be sent by unicast to individual clients only, you have to configure the clients' link local addresses here. Link local addresses always start with "fe80:".

Prefixes for stateless address autoconfiguration

Add IPv6 prefixes clients may use for stateless automatic address configuration.

The prefix may be based on a dynamic prefix SX-GATE requested from your provider. Therefore you can also select from the list of prefixes defined in menu "Definitions > IP objects" when adding a new entry. In said menu you can also add entries of type "IPv6 prefix" yourself to e.g. subdivide the prefix SX-GATE received.

DHCPv6

This setting tells device if a DHCPv6 server is available or not.

no IP assignment, other information only (O flag)

Select this option if DHCP is used to provide information like the DNS server IPs only.

yes (M flag and O flag)

To use DHCPv6 to assign IPv6 addresses to devices, you must select this option.

DNS 1 (RDNSS)

The name server IPs can be announced with the RA extension RDNSS. As many devices don't support this extension yet, you should consider to use DHCPv6 for this purpose, too.

DNS suffix (DNSSL)

The DNS suffix for resolving host names without domain can be configured with RA. But this extension is also not widely supported yet.

Published routes

You can use router advertisements to announce routes to individual IPv6 prefixes.



Some devices ignore this option or must be configured to consider it.

14.1.2.4-D Authentication

Authentication and encryption

Please select an authentication and encryption method. For pairwise encryption, AES (CCMP) is used for all methods.



WPA3 is only supported by newer hardware and also requires current software versions (iOS 13/iPadOS 13, Android 10 or Windows 10 version 1903 or later).

Management Frame Protection (MFP)

Management Frame Protection (MFP) is used to protect management frames that have to be transmitted unencrypted. If this option is set to "Required", only clients that support Management Frame Protection (MFP) can connect. With the "Optional" setting, non-MFP-capable clients can also connect, but without the additional protection.



For WPA3-SAE, the "Management Frame Protection (MFP)" is a prerequisite and can therefore not be disabled. It is recommended to select the option "Required" here.

WPA Passphrase

Please enter the WLAN password here. It must be at least 8 characters long. We recommend a rather complicated passphrase with at least 32 characters instead of a simple password. Use lowercase and uppercase letters, digits and special characters and avoid words that can be found in a dictionary.

Authentication server address

Please enter the authentication server here.

Authentication server port

This is the port where the authentication server can be reached.

Authentication server passphrase

Enter the secret key used by SX-GATE to log on to the authentication server.

Accounting

Enable the Accounting here.

Accounting server address

Please enter the accounting server here.

Accounting server port

This is the port where the accounting server can be reached.

Accounting server passphrase

Enter the secret key used by SX-GATE to log on to the accounting server.

NAS ID

The NAS ID is used in the communication with the authentication/account server. Since each SSID has its own NAS ID, it should be as unique as possible. For example, a combination of SSID and FQDN.

14.1.2.4-E MAC filter

If the MAC filter is enabled, a WLAN client will be accepted only if its MAC address has been whitelisted here.



The MAC filter provides just limited protection as the MAC address of a client can be spoofed by advanced users or attackers.

MAC filter

Enable the MAC filter here.

Accepted MAC addresses

To grant access, please enter the MAC addresses of the clients here. You can also refer to objects of type "Host", defined in menu "Definitions > IP objects". Only those

objects including a MAC address will be considered. Any IP addresses configured in the object will be ignored.

14.1.2.5 L2TP

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

14.1.2.5-A IP addresses.....	317
14.1.2.5-B DNS.....	318

14.1.2.5-A IP addresses

This interface is meant to be used in combination with the IPSEC VPN server of SX-GATE. Nevertheless it is also possible to connect to the L2TP server without using a VPN connection.

Description

This input serves for documentation purposes only.

Local IP address

Specify the IP address used by SX-GATE on this interface. It suggests itself to use the LAN IP address here.

Remote IP address

Insert the IP addresses which SX-GATE will assign to the peers. If these IP addresses belong to the IP range of one of the networks which are directly connected to SX-GATE, a proxy ARP entry will be added as well. With this, the remote device will become a member of the network.



The number of IP addresses specified here will determine the maximum number of concurrent L2TP connections.

You can add a block of addresses by entering a network address with the corresponding netmask. If for example the LAN network is 192.168.0.0/24, the entry 192.168.0.160/27 will add the 32 IP addresses from the range 192.168.0.160 to 192.168.0.191.



The address ranges must not include network or broadcast addresses of a local ethernet, except for the network and broadcast addresses of a class C network (*.0 and *.255). The system will exclude these automatically.

14.1.2.5-B DNS

Assign DNS server

With this setting you will determine which name server the client will use.

Secondary DNS

If required, you can enter an additional name server here.

WINS 1

Here you can specify the primary WINS server. WINS is required by Windows to resolve hostnames in multi-subnetted networks.

WINS 2

Here you can enter a secondary WINS server.

14.1.2.6 Wireguard (wg)

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

14.1.2.6-A General.....	318
14.1.2.6-B Connections.....	320

14.1.2.6-A General

Description

This input serves for documentation purposes only.

Private key

Pick one of the X25519 keys managed in menu "System > Certificate manager > Keyring".

Import connection

Import a Wireguard configuration file or a SX-GATE Wireguard configuration package.



This option is only available if no private key has been selected yet.

Public key

The corresponding public key is displayed here. To configure a VPN, the peer needs to know your public key.

Local port

Here you have to enter the wireguard server's port number.



You need to add a custom protocol definition for this UDP port and grant Internet access to SX-GATE for this protocol.



When running multiple wireguard interfaces, they must either differ by port. You must not use a port number which is already in use by other UDP services of SX-GATE.

Virtual IPv4 address

The IP address configured here is set as source IP when applying NAT to outbound connections on the Wireguard interface and when SX-GATE itself initiates connections via the VPN.



You can either configure an IP address which is already set for an other SX-GATE interface or you can set an IP from a network which is not used otherwise.

Virtual IPv6 address

Configure an IPv6 address if SX-GATE itself is going to initiate IPv6 connections via the VPN.

Keepalive interval

If configured, SX-GATE regularly sends empty packets via VPN. This can be necessary if a NAT router is situated in front of SX-GATE that otherwise would close an idle connection for inbound packets.



The peer will not reply to these packets.

14.1.2.6-B Connections**Peers**

Create a new entry for every VPN you want to configure via the selected Wireguard interface. The following parameters can be configured:

Name or group/name

For your reference. If you have to configure a lot of connections you can use the separator character '/' to group them.

Address of peer and Port

If configured, SX-GATE will try to initiate the connection (Wireguard parameter "Endpoint").

Client IP or remote networks

Enter the remote IP or network you want to connect with via VPN. SX-GATE will route packets to these addresses into the VPN. Packets received via VPN will be accepted only if the source address matches (Wireguard parameter "AllowedIPs").



To configure multiple addresses, please create an IP group in menu "Definitions > IP objects", then select the group here.

Preshared key

As an additional layer of protection, the VPN may be secured by a symmetric key. The same key has to be configured on both sides of the tunnel. In contrast to the public key, this key must be shared via a secured channel.

Public key

Enter the public key of the peer.

Add new connection to a client with configuration export for client

With this wizard you can add a new connection to a client like e.g. a smartphone or a PC and at the same time you can export the settings to configure this client.

To configure mobile devices, a QR code is displayed. A Wireguard configuration file (*.conf) is available for export, too.



A dedicated connection has to be configured for each client.

Settings for the local SX-GATE

The settings on this screen will be added to the Wireguard connection list of your local SX-GATE. Some settings will also become part of the exported configuration for the peer.

Connection name or group/name

Client IP for communication via Wireguard

Enter the IP the client shall use within the encrypted Wireguard connection (on the client: Wireguard parameter "Address"). SX-GATE will route packets to this IP into the VPN. Packets received via VPN will be accepted only if the source address matches (on SX-GATE: Wireguard parameter "AllowedIPs").



Please enter unique, otherwise unused IP address for each client. The address may not be part of any other local network like e.g. the LAN.

Preshared key

Public key of peer

Settings for peer

On this screen you will prepare the settings for the peer. They will become part of the exported configuration.

Internet address of your local SX-GATE

The peer will later connect to this address (Wireguard parameter "Endpoint" in peer's configuration file).

Local networks

Enter all local IPs and networks the peer should be able to reach via VPN. The peer will route packets to these destination addresses into the VPN and will accept packets from the VPN with these source addresses only (Wireguard parameter "AllowedIPs" in peer's configuration file).



The peer can change this setting at will in an attempt to reach other networks. If you don't trust the peer, you should use firewall rules to make sure the peer can address only those systems it is supposed to talk with.

Preshared key

The PSK is stored in the local SX-GATE settings and it is exported to the peer.

Public key of your local SX-GATE

The public key of your local SX-GATE will be exported to the peer.

IP address of client

The client will assign this IP to its Wireguard interface and uses it within the encrypted Wireguard connection (Wireguard parameter "Address" in peer's configuration file).

Assign DNS IP

You can try to assign a DNS server to the peer with this setting (Wireguard parameter "DNS" in peer's configuration file).

Connection-specific DNS suffix

You can optionally set a connection-specific DNS suffix on the client (Domainname in Wireguard parameter "DNS" of peer's configuration file).

Keepalive interval

You can try to enable the keepalive feature on the peer with this setting. At regular time intervals the peer would then send empty packets via VPN which aren't answered. This can be necessary if a NAT router is situated in front of peer that otherwise would close an idle connection for inbound packets (Wireguard parameter "PersistentKeepalive" in peer's configuration file).

Add new connection to a router with configuration export for peer

With this wizard you can add a new connection and at the same time export the settings to configure the peer. If the peer is also a SX-GATE, you should export an encrypted installation package. To configure mobile devices a QR code is displayed. Finally a Wireguard configuration file (*.conf) can be exported, too.

Settings for the local SX-GATE

The settings on this screen will be added to the Wireguard connection list of your local SX-GATE. Some settings will also become part of the exported configuration for the peer.

Connection name or group/name

For your reference. If you have to configure a lot of connections you can use the separator character '/' to group them.

Address of peer

If you configure the IP address or hostname of the peer and also configure a port number in the next field, SX-GATE will try to initiate the connection (Wireguard parameter "Endpoint").

corresponding port (static IP only)

Will be ignored if option "dynamic" is selected as "Address of peer" (will be part of parameter "Endpoint" in the local Wireguard configuration file and will be set as "ListenPort" in the peer's configuration file).

Remote networks

Enter the remote network you want to connect with via VPN. SX-GATE will route packets to these addresses into the VPN. Packets received via VPN will be accepted only if the source address matches (Wireguard parameter "AllowedIPs").



To configure multiple addresses, please create an IP group in menu "Definitions > IP objects", then select the group here.

Preshared key

As an additional layer of protection, the VPN may be secured by a symmetric key. The same key has to be configured on both sides of the tunnel. In contrast to the public key, this key must be shared via a secured channel.

Public key of peer

In the local SX-GATE settings the new connection will be associated with the public key of the peer. The corresponding private key has just been generated and will be part of the exported configuration.

Settings for peer

On this screen you will prepare the settings for the peer. They will become part of the exported configuration.

Comment

This setting will only be part of SX-GATE setup packages.

Internet address of your local SX-GATE

The peer will later connect to this address (Wireguard parameter "Endpoint" in peer's configuration file).

Local networks

Enter all local IPs and networks the peer should be able to reach via VPN. The peer will route packets to these destination addresses into the VPN and will accept packets from the VPN with these source addresses only (Wireguard parameter "AllowedIPs" in peer's configuration file).



The peer can change this setting at will in an attempt to reach other networks. If you don't trust the peer, you should use firewall rules to make sure the peer can address only those systems it is supposed to talk with.

Preshared key

The PSK is stored in the local SX-GATE settings and it is exported to the peer.

Public key of your local SX-GATE

The public key of your local SX-GATE will be exported to the peer.

Assign IPv4 address

You can try to assign an IP to the peer with this setting (Wireguard parameter "Address" in peer's configuration file).

Assign IPv6 address

You can try to assign an IPv6 address to the peer with this setting (Wireguard parameter "Address" in peer's configuration file).

Assign DNS IP

You can try to assign a DNS server to the peer with this setting (Wireguard parameter "DNS" in peer's configuration file).

Connection-specific DNS suffix

You can optionally set a connection-specific DNS suffix on the client (Domainname in Wireguard parameter "DNS" of peer's configuration file).

Keepalive interval

You can try to enable the keepalive feature on the peer with this setting. At regular time intervals the peer would then send empty packets via VPN which aren't answered. This can be necessary if a NAT router is situated in front of peer that otherwise would close

an idle connection for inbound packets (Wireguard parameter "PersistentKeepalive" in peer's configuration file).

14.1.2.7 OpenVPN Client (ovpnc)

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

14.1.2.7-A OpenVPN Server.....	325
14.1.2.7-B Authentication.....	327
14.1.2.7-C Encryption.....	327

14.1.2.7-A OpenVPN Server

Description

This input serves for documentation purposes only.

Server

Specify the hostname or IP address of the OpenVPN server here.

Wrapper protocol

OpenVPN can either wrap the actual data in UDP or in TCP packets. Please select the protocol used by the server.

Port

Here you have to enter the server's port number.

Additional constraints for server certificate

An additional verification of the server certificate's data should be performed in order to protect SX-GATE from man-in-the-middle attacks.

certificate type "server"

If this option is selected, the connection will be established only if the server presents a certificate which contains an nsCertType attribute with a value of "server".



Certificates issued by SX-GATE's CA don't contain this attribute, so don't choose this option if the server uses such a certificate.

certificate usage "server"

If this option is selected, the connection will be established only if the server presents a certificate which contains a keyUsage attribute with a value of "digitalSignature" plus either "keyEncipherment" or "keyAgreement". In addition an extendedKeyUsage attribute with the value "TLS Web Server Authentication" must be present.

Certificate ID

Enter the certificate data (subject) of the server certificate. Connecting will only be possible if the server certificate contains the same data. It is also possible to enter only the common name (CN).

Compression

If the server uses the "compress" or "comp-lzo" option, it must be enabled on the client, too.

Import setup archive or configuration file

Use this wizard to import a private key, the corresponding certificate and the CA certificate. You can upload PKCS#12 files (*.p12, *.pfx), SX-GATE OpenVPN setup packages for Windows (*.exe) or OpenVPN configuration files with embedded keys (*.ovpn). When using a setup package or an OpenVPN configuration file, this connection's configuration parameters are adjusted as necessary.



The imported key and the certificates are not included in SX-GATE's backups. Please keep the file you use for import as a backup. Make sure it is protected, as it includes a private key.

Select file

Please select the setup archive or a PKCS#12 file. The setup archive contains a file with the required configuration parameters and a PKCS#12 file. This is a password protected file with an RSA key-pair. You will have to enter the password to open the PKCS#12 file.

Check certificate

Check the certificate you just uploaded before it's going to be installed.

Please read on at [Imported OpenVPN client certificate](#)

Select CA certificate file

Now the certificate chain must be added to the certificate. This may include one or more intermediate CAs. The chain ends with the root CA. All certificates must be in PEM or DER format. Please ask your CA for the required certificates.

Check CA certificate

The uploaded certificate is appended to the certificate chain.

Please read on at [Select CA certificate file](#)

Imported OpenVPN client certificate

The key-pair has been imported.

14.1.2.7-B Authentication

Certificate

SX-GATE always uses certificates to authenticate OpenVPN connections. By default it uses the certificates from menu "Modules > Network" on tabs "VPN Certificate" and "Trusted VPN CA". But you can also select individual keying material for use in this OpenVPN connection only. Pick one of the keys managed in menu "System > Certificate manager > Keyring".

14.1.2.7-C Encryption

Cipher algorithm

Please select the cipher algorithm as configured on the server. This determines how the transmitted data is protect. This setting corresponds to the OpenVPN configuration parameters "cipher" and, if applicable, "keysize".



SX-GATE additionally accepts a cipher pushed by the server. It must be an AES-GCM cipher with 128, 192 or 256 bit (configuration parameter "ncp-ciphers").

Hash algorithm

Please select the hash algorithm configured on the server for authentication of the individual data packets (HMAC). This setting corresponds to the OpenVPN configuration parameter "auth".



This parameter is not used for payload transmission when an AES-GCM cipher is used. The parameter is required to protect the control channel if "tls-auth" is enabled.

Protection of control channel

Select an option if it is required by the server.

TLS-Auth/TLS-Crypt key

Enter the tls-auth or tls-crypt key here. The key is multiple lines long. Please include the start line "-----BEGIN OpenVPN Static key V1-----" and the end line "-----END OpenVPN Static key V1-----".

14.1.2.8 OpenVPN Server (ovpns)

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

14.1.2.8-A VPN-Tunnel.....	328
14.1.2.8-B Authentication.....	330
14.1.2.8-C Encryption.....	331
14.1.2.8-D DHCP options.....	332

14.1.2.8-A VPN-Tunnel

Description

This input serves for documentation purposes only.

Wrapper protocol

OpenVPN can either wrap the actual data in UDP or in TCP packets. Although UDP is considered to perform better, TCP causes less problems, e.g. with firewalls or fragmentation. In some situations you might even be able to connect with TCP via a web proxy.



You might want to add a second OpenVPN server interface and select the other protocol in there. The client can then choose the protocol itself.

Port

Here you have to enter the server's port number.



Remember to add a custom protocol definition in the firewall setup if you don't use the default port 1194.



When running multiple OpenVPN server interfaces, they must either differ by protocol or by port.

IPv4 transfer network

This parameter determines the IPv4 pool assigned to clients. The network you configure here must not be used otherwise. We recommend using a subnet from the networks reserved for private use according to RFC 1918 (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16).



If you are running multiple OpenVPN server interfaces, they all must assign different address ranges.

The address pool size determines the maximum number of simultaneous connections according to the formula: $\text{Number of addresses} / 4 - 2 = \text{number of connections}$. With a netmask of 255.255.255.0 this yields $256 / 4 - 2 = 62$ connections.

IPv6 transfer network

This parameter determines the IPv6 pool assigned to clients. The network you configure here must not be used otherwise. We recommend spending a full /64 address block, however smaller address blocks may be used here.



If you are running multiple OpenVPN server interfaces, they all must assign different address ranges.

Access for selected certificates only

When enabled, only clients with a certificate listed below "Per-client setup" are allowed to connect.

Published local networks

An OpenVPN client usually obtains the VPN network configuration from the server. With this parameter you select the relevant local networks.



The client is not obliged to follow this suggestion. It may route other network across the VPN.

14.1.2.8-B Authentication

User authentication

When enabled, all clients have to authenticate themselves with their SX-GATE username. We recommend to use one of the methods with time-based one-time password (TOTP). One-time-passwords are enabled for each individual user in the user administration.



Only members of group "system-ras" may login.

User password

Enter the password that has been configured for the user in the SX-GATE user administration. If this option is enabled at a later point in time, the client configuration must include the line "auth-user-pass".

One-time password

Enter a one-time password (6 digits) as password. Do not enter the user password. To activate authentication in an OpenVPN client at a later point in time, you have to add the following directives to its configuration file: "auth-user-pass", "auth-nocache" and "reneg-sec 0".

User password + one-time password

This setting will prompt for both, the user password and a one-time password. If this option is selected at a later point in time, clients must have the following options configured in the config file: "auth-user-pass", "auth-nocache", "static-challenge PIN 1" and "reneg-sec 0".

Protection of control channel

Once this option is enabled and a key has been generated, the control channel is encrypted and all its messages will be authenticated. This protects against Denial-of-Service attacks, encrypts the TLS handshake including the certificates which are transmitted as part of the handshake and makes it harder to identify the network traffic as OpenVPN.



The same key has to be configured on all clients.

14.1.2.8-C Encryption

Cipher

Please select the cipher algorithm used to protect the transmissions. This setting corresponds to the OpenVPN configuration parameters "cipher" and "ncp-cipher".

Additionally accepted old cipher

Please select the cipher algorithm used to protect the transmissions. This setting corresponds to the OpenVPN configuration parameters "cipher" and, if applicable, "keysize". All ciphers use CBC mode. The selected ciphers will be appended to the OpenVPN configuration parameter "ncp-cipher".



CBC should no longer be used. Please change the client config to AES-GCM (e.g. "cipher AES-256-GCM").

Corresponding hash algorithm

Please select the hash algorithm used to authenticate the individual data packets (HMAC). This setting corresponds to the OpenVPN configuration parameter "auth".



This parameter is not required for AES-GCM.

TLS protocol

Select the TLS encryption strength.



The actual encryption parameters associated with each option are updated from time to time.

outdated

For compatibility with older devices, AES ciphers using the discouraged Cipher Block Chaining (CBC) and the obsolete hash SHA1 will be enabled when selecting this option. The minimum TLS version is 1.0.

compatibel

Select this option for wide compatibility with older client systems. This will enable the obsolete hash SHA1. The minimum TLS version is 1.2.

contemporary

Only halfway recent client systems will be supported when selecting this option. At least TLS 1.2 is required. It is a good choice for security.

maximum

Requires TLS 1.3.

14.1.2.8-D DHCP options

Assign DNS server

With this setting you will determine which name server the client will use.

Secondary DNS

If required, you can enter an additional name server here.

DNS via OpenVPN only

Despite of being connected via VPN, Windows clients might use DNS servers configured on other Windows network adapters. If you enable this option, OpenVPN on Windows will block these DNS requests, so that Windows will use only the name servers assigned by OpenVPN.



Non-Windows devices will ignore this setting.

WINS 1

Here you can specify the primary WINS server. WINS is required by Windows to resolve hostnames in multi-subnetted networks.

WINS 2

Here you can enter a secondary WINS server.

DNS suffix

Enter a suitable domain suffix, which is assigned to the client for this connection.

14.1.2.9 OpenVPN Server (ovpns) - Per-client setup

A table gives you an overview of the available objects. If multiple columns are displayed you can change the sort order by clicking the column title. If there are more than 20 entries, a navigation bar will appear below the bottom right hand corner of the table. You can switch between a grouped view or a pager. The full screen mode allows you to see all entries at the same time. Pick an entry by clicking its title in the left column. A pencil icon or a trashcan in the right column allow you to rename or delete an entry. Add new objects by clicking "New Entry" below the table on the left.

Client's certificate Common Name

There's no need to add entries here unless OpenVPN is used to interconnect whole networks. In this case OpenVPN must add routes to the networks behind the peer.

When a peer opens a new connection, the certificate it presents is used to associate the corresponding remote networks. You will need the value of the certificate's "Common Name" (CN). Enter it here.

Assigned IPv4 transfer network

In the OpenVPN server interface configuration an IP range has been reserved for the dynamic allocation of transfer networks to clients. If you need to assign a specific IPv4 transfer network, i.e. a static IPv4 address, you can define it here.



With the IP address you enter here, you actually select a four IP address transfer network. The client will get the third IP from this transfer network. To figure out the client's actual IP, please proceed as follows: If the last number of the IP address is not a multiple of four, replace it by the next smaller number which is a multiple of four. Add two and you get the client's IP.



The transfer network may not be in use otherwise. In particular it must not be part of the address range which has been reserved for dynamically assigned transfer networks.

Assigned IPv6 IP

In the OpenVPN server interface configuration an IP range has been reserved for the dynamic allocation of transfer networks to clients. If you need to assign a specific IPv6 address, you can define it here. The corresponding /64 network is configured as transfer network.



The IPv6 address may not be in use otherwise. In particular it must not be part of the address range which has been reserved for dynamically assigned transfer networks. The static IPv6 addresses of multiple clients in this OpenVPN interface may have the same network prefix.

Remote networks

Please enter the networks you want to route via the selected client.

14.1.2.10 IPSec VPN (ipsec)

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

14.1.2.10-A Common settings.....	334
14.1.2.10-B Dynamic peer setup.....	335
14.1.2.10-C Priorities.....	336

14.1.2.10-A Common settings

Description

This input serves for documentation purposes only.

Host interface

Here you can select the interface which is linked to the ipsec interface. This adds VPN functionality to the host interface. You can operate an arbitrary amount of VPN connections through a single ipsec interface.



Every host interface can only take one ipsec interface.

Internet / dynamic IP

This option can only be selected with the ipsec0 interface. Its use is mandatory if the host interface has a dynamic IP address.

14.1.2.10-B Dynamic peer setup

Common preshared key

If there are connections to peers with a dynamic IP address, all connections authenticated by preshared key must use the same preshared key. So it is not possible to clearly identify the peer. Changing the preshared key requires making changes in the configuration of all peers. Therefore we recommend that you use certificates for authentication purpose.

To offer the expected security of a VPN connection, the preshared key should be a rather complicated passphrase instead of a simple password. Use lowercase and uppercase letters, digits and special characters and avoid words that can be found in a dictionary. If these conditions are met, the recommended minimum length of the preshared key depending on the cipher and hash algorithm are:

Encryption	Hash	Characters
3DES	MD5 / SHA1	14
AES-128	SHA2-256	22
AES-256	SHA2-512	43

IKEv1 IKE proposals (phase 1)

A phase 1 proposal combines a cipher with a hash algorithm and a Diffie-Hellman group. It is used to secure the communication between two IKE servers.



If no proposals have been entered here, all proposals the SX-GATE can deal with are accepted.

The proposals configured here are used for connections to those peers using a dynamic IP addresses. This includes all client connections. For those peers it is not possible to use an individual proposal, as at the beginning of a mainmode phase 1 negotiation the peer's identity is unknown.

IKEv2 IKE proposals (phase 1)

A phase 1 proposal combines a cipher with a hash algorithm and a Diffie-Hellman group. It is used to secure the communication between two IKE servers.



If no proposals have been entered here, all combinations of AES, SHA2 SX-GATE supports and at least Diffie-Hellman group 14 will be accepted. Since AES-GCM is an AEAD algorithm that does the encryption and authentication in one step, the selected hash function defines the pseudo-random function (PRF) only.

The proposals configured here are used for connections to those peers using a dynamic IP addresses. This includes all client connections. For those peers it is not possible to use an individual proposal, as at the beginning of a mainmode phase 1 negotiation the peer's identity is unknown.

14.1.2.10-C Priorities

Use this feature to determine the priority of outgoing data packets. A proportional minimum bandwidth is assigned to each priority class. Unused bandwidth of a class will be used by classes with lower priority.

From a technical point of view the rules overwrite the ToS/DSCP field of matching IP packets. If a local application already takes care of this field, a rule would not be necessary for outbound packets. For inbound packets however the ToS/DSCP field is often modified in transit. So inbound traffic shaping usually requires rules.



Some ISPs will charge you for IP packets with certain ToS/DSCP values. Please check the ISPs terms of service.

The minimum bandwidth is assigned as follows: The bandwidth required for VoIP according to the configuration is reserved and subtracted from the total available bandwidth. Of the remaining bandwidth, 10% goes to empty TCP ACK packets, 50% to packets with high priority and 20% to packets with normal and low priority respectively.



Inbound traffic shaping treats all non-TCP packets as high priority.

Priorization of connections

Use this list to assign a higher or lower priority to specific data packets. If more than one rule matches, the priority of the topmost rule will be used.

The following inputs are available:

Protocol

Selects the IP protocol and port signature. With inbound bandwidth management, only TCP protocols will actually be processed.



Protocols are defined in menu "Definitions > Protocols".

Local IP/network

Viewed from the perspective of the selected interface, you can enter a local address here. This corresponds to the source IP of outbound packets (before SNAT) and the destination IP of inbound packets (before DNAT).



When SNAT or DNAT is involved, restricting a priority rule to specific local IPs usually requires two rules to catch both, in- and outbound packets: For inbound packets you would enter a SX-GATE IP, for outbound packets the internal IP (of the LAN client or the server addressed with DNAT).

Direction

Decide in which direction the port signature of the selected protocol has to be applied. Let's take the HTTP protocol as an example. The arrow "-->" means the HTTP port 80 is on the external side. So outbound bandwidth management will process packets to port 80, inbound bandwidth management packets from port 80. With "-->" you will get the opposite: Packets to port 80 are processed by inbound, packets from port 80 by outbound bandwidth management. The double arrow "<-->" combines both directions.

External IP/network

Viewed from the perspective of the selected interface, you can enter a remote address here. This corresponds to the destination IP of outbound packets and the source IP of inbound packets.

Priority

Select the priority for matching packets.

14.1.2.11 IPSec VPN (ipsec) - Connections

A table gives you an overview of the available objects. If multiple columns are displayed you can change the sort order by clicking the column title. If there are more than 20 entries, a navigation bar will appear below the bottom right hand corner of the table. You can switch between a grouped view or a pager. The full screen mode allows you to see all entries at the same time. Pick an entry by clicking its title in the left column. A pencil icon or a trashcan in the right column allow you to rename or delete an entry. Add new objects by clicking "New Entry" below the table on the left.

Connection with

First of all you have to decide which type VPN connection you want to add.

Server

A server can have either a static or a dynamic IP address. Typically you want to establish a VPN connection with a network which is situated behind the server. In this case the server is in fact a VPN gateway. For each server you have to add a connection of its own.

AWS

Optimized configuration for connecting with AWS.

Client

A client is expected to have a dynamic IP address. However you can use this connection type even if the client has a static IP. With a client connection it is not possible to establish a VPN tunnel to networks behind the client, only to the client itself. Only a single client connection is necessary to define the connections with all identically configured clients.

Windows IKEv2

This connection type is a special connection for Windows clients with IKEv2 and computer certificate. If you have created a Windows IKEv2 connection you can download an installation package for Windows at the end of the client certificate creation.

XAuth Client

An XAuth client connection is quite similar to a client connection, however an additional user authentication is requested using the IPSec extension "XAuth". Depending on the authenticated user it is possible to assign an individual IP to the client.

L2TP Client

This connection type also corresponds to the client connection. However the VPN tunnel will always be established between the client and SX-GATE itself. Furthermore it will transmit L2TP connections only. After decrypting the VPN packets the L2TP data stream will be forwarded to the L2TP server of SX-GATE. It authenticates the user and, if requested, assigns an individual IP to the client. To configure SX-GATE's L2TP server, please refer to the L2TP interface.

Connection name

Here you have to specify a name for the VPN connection. It is only used to identify a connection, so you can choose any appropriate name.

14.1.2.11.1 Connection with Server

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

14.1.2.11.1-A VPN-Tunnel.....	339
14.1.2.11.1-B Authentication.....	340
14.1.2.11.1-C Encryption.....	343
14.1.2.11.1-D Options.....	345
14.1.2.11.1-E Connection.....	346
14.1.2.11.1-F Commands.....	346

Peer has

Use this control to determine, if the peer has a dynamic or a static IP address. When changing to "static IP / dyn. DNS" the value "0.0.0.0" is displayed as the peer's IP. Please replace this by the correct address.

14.1.2.11.1-A VPN-Tunnel

Remote address

This setting is only available for peers with a static IP address. Specify the IP address of the peer here. It is possible to enter a DNS name as well. Use this if the peer has a dynamic IP but can always be contacted using a dynamic DNS name.



The DNS name will be resolved only once when starting the VPN server. A VPN restart will be performed right after a new Internet dial-up connection has been established, if the VPN hostinterface has a dynamic IP.



With the help of dynamic DNS it is possible to establish a VPN connection between two VPN servers, both with a dynamic IP. However due to the latency of dynamic DNS updates it can happen, that both peers use an outdated DNS record and so they can no longer contact each other. In this case it is necessary to restart the VPN server of one of the peers.

Remote networks

The VPN connection will be established with the networks you specify here. To add a connection to a single host you have to supply its IP. If no remote networks have been specified, the target of the VPN connections will be the peer itself.

Local networks

The VPN connection will be established with the networks you specify here. To add a connection to a single host you have to supply its IP. If no local networks have been specified, the target of the VPN connections will be the SX-GATE itself.

Tunnel SX-GATE <-> remote server

If you have specified local or remote networks, there will be no VPN connection between SX-GATE itself with its external IP and the peer itself with its external IP. Activate this option to add this connection.

Tunnel SX-GATE <-> remote networks

If you have specified both, local and remote networks, by default the only VPN connections negotiated will connect the local and remote nets. Activate this option to add an additional connection between the external IP of SX-GATE itself and the remote networks.

Tunnel local networks <-> remote Server

If you have specified both, local and remote networks, by default the only VPN connections negotiated will connect the local and remote nets. Activate this option to add an additional connection between the external IP of the peer itself and the local networks.

14.1.2.11.1-B Authentication

Authentication method

Please choose the authentication method used by the peer's. You can use either a X.509 certificate based authentication or use a preshared key.

The efforts for configuring authentication with certificates are higher, however this public key based method is conceptually more secure. Each peer has a private key which has to be kept secret and a corresponding public key which does not have to be protected.

In contrast authentication by preshared key can be compared to a simple password authentication. Both peers have to know this key which of course has to remain secret. However in contrast to a password the key should be longer and more complicated.

specified certificate

Using this option, the public key of the peer must be imported on SX-GATE. Drawback of this method: Whenever the peer changes its certificate (e.g. after expiration) the new public key has to be imported before the VPN connection can be reestablished. The administration effort will increase with the number of peers.



A certificate is only valid for a certain period of time (e.g. 1 year).

Certificate by CA

This is the commonly used and recommended way for certificate based authentication. The peer is accepted if it presents a certificate which has been issued by a Certificate Authority (CA) which is trusted by SX-GATE. The trusted CA is configured at "Modules > Network > Settings".



SX-GATE's VPN server certificate must have been issued by the same CA or otherwise authentication will fail.

As the certificate of the peer itself is not installed on SX-GATE it can be renewed by the peer anytime without local changes. The only requirement is that the new certificate also has to be issued by the trusted CA.



If the CA certificate expires, all certificates will become invalid. However a CA certificate is usually valid for a longer period of time (e.g. 10 years).

Preshared key

Using this setting, the peer will be authenticated by a preshared key. To enhance the security of the connection the preshared key should be a rather complicated passphrase instead of a simple password. Use lowercase and uppercase letters, digits and special characters and avoid words that can be found in a dictionary.



For all peers with a dynamic IP the same preshared key has to be used. Therefore it is configured along with the settings of the ipsec interface and not with the connection specific settings.

Local ID

With preshared key authentication the external IP addresses are used by the peers to mutually identify each other. If necessary, a different IP can be specified. Also hostnames or email addresses can be used instead of IPs.

Here you can modify the ID SX-GATE sends to the peer.

Remote ID (with PSK)

If a peer with static IP has been configured, its external IP is expected as ID. In case the peer uses a different IP (e.g. because it is situated behind a NAT router), a hostname (FQDN) or an email address (USER@FQDN) as its ID, you must supply it here.

For a peer with dynamic IP it makes sense to configure a static ID on the peer and configure this ID here. This reduces the risk that the wrong party connects with this server connection in case that multiple peers use the same preshared key.

Preshared key

If authentication by preshared key has been selected, you have to supply the key here. To offer the expected security of a VPN connection, the preshared key should be a rather complicated passphrase instead of a simple password. Use lowercase and uppercase letters, digits and special characters and avoid words that can be found in a dictionary. If these conditions are met, the recommended minimum length of the preshared key depending on cipher and hash algorithm are:

Encryption	Hash	Characters
3DES	MD5 / SHA1	14
AES-128	SHA2-256	22
AES-256	SHA2-512	43



It is not possible to configure an individual passphrase if the peer has been configured for a dynamic IP. The same passphrase applies to all preshared key connections on this interface with dynamic IPs involved. This special key is configured on the previous menu level on tab "Dynamic peer setup".

Remote ID (with CA based authentication)

For IPSec server connections authenticated by a trusted CA's certificate it is highly recommended to restrict the connection to a specific peer ID. Otherwise the owner of any certificate issued by the trusted CA would be able to impersonate the server. The remote ID is mandatory for peers with static IP. If you don't know the peer's ID, you can

find it in the logs after an attempt of the peer to establish a VPN connection with SX-GATE. Certificate data (i.e. a Distinguished name, DN) is expected as the peer's ID. It is not possible to enter an IP address or DNS name as ID here.



This setting must be adjusted whenever the peer changes its ID, e.g. because it received a new certificate and the new certificate's DN differs from the old one.

Import public key

Here you can specify the public key of the peer. If the peer's certificate was issued by the local SX-GATE CA, you can copy it from there. Otherwise you have to import the public key from a file in PEM format.



You have to import the public key of the peer's VPN server certificate and not the public key of the issuing Certification Authority (CA).

14.1.2.11.1-C Encryption

Internet Key Exchange Protocol

Here you select the type of protocol which is used for the key exchange.

IKEv1

Only IKEv1 connections are allowed in both directions.

IKEv2

Only IKEv2 connections are allowed in both directions.

Rekeying of IKE communication (Phase 1) every

Select the period of time after which the Internet key exchange servers have to negotiate a new session key for encrypting the messages passed between them.

IKEv1 IKE proposals (Phase 1)

A phase 1 proposal combines a cipher with a hash algorithm and a Diffie-Hellman group. It is used to secure the communication between two IKE servers.



If no proposals have been entered here, all combinations SX-GATE supports will be accepted. If SX-GATE initiates an IKEv1 connection, it will propose AES-256, AES-128 and 3DES together with SHA2-256, SHA2-512 and SHA1 plus Diffie-Hellman groups 14 and 5.

IKEv2 IKE proposals (Phase 1)

A phase 1 proposal combines a cipher with a hash algorithm and a Diffie-Hellman group. It is used to secure the communication between two IKE servers.



If no proposals have been entered here, all combinations of AES, SHA2 SX-GATE supports and at least Diffie-Hellman group 14 will be accepted. For outgoing connections AES_GCM256 and AES_GCM128 are preferred, followed by AES-256 and AES-128 combined with SHA2-512, SHA2-256 and the Diffie-Hellman groups 14, 15, 16, 18, 19, 20, 21 and 31. Since AES-GCM is an AEAD algorithm that does the encryption and authentication in one step, the selected hash function defines the pseudo-random function (PRF) only.

Rekeying of VPN connection (Phase 2) every

Select the period of time after which a new session key for the VPN data packets has to be negotiated.

IKEv1 ESP proposals (Phase 2)

The phase 2 proposals determine acceptable ciphers and hash-algorithms for the actual data transmission.



If no proposals have been entered here, all proposals SX-GATE supports are accepted. As an IKEv1 initiator, it will propose all combinations of AES-128 and 3DES with SHA1.

IKEv2 ESP proposals (Phase 2)

The phase 2 proposals determine acceptable ciphers and hash-algorithms for the actual data transmission. Because AES_GCM is an AEAD algorithm it do not require a separate hash-algorithm.



If no proposals have been entered here, all secure proposals SX-GATE supports are accepted.

Perfect forward secrecy

Perfect forward secrecy (PFS) for phase 2 enhances the security of a VPN connection. An intruder who manages to access the preshared key or the private key of a VPN will not be able to decrypt a recorded VPN session when PFS is active. Disabling PFS is not recommended, but may be necessary for interoperability with other IPSEC implementations.

With inbound connections, SX-GATE will accept connections without PFS only when this option is set to "disabled". An arbitrary Diffie-Hellman group is accepted when set to any other value. If however SX-GATE initiates the connection, it will use the same DH group which has been negotiated for phase 1 when set to "required". For IKEv1 you can configure a specific DH group if the "IKEv1 ESP proposals (Phase 2)" list is not empty.

SHA2-256 96bit draft version

The default ESP hash truncation for sha2_256 is 128 bits. Some IPsec implementations (Linux before 2.6.33, some Cisco routers) implement the draft version which stated 96 bits.

This option enables using the draft 96 bits version to interop with those implementations.

Another workaround is to switch from sha2_256 to sha2_384 or sha2_512.

14.1.2.11.1-D Options

Dead Peer Detection

With Dead Peer Detection (DPD) enabled, SX-GATE checks every 30 seconds whether the peer is still alive. The check is only performed when the link is idle. If there's no reply for 120 seconds, the connection is terminated. In case of a peer with static IP address, SX-GATE tries to negotiate a new connection.



The peer needs to support DPD according to RFC3706 if you want to use this feature.

IPComp compression

If enabled the data to transmit is compressed before encryption.



An inbound connection will be refused if the peer uses a different compression setting.

14.1.2.11.1-E Connection

Connection

Here you have to determine how the VPN connection will be established.

automatically

The VPN server of SX-GATE tries to contact the peer in order to establish a VPN connection. Of course it will also respond if the peer contacts SX-GATE. This option is not available if the peer has a dynamic IP address.

wait for incoming connection

Here, SX-GATE waits for the peer to establish the connection.

disabled

This setting will deactivate the corresponding VPN connection.

Routing gateway

For proper setup of the routing table you have to provide the gateway. If SX-GATE and the peer are members of the same network segment, please select the corresponding option.

14.1.2.11.1-F Commands

Action

This control allows you to manually change the connection state.



Whenever the IPsec service is restarted (e.g. when altering the setup) the default connection state as configured on tab "Connection" is restored.

(Re-)establish connection

If applicable, the connection is closed, first. SX-GATE will then start to negotiate a new connection. A log of this attempt will be shown below.

Wait for inbound connections

An established connection will be closed. SX-GATE waits for the peer to re-establish the connection.

Disable connection

Abort the connection. For the time being it will not be possible to re-connect.

14.1.2.11.2 Connection with AWS

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

14.1.2.11.2-A VPN-Tunnel.....	347
14.1.2.11.2-B Authentication.....	348
14.1.2.11.2-C Encryption.....	350
14.1.2.11.2-D Options.....	352
14.1.2.11.2-E Connection.....	352
14.1.2.11.2-F Commands.....	353

14.1.2.11.2-A VPN-Tunnel

To configure a VPN between SX-GATE and AWS, the following parameters have to be configured on the AWS side:

- Static routing
- The local IPv4 network on the AWS side must correspond to the setting "AWS network" on SX-GATE
- The remote IPv4 network on the AWS side must correspond to the setting "Local network" on SX-GATE

AWS Virtual Private Gateway (VPG) IP 1

Enter the first IP address of the Virtual Private Gateway (VPG) here.

AWS Virtual Private Gateway (VPG) IP 2

Enter the second IP address of the Virtual Private Gateway (VPG) here.

AWS network

Enter the network of the Virtual Private Cloud (VPC) you want to connect with.

Local network

Enter the local network that should be able to use the VPN.

To grant access to multiple local networks you have to aggregate them by configuring a suitable netmask (e.g. "192.168.0.0/16" would allow any 192.168 network). In the extreme case you can even configure "0.0.0.0/0" here.

As an alternative you can work with SNAT. In this case, configure an arbitrary network here. It may be a network which is really in use locally, but you can also configure any unused network here. Then you have to configure SNAT rules in the firewall configuration of the ipsec interface, mapping necessary local networks to the network you configured here.

14.1.2.11.2-B Authentication

Authentication method

Please choose the authentication method used by the peer's. You can use either a X.509 certificate based authentication or use a preshared key.

The efforts for configuring authentication with certificates are higher, however this public key based method is conceptually more secure. Each peer has a private key which has to be kept secret and a corresponding public key which does not have to be protected.

In contrast authentication by preshared key can be compared to a simple password authentication. Both peers have to know this key which of course has to remain secret. However in contrast to a password the key should be longer and more complicated.

specified certificate

Using this option, the public key of the peer must be imported on SX-GATE. Drawback of this method: Whenever the peer changes its certificate (e.g. after expiration) the new public key has to be imported before the VPN connection can be reestablished. The administration effort will increase with the number of peers.



A certificate is only valid for a certain period of time (e.g. 1 year).

Certificate by CA

This is the commonly used and recommended way for certificate based authentication. The peer is accepted if it presents a certificate which has been issued by a Certificate Authority (CA) which is trusted by SX-GATE. The trusted CA is configured at "Modules > Network > Settings".



SX-GATE's VPN server certificate must have been issued by the same CA or otherwise authentication will fail.

As the certificate of the peer itself is not installed on SX-GATE it can be renewed by the peer anytime without local changes. The only requirement is that the new certificate also has to be issued by the trusted CA.



If the CA certificate expires, all certificates will become invalid. However a CA certificate is usually valid for a longer period of time (e.g. 10 years).

Preshared key

Using this setting, the peer will be authenticated by a preshared key. To enhance the security of the connection the preshared key should be a rather complicated passphrase instead of a simple password. Use lowercase and uppercase letters, digits and special characters and avoid words that can be found in a dictionary.



For all peers with a dynamic IP the same preshared key has to be used. Therefore it is configured along with the settings of the ipsec interface and not with the connection specific settings.

Local ID

With preshared key authentication the external IP addresses are used by the peers to mutually identify each other. If necessary, a different IP can be specified. Also hostnames or email addresses can be used instead of IPs.

Here you can modify the ID SX-GATE sends to the peer.

Preshared key for Virtual Private Gateway (VPG) IP 1

Enter the preshared key for the connection to the first Virtual Private Gateway IP.

Preshared key for Virtual Private Gateway (VPG) IP 2

Enter the preshared key for the connection to the second Virtual Private Gateway IP.

ID (certificate DN) of Virtual Private Gateway (VPG) IP 1

Enter the ID used by the first Virtual Private Gateway IP.

ID (certificate DN) of Virtual Private Gateway (VPG) IP 2

Enter the ID used by the second Virtual Private Gateway IP.

Import public key

Here you can specify the public key of the peer. If the peer's certificate was issued by the local SX-GATE CA, you can copy it from there. Otherwise you have to import the public key from a file in PEM format.



You have to import the public key of the peer's VPN server certificate and not the public key of the issuing Certification Authority (CA).

14.1.2.11.2-C Encryption**Internet Key Exchange Protocol**

Here you select the type of protocol which is used for the key exchange.

IKEv1

Only IKEv1 connections are allowed in both directions.

IKEv2

Only IKEv2 connections are allowed in both directions.

Rekeying of IKE communication (Phase 1) every

Select the period of time after which the Internet key exchange servers have to negotiate a new session key for encrypting the messages passed between them.

IKEv1 IKE proposals (Phase 1)

A phase 1 proposal combines a cipher with a hash algorithm and a Diffie-Hellman group. It is used to secure the communication between two IKE servers.



If no proposals have been entered here, all combinations SX-GATE supports will be accepted. If SX-GATE initiates an IKEv1 connection, it will propose AES-256, AES-128 and 3DES together with SHA2-256, SHA2-512 and SHA1 plus Diffie-Hellman groups 14 and 5.

IKEv2 IKE proposals (Phase 1)

A phase 1 proposal combines a cipher with a hash algorithm and a Diffie-Hellman group. It is used to secure the communication between two IKE servers.



If no proposals have been entered here, all combinations of AES, SHA2 SX-GATE supports and at least Diffie-Hellman group 14 will be accepted. For outgoing connections AES_GCM256 and AES_GCM128 are preferred, followed by AES-256 and AES-128 combined with SHA2-512, SHA2-256 and the Diffie-Hellman groups 14, 15, 16, 18, 19, 20, 21 and 31. Since AES-GCM is an AEAD algorithm that does the encryption and authentication in one step, the selected hash function defines the pseudo-random function (PRF) only.

Rekeying of VPN connection (Phase 2) every

Select the period of time after which a new session key for the VPN data packets has to be negotiated.

IKEv1 ESP proposals (Phase 2)

The phase 2 proposals determine acceptable ciphers and hash-algorithms for the actual data transmission.



If no proposals have been entered here, all proposals SX-GATE supports are accepted. As an IKEv1 initiator, it will propose all combinations of AES-128 and 3DES with SHA1.

IKEv2 ESP proposals (Phase 2)

The phase 2 proposals determine acceptable ciphers and hash-algorithms for the actual data transmission. Because AES_GCM is an AEAD algorithm it does not require a separate hash-algorithm.



If no proposals have been entered here, all secure proposals SX-GATE supports are accepted.

Perfect forward secrecy

Perfect forward secrecy (PFS) for phase 2 enhances the security of a VPN connection. An intruder who manages to access the preshared key or the private key of a VPN will not be able to decrypt a recorded VPN session when PFS is active. Disabling

PFS is not recommended, but may be necessary for interoperability with other IPSEC implementations.

With inbound connections, SX-GATE will accept connections without PFS only when this option is set to "disabled". An arbitrary Diffie-Hellman group is accepted when set to any other value. If however SX-GATE initiates the connection, it will use the same DH group which has been negotiated for phase 1 when set to "required". For IKEv1 you can configure a specific DH group if the "IKEv1 ESP proposals (Phase 2)" list is not empty.

14.1.2.11.2-D Options

Dead Peer Detection

With Dead Peer Detection (DPD) enabled, SX-GATE checks at regular intervals whether the peer is still alive. The check is only performed when the link is idle. If there's no reply, the connection is terminated and SX-GATE tries to connect with the other Virtual Private Gateway IP.

DPD intervall

Time intervall for sending DPD keepalive packets.

DPD timeout

If the peer is not responding for the period configured here, SX-GATE will switch to the other VGP IP. Configure a value which is at least three times larger as "DPD intervall".

IPComp compression

If enabled the data to transmit is compressed before encryption.



An inbound connection will be refused if the peer uses a different compression setting.

14.1.2.11.2-E Connection

Connection

Here you have to determine how the VPN connection will be established.

automatically

The VPN server of SX-GATE tries to establish a VPN connection with AWS.

wait for incoming connection

Here, SX-GATE waits for AWS to establish the connection.

disabled

This setting will deactivate the corresponding VPN connection.

Routing gateway

For proper setup of the routing table you have to provide the gateway. If SX-GATE and the peer are members of the same network segment, please select the corresponding option.

14.1.2.11.2-F Commands

Action

This control allows you to manually change the connection state.



Whenever the IPsec service is restarted (e.g. when altering the setup) the default connection state as configured on tab "Connection" is restored.

(Re-)establish connection

If applicable, the connection is closed, first. SX-GATE will then start to negotiate a new connection. A log of this attempt will be shown below.

Wait for inbound connections

An established connection will be closed. SX-GATE waits for the peer to re-establish the connection.

Disable connection

Abort the connection. For the time being it will not be possible to re-connect.

14.1.2.11.3 Connection with Client

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

14.1.2.11.3-A VPN-Tunnel.....	354
14.1.2.11.3-B Authentication.....	355
14.1.2.11.3-C Encryption.....	357
14.1.2.11.3-D Options.....	358
14.1.2.11.3-E Connection.....	358
14.1.2.11.3-F Commands.....	358

14.1.2.11.3-A VPN-Tunnel

Local networks

The VPN connection will be established to the networks you specify here. To add a connection to a single host you have to supply its IP. If no local networks have been specified, the target of the VPN connections will be SX-GATE itself.

Tunnel SX-GATE <-> Client

If you have specified local networks, there will be no VPN connection between SX-GATE itself with its external IP and the client. Activate this option to add this connection.

Virtual IP

The IKEv1 IPsec extension "mode config" or IKEv2 addresspool lets you assign an IP address to the client to be used for connections via IPsec. Without virtual ip the client will use its own (external) IP address when connecting via IPsec.



An address pool is strictly required for IKEv2 clients behind a NAT router.

Set an address range here from which the client obtains its IP address. The number of IP addresses determines the maximum number of simultaneously connected clients.

Assign DNS server

With this setting you will determine which name server the client will use.

14.1.2.11.3-B Authentication

Authentication method

Please choose the authentication method used by the peer's. You can use either a X.509 certificate based authentication or use a preshared key.

The efforts for configuring authentication with certificates are higher, however this public key based method is conceptually more secure. Each peer has a private key which has to be kept secret and a corresponding public key which does not have to be protected.

In contrast authentication by preshared key can be compared to a simple password authentication. Both peers have to know this key which of course has to remain secret. This method is however a bad choice for client connections, as every connection which involves dynamic IPs has to use the same preshared key.

specified X.509 certificates only

Using this option, the public key of the client must be imported on SX-GATE. Drawback of this method: Whenever the peer changes its certificate (e.g. after expiration) the new public key has to be imported before the VPN connection can be reestablished. The administration effort will increase with the number of peers.



A certificate is only valid for a certain period of time (e.g. 1 year).

If you still want to use this option, please create a similar connection for each client and import the corresponding certificate.

any certificate signed by trusted CA

This is the commonly used and recommended way for certificate based authentication. The client is accepted if it presents a certificate which has been issued by a Certificate Authority (CA) which is trusted by SX-GATE. The trusted CA is configured at "Modules > Network > Settings".



SX-GATE's VPN server certificate must have been issued by the same CA or otherwise authentication will fail.

As the client's certificate is not installed on SX-GATE it can be renewed anytime without local changes. The only requirement is that the new certificate also has to be issued by the trusted CA.



If the CA certificate expires, all certificates will become invalid. However a CA certificate is usually valid for a longer period of time (e.g. 10 years).

Preshared key

Using this setting, the peer will be authenticated by a preshared key.



All connections with dynamic IPs involved must use the same key. Therefore it is configured along with the settings of the ipsec interface and not with the connection specific settings.

Remote ID (with PSK)

With preshared key authentication the peers identify each other using an IP address, a hostname (FQDN) or an email address (USER@FQDN). To restrict this connection to a client with a certain ID you can enter its ID here. If you don't know the peer's ID, you can find it in the logs after an attempt of the peer to establish a VPN connection with SX-GATE.



A client with dynamic IP which identifies itself by its IP must provide an option to set a static ID. Otherwise it is not identifiable by ID.

Remote ID (with CA based authentication)

Limit access to this connection to a single peer by entering the peer's ID. If you don't know the peer's ID, you can find it in the logs after an attempt of the peer to establish a VPN connection with SX-GATE. Certificate data (i.e. a Distinguished name, DN) is expected as the peer's ID. It is not possible to enter an IP address or DNS name as ID here.



This setting must be adjusted whenever the peer changes its ID, e.g. because it received a new certificate and the new certificate's DN differs from the old one.

Import public key

Here you can specify the public key of the client. If the client's certificate was issued by the local SX-GATE CA, you can copy it from there. Otherwise you have to import it from a file in PEM format.



You have to import the public key of the client itself and not the public key of the issuing Certification Authority (CA).

14.1.2.11.3-C Encryption

Internet Key Exchange Protocol

Here you select the type of protocol which is used for the key exchange.

IKEv1

Only IKEv1 connections are allowed.

IKEv2

Only IKEv2 connections are allowed.

IKEv1 ESP proposals (Phase 2)

The phase 2 proposals determine acceptable ciphers and hash-algorithms for the actual data transmission.



If no proposals have been entered here, all proposals SX-GATE supports are accepted.

IKEv2 ESP proposals (Phase 2)

The phase 2 proposals determine acceptable ciphers and hash-algorithms for the actual data transmission. Because AES_GCM is an AEAD algorithm it does not require a separate hash-algorithm.



If no proposals have been entered here, all secure proposals SX-GATE supports are accepted.

Perfect forward secrecy

Perfect forward secrecy (PFS) for phase 2 enhances the security of a VPN connection. An intruder who manages to access the preshared key or the private key of a VPN will not be able to decrypt a recorded VPN session when PFS is active. Setting PFS to "disabled" is not recommended, but may be necessary for interoperability with other IPSEC implementations.

14.1.2.11.3-D Options

Dead Peer Detection

With Dead Peer Detection (DPD) enabled, SX-GATE checks every 30 seconds whether the peer is still alive. The check is only performed when the link is idle. If there's no reply for 120 seconds, the connection is terminated. In case of a peer with static IP address, SX-GATE tries to negotiate a new connection.



The peer needs to support DPD according to RFC3706 if you want to use this feature.

14.1.2.11.3-E Connection

Connect

Here you can enable or disable the VPN connection.

wait for incoming connection

Here, SX-GATE waits for the peer to establish the connection.

disabled

This setting will deactivate the corresponding VPN connection.

Routing gateway

For proper setup of the routing table you have to provide the gateway. If SX-GATE and the peer are members of the same network segment, please select the corresponding option.

14.1.2.11.3-F Commands

Action

This control allows you to manually change the connection state.



Whenever the IPsec service is restarted (e.g. when altering the setup) the default connection state as configured on tab "Connection" is restored.

Wait for inbound connections

All established connections will be closed. SX-GATE waits for the peers to re-establish the connection.

Disable connections

Abort all connections. For the time being it will not be possible to re-connect.

14.1.2.11.4 Connection with Windows IKEv2

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

14.1.2.11.4-A VPN-Tunnel.....	359
14.1.2.11.4-B Options.....	361
14.1.2.11.4-C Connection.....	361
14.1.2.11.4-D Commands.....	362

14.1.2.11.4-A VPN-Tunnel

This connection uses the IKEv2 IKE proposals (phase 1) set under "Dynamic peer setup". You should therefore ensure that either no proposals are specified or enter the recommended proposals "AES-256-SHA2_256-MODP2048 (DH14)" for this connection.

In phase 2, all common secure IKEv2 ESP proposals are accepted.

Windows uses the insecure Diffie-Hellman Group 2 (MODP1024) by default. Therefore, either use our installation package for connection with "Connection with Windows IKEv2" or make sure that the correct proposals are set in Windows.

You can do this e.g. with the following powershell command:

```
Set-VpnConnectionIPsecConfiguration -ConnectionName "Verbindungsname" -
CipherTransformConstants AES256 -AuthenticationTransformConstants SHA256128
-EncryptionMethod AES256 -IntegrityCheckMethod SHA256 -PfsGroup PFS2048 -
DHGroup Group14
```

Authentication method

Please choose the authentication method used by the peer's.

any certificate signed by trusted CA

This is the commonly used and recommended way for certificate based authentication. The client is accepted if it presents a certificate which has been

issued by a Certificate Authority (CA) which is trusted by SX-GATE. The trusted CA is configured at "Modules > Network > Settings".



SX-GATE's VPN server certificate must have been issued by the same CA or otherwise authentication will fail.

As the client's certificate is not installed on SX-GATE it can be renewed anytime without local changes. The only requirement is that the new certificate also has to be issued by the trusted CA.



If the CA certificate expires, all certificates will become invalid. However a CA certificate is usually valid for a longer period of time (e.g. 10 years).

specified X.509 certificates only

Using this option, the public key of the client must be imported on SX-GATE. Drawback of this method: Whenever the peer changes its certificate (e.g. after expiration) the new public key has to be imported before the VPN connection can be reestablished. The administration effort will increase with the number of peers.



A certificate is only valid for a certain period of time (e.g. 1 year).

If you still want to use this option, please create a similar connection for each client and import the corresponding certificate.

Global addresspool

If the global addresspool is disabled, only clients specified in "Addresspools of defined peers" are allowed. If you want to allow clients with any ID, you must define an appropriate address range. The size of the address range determines the maximum number of simultaneous connections.

Pool of assigned IP addresses

Set an address range here from which the client obtains its IP address.

The number of IP addresses determines the maximum number of simultaneously connected clients.

Addresspools of defined peers

In this table, you can use the Relative Distinguished Names (RDN) of a certificate to assign specific IP addresses to Windows clients. This allows you to e.g. assign different

address ranges to different groups, which in turn can be handled separately in the firewall.

The specified address ranges must not overlap. However, it is possible to assign the same address range to several clients. The size of the addresspool limits the maximum number of clients, which can connect at the same time.

Import public key

Here you can specify the public key of the client. If the client's certificate was issued by the local SX-GATE CA, you can copy it from there. Otherwise you have to import it from a file in PEM format.



You have to import the public key of the client itself and not the public key of the issuing Certification Authority (CA).

14.1.2.11.4-B Options

Dead Peer Detection

With Dead Peer Detection (DPD) enabled, SX-GATE checks every 30 seconds whether the peer is still alive. The check is only performed when the link is idle. If there's no reply for 120 seconds, the connection is terminated. In case of a peer with static IP address, SX-GATE tries to negotiate a new connection.



The peer needs to support DPD according to RFC3706 if you want to use this feature.

Assign DNS server

With this setting you will determine which name server the client will use.

14.1.2.11.4-C Connection

Connect

Here you can enable or disable the VPN connection.

wait for incoming connection

Here, SX-GATE waits for the peer to establish the connection.

disabled

This setting will deactivate the corresponding VPN connection.

Routing gateway

For proper setup of the routing table you have to provide the gateway. If SX-GATE and the peer are members of the same network segment, please select the corresponding option.

14.1.2.11.4-D Commands

Action

This control allows you to manually change the connection state.



Whenever the IPSec service is restarted (e.g. when altering the setup) the default connection state as configured on tab "Connection" is restored.

Wait for inbound connections

All established connections will be closed. SX-GATE waits for the peers to re-establish the connection.

Disable connections

Abort all connections. For the time being it will not be possible to re-connect.

14.1.2.11.5 Connection with XAuth Client

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

14.1.2.11.5-A VPN-Tunnel.....	363
14.1.2.11.5-B Authentication.....	363
14.1.2.11.5-C Encryption.....	365
14.1.2.11.5-D Options.....	366
14.1.2.11.5-E Connection.....	366
14.1.2.11.5-F Commands.....	367

14.1.2.11.5-A VPN-Tunnel

Virtual IP (Mode Config)

The IPsec extension "mode config" lets you assign an IP address to the client to be used for connections via IPsec. Without mode config the client will use its own (external) IP address when connecting via IPsec.

To enable mode config, please supply an IP address range to be assigned to the clients. The number of IP addresses determines the maximum number of simultaneously connected clients. In addition it is possible to assign user specific XAuth addresses in the user administration. A user with an individual IP does not claim an address from the pool configured here, thus increasing the number of possible simultaneous connections. Select the option "individual user IPs only" to assign user specific IPs only.

Assign DNS server

With this setting you will determine which name server the client will use.

14.1.2.11.5-B Authentication

Authentication method

Please choose the authentication method used by the peer's. You can use either a X.509 certificate based authentication or use a preshared key.

The efforts for configuring authentication with certificates are higher, however this public key based method is conceptually more secure. Each peer has a private key which has to be kept secret and a corresponding public key which does not have to be protected.

In contrast authentication by preshared key can be compared to a simple password authentication. Both peers have to know this key which of course has to remain secret. This method is however a bad choice for client connections, as every connection which involves dynamic IPs has to use the same preshared key.

specified X.509 certificates only

Using this option, the public key of the client must be imported on SX-GATE. Drawback of this method: Whenever the peer changes its certificate (e.g. after expiration) the new public key has to be imported before the VPN connection can be reestablished. The administration effort will increase with the number of peers.



A certificate is only valid for a certain period of time (e.g. 1 year).

If you still want to use this option, please create a similar connection for each client and import the corresponding certificate.

any certificate signed by trusted CA

This is the commonly used and recommended way for certificate based authentication. The client is accepted if it presents a certificate which has been issued by a Certificate Authority (CA) which is trusted by SX-GATE. The trusted CA is configured at "Modules > Network > Settings".



SX-GATE's VPN server certificate must have been issued by the same CA or otherwise authentication will fail.

As the client's certificate is not installed on SX-GATE it can be renewed anytime without local changes. The only requirement is that the new certificate also has to be issued by the trusted CA.



If the CA certificate expires, all certificates will become invalid. However a CA certificate is usually valid for a longer period of time (e.g. 10 years).

Preshared key

Using this setting, the peer will be authenticated by a preshared key.



All connections with dynamic IPs involved must use the same key. Therefore it is configured along with the settings of the ipsec interface and not with the connection specific settings.

Remote ID (with PSK)

With preshared key authentication the peers identify each other using an IP address, a hostname (FQDN) or an email address (USER@FQDN). To restrict this connection to a client with a certain ID you can enter its ID here. If you don't know the peer's ID, you can find it in the logs after an attempt of the peer to establish a VPN connection with SX-GATE.



A client with dynamic IP which identifies itself by its IP must provide an option to set a static ID. Otherwise it is not identifiable by ID.

Remote ID (with CA based authentication)

Limit access to this connection to a single peer by entering the peer's ID. If you don't know the peer's ID, you can find it in the logs after an attempt of the peer to establish a VPN connection with SX-GATE. Certificate data (i.e. a Distinguished name, DN) is expected as the peer's ID. It is not possible to enter an IP address or DNS name as ID here.



This setting must be adjusted whenever the peer changes its ID, e.g. because it received a new certificate and the new certificate's DN differs from the old one.

Import public key

Here you can specify the public key of the client. If the client's certificate was issued by the local SX-GATE CA, you can copy it from there. Otherwise you have to import it from a file in PEM format.



You have to import the public key of the client itself and not the public key of the issuing Certification Authority (CA).

14.1.2.11.5-C Encryption

The IKE proposals configured for peers with dynamic IP will always apply.

IKEv1 ESP proposals (Phase 2)

The phase 2 proposals determine acceptable ciphers and hash-algorithms for the actual data transmission.



If no proposals have been entered here, all proposals SX-GATE supports are accepted.

Perfect forward secrecy

Perfect forward secrecy (PFS) for phase 2 enhances the security of a VPN connection. An intruder who manages to access the preshared key or the private key of a VPN will not be able to decrypt a recorded VPN session when PFS is active. Setting PFS to "disabled" is not recommended, but may be necessary for interoperability with other IPSEC implementations.

SHA2-256 96bit draft version

The default ESP hash truncation for sha2_256 is 128 bits. Some IPsec implementations (Linux before 2.6.33, some Cisco routers) implement the draft version which stated 96 bits.

This option enables using the draft 96 bits version to interop with those implementations.

Another workaround is to switch from sha2_256 to sha2_384 or sha2_512.

14.1.2.11.5-D Options**Dead Peer Detection**

With Dead Peer Detection (DPD) enabled, SX-GATE checks every 30 seconds whether the peer is still alive. The check is only performed when the link is idle. If there's no reply for 120 seconds, the connection is terminated. In case of a peer with static IP address, SX-GATE tries to negotiate a new connection.



The peer needs to support DPD according to RFC3706 if you want to use this feature.

14.1.2.11.5-E Connection**Connect**

Here you can enable or disable the VPN connection.

wait for incoming connection

Here, SX-GATE waits for the peer to establish the connection.

disabled

This setting will deactivate the corresponding VPN connection.

Routing gateway

For proper setup of the routing table you have to provide the gateway. If SX-GATE and the peer are members of the same network segment, please select the corresponding option.

14.1.2.11.5-F Commands

Action

This control allows you to manually change the connection state.



Whenever the IPSec service is restarted (e.g. when altering the setup) the default connection state as configured on tab "Connection" is restored.

Wait for inbound connections

All established connections will be closed. SX-GATE waits for the peers to re-establish the connection.

Disable connections

Abort all connections. For the time being it will not be possible to re-connect.

14.1.2.11.6 Connection with L2TP Client

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

14.1.2.11.6-A Authentication.....	367
14.1.2.11.6-B Encryption.....	370
14.1.2.11.6-C Options.....	370
14.1.2.11.6-D Connection.....	370
14.1.2.11.6-E Commands.....	371

14.1.2.11.6-A Authentication

Authentication method

Please choose the authentication method used by the peer's. You can use either a X.509 certificate based authentication or use a preshared key.

The efforts for configuring authentication with certificates are higher, however this public key based method is conceptually more secure. Each peer has a private key which has to be kept secret and a corresponding public key which does not have to be protected.

In contrast authentication by preshared key can be compared to a simple password authentication. Both peers have to know this key which of course has to remain secret. This method is however a bad choice for client connections, as every connection which involves dynamic IPs has to use the same preshared key.

specified X.509 certificates only

Using this option, the public key of the client must be imported on SX-GATE. Drawback of this method: Whenever the peer changes its certificate (e.g. after expiration) the new public key has to be imported before the VPN connection can be reestablished. The administration effort will increase with the number of peers.



A certificate is only valid for a certain period of time (e.g. 1 year).

If you still want to use this option, please create a similar connection for each client and import the corresponding certificate.

any certificate signed by trusted CA

This is the commonly used and recommended way for certificate based authentication. The client is accepted if it presents a certificate which has been issued by a Certificate Authority (CA) which is trusted by SX-GATE. The trusted CA is configured at "Modules > Network > Settings".



SX-GATE's VPN server certificate must have been issued by the same CA or otherwise authentication will fail.

As the client's certificate is not installed on SX-GATE it can be renewed anytime without local changes. The only requirement is that the new certificate also has to be issued by the trusted CA.



If the CA certificate expires, all certificates will become invalid. However a CA certificate is usually valid for a longer period of time (e.g. 10 years).

Preshared key

Using this setting, the peer will be authenticated by a preshared key.



All connections with dynamic IPs involved must use the same key. Therefore it is configured along with the settings of the ipsec interface and not with the connection specific settings.

Remote ID (with PSK)

With preshared key authentication the peers identify each other using an IP address, a hostname (FQDN) or an email address (USER@FQDN). To restrict this connection to a client with a certain ID you can enter its ID here. If you don't know the peer's ID, you can find it in the logs after an attempt of the peer to establish a VPN connection with SX-GATE.



A client with dynamic IP which identifies itself by its IP must provide an option to set a static ID. Otherwise it is not identifiable by ID.

Remote ID (with CA based authentication)

Limit access to this connection to a single peer by entering the peer's ID. If you don't know the peer's ID, you can find it in the logs after an attempt of the peer to establish a VPN connection with SX-GATE. Certificate data (i.e. a Distinguished name, DN) is expected as the peer's ID. It is not possible to enter an IP address or DNS name as ID here.



This setting must be adjusted whenever the peer changes its ID, e.g. because it received a new certificate and the new certificate's DN differs from the old one.

Import public key

Here you can specify the public key of the client. If the client's certificate was issued by the local SX-GATE CA, you can copy it from there. Otherwise you have to import it from a file in PEM format.



You have to import the public key of the client itself and not the public key of the issuing Certification Authority (CA).

14.1.2.11.6-B Encryption

The IKE proposals configured for peers with dynamic IP will always apply.

IKEv1 ESP proposals (Phase 2)

The phase 2 proposals determine acceptable ciphers and hash-algorithms for the actual data transmission.



If no proposals have been entered here, all proposals SX-GATE supports are accepted.

Perfect forward secrecy

Perfect forward secrecy (PFS) for phase 2 enhances the security of a VPN connection. An intruder who manages to access the preshared key or the private key of a VPN will not be able to decrypt a recorded VPN session when PFS is active. Setting PFS to "disabled" is not recommended, but may be necessary for interoperability with other IPSEC implementations.

14.1.2.11.6-C Options

Dead Peer Detection

With Dead Peer Detection (DPD) enabled, SX-GATE checks every 30 seconds whether the peer is still alive. The check is only performed when the link is idle. If there's no reply for 120 seconds, the connection is terminated. In case of a peer with static IP address, SX-GATE tries to negotiate a new connection.



The peer needs to support DPD according to RFC3706 if you want to use this feature.

14.1.2.11.6-D Connection

Connect

Here you can enable or disable the VPN connection.

wait for incoming connection

Here, SX-GATE waits for the peer to establish the connection.

disabled

This setting will deactivate the corresponding VPN connection.

Routing gateway

For proper setup of the routing table you have to provide the gateway. If SX-GATE and the peer are members of the same network segment, please select the corresponding option.

14.1.2.11.6-E Commands

Action

This control allows you to manually change the connection state.



Whenever the IPsec service is restarted (e.g. when altering the setup) the default connection state as configured on tab "Connection" is restored.

Wait for inbound connections

All established connections will be closed. SX-GATE waits for the peers to re-establish the connection.

Disable connections

Abort all connections. For the time being it will not be possible to re-connect.

14.2 Firewall

14.2.1 Settings

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

14.2.1-A General.....	372
14.2.1-B ALGs.....	373
14.2.1-C Intrusion Detection.....	374
14.2.1-D Intrusion Detection Update.....	375

14.2.1-A General

Application control

This switch enables application control in the firewall. The firewall will then analyse the transmitted payloads and tries to detect the actual application.

When enabled, detected protocols and, if available, hostnames will be displayed in "Monitoring > Firewall" on tab "Connections".

You can create your own protocols in menu "Definitions > Protocols" and enable application control in there. Firewall rules (except for SNAT) and bandwidth management rules using such a protocol won't match until the application has been detected.



If the firewall, while processing the rules, hits a protocol with application control enabled, communication has to be granted at first to allow further analyses. Rule processing won't continue until the configured application has either been detected or can be rules out. The firewall "leaks"!

IPv4 routing

This tab will allow you to activate IPv4 routing. If IPv4 routing is not active, only connections to or from SX-GATE are possible. Connections through SX-GATE are completely suppressed, regardless of the configured firewall rules.

Asymmetric routing in LAN

This switch disables Stateful Inspection for packets routed within the same interface. Only Ethernet and VLAN interfaces with "Zone/Classification (Trustlevel) LAN (high)" in the firewall configuration will be considered.

IP whitelist

IP addresses on this list are excluded from

- blocking of suspicious IPs by dynamic firewall
- blocking after repeated authentication failure
- portscan detection
- the following blocklist

IP blocklist

Connections from and to IP addresses on this list are dropped.

14.2.1-B ALGs

Application-Level-Gateways

Some protocols use multiple different connections. Often a control channel is used to dynamically negotiate a set of ports used to transmit the actual data. For some of these protocols SX-GATE provides a firewall module that monitors the control channel and temporarily allows the required connections automatically. Use these modules whenever possible, as otherwise you might have to permanently open larger blocks of ports - sometimes even for inbound connections from the Internet.

On the other hand these firewall modules might be abused by an attacker, opening unwanted connections with crafted data packets. So you should enable the modules only for connections that really require the module. For instance to enable Voice-over-IP, you should enable the SIP module only for connections from your PBX to the SIP gateway of your VoIP provider.

Changes to this list will apply to new connections only. For TCP connections it is usually enough to restart the application on the client.



UDP connections however might be remembered by the firewall for hours. So we recommend a reboot after applying changes.

14.2.1-C Intrusion Detection

The Intrusion Detection System (IDS) of SX-GATE analyses IP packets to detect potential security violations. The IP header information as well as the actual payload is examined. The analysis is based on a signature database.

The IDS is always enabled on SX-GATE's Internet interface. There it uses a subset of the available signatures, focusing on the detection of infected local systems. It tries to prevent that these systems transmit data into the Internet or try to infect other systems with malware. To achieve this, detected malicious packets are discarded.



In addition to the default gateway interface all interfaces with routes to destination network "*" are counted as Internet interface.

Additionally the IDS may be connected to the monitor port of a switch using a dedicated network interface. In this configuration the complete signature base is available. However the IDS operates in a passive mode only, i.e. malicious data packets will be logged but not dropped.

Disabled rules

Here you can disable individual rules in case of repeated false alerts. Please enter the rule number which is visible in the logs. The log format is [1:RULENUMBER:number]. If for example the log shows [1:2010123:0], please add 2010123.



The rules will be disabled in both, the active IDS (Internet interface) and the passive IDS (monitor port).

Connection Whitelist

If you want to exclude individual connections or entire protocols from the intrusion detection, you can configure the necessary rules here.



Please note that connections initiated from the SX-GATE (proxy, mail server, etc.) through an additionally configured Internet interface cannot be directly identified using the source IP. Normally the source IP of the default interface can be used for these connections.

Local networks

Some IDS rules distinguish between internal and external IP addresses. Here you configure which addresses are considered to be internal.



Static IPs of Internet interfaces are automatically appended to the list.

Additional IPS rules against Web server attacks

Enables specific rules to detect attacks against web and FTP servers.

Additional IPS rules against mail server attacks

Enables specific rules to detect attacks against SMTP, IMAP4 and POP3 servers.

14.2.1-D Intrusion Detection Update

Systems with a software maintenance contract receive signature updates multiple times a week.

Update server

The update server address can be changed in menu "System > Update". Also a proxy can be configured there if necessary.

Update IDS signatures automatically

When enabled, SX-GATE will check for new signatures daily between 18:00 and 21:00.

14.2.2 Policies

SX-GATE's firewall is configured per interface. Additionally each interface has to be classified into one of four zones, depending on the trustworthiness of the attached networks. This classification determines the firewall's base setup. You may then define firewall rules to elaborate the firewall configuration.



Imprudent changes of settings in this menu can affect the system security of SX-GATE and of all networks protected by SX-GATE.

Firewall rules always have to be specified only for the initial packet. Stateful inspection will associate related packets with the connection, so e.g. reply packets will be accepted automatically.

It is crucial that firewall rules are configured in the right place. In the following explanation, the term "inbound interface" refers to the interface through which the initial packet of a connection is received by SX-GATE. The "outbound interface" is the interface through which a connection's initial packet leaves SX-GATE towards its destination. There are four kinds of connections:

DNAT (in)

DNAT, also known as portforwarding, changes the destination of a connection. Rules have to be configured in the inbound interface on tab "DNAT > *". DNAT affects both, inbound and forwarded connections. A rule can make an inbound connection out of a forwarding connection, vice versa. No additional inbound or forwarding rule is required to make a DNAT rule work.

Inbound connections (in)

All connections destined for SX-GATE belong to this group. Select the inbound interface in the tree menu of SX-GATE's web administration and configure rules on tab " ... > SX-GATE".

Forwarded connections / Routing (fwd)

Connections passing through SX-GATE belong to this group. SX-GATE is neither the source nor the destination of the connection. The connection is routed by SX-GATE. Forwarding rules can be defined on tab "* > SX-GATE > ...".



Firewall rules for forwarded connections go into the outbound interface. In the web administration, please select the interface through which the connection's initial packet leaves SX-GATE.

Outgoing connections(out)

Here we are talking about connections initiated by SX-GATE. Select the outbound interface in SX-GATE's web administration and edit rules on tab "SX-GATE > ...". Both, forwarded and outbound connections additionally pass the SNAT rules configured on tab "* > SNAT". SNAT replaces the original sender IP. By default, SNAT replaces the sender IP of IPv4 connections forwarded from zones LAN and RAS to zone Internet, with SX-GATE's primary IP of the outbound interface (Auto SNAT), as we assume that the internal networks use IPv4 addresses which are not allowed in the Internet.

A table gives you an overview of the available objects. If multiple columns are displayed you can change the sort order by clicking the column title. If there are more than 20 entries, a navigation bar will appear below the bottom right hand corner of the table. You can switch between a grouped view or a pager. The full screen mode allows you to see all entries at the same time. Pick an entry by clicking its title in the left column. A pencil icon or a trashcan in the right column allow you to rename or delete an entry.

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

14.2.2-A General.....	380
14.2.2-B DNAT > *	380
14.2.2-C Transp. proxy.....	383
14.2.2-D ... > SX-GATE.....	386
14.2.2-E * > SX-GATE >	388
14.2.2-F * > SX-GATE >	391
14.2.2-G SX-GATE >	393
14.2.2-H * > SNAT.....	395
14.2.2-I Options.....	397

Zone/Classification (Trustlevel)

Use this control to define the base configuration of the firewall for the selected interface. The following table shows the default behaviour of the firewall. The source refers to the classification of the inbound interface whereas the destination refers to the classification of the outbound interface. The row and the column labeled "SX-GATE" shows the default policy for connections from and to SX-GATE respectively.

Source	Destination				
	Internet (none)	DMZ (low)	RAS (medium)	LAN (high)	SX-GATE
Internet (none)					
DMZ (low)					
RAS (medium)	Auto SNAT				
LAN (high)	Auto SNAT				
SX-GATE					

	Access denied. Add rules to allow specific connections
	Access denied. Add rules or change default policy to grant access
	Access granted. Restrict by changing the default policy

The names of the available classes reflect the typical use of this class. However this is just to aid orientation. In individual cases it can make sense to select a different value. However you should be aware of the effect of every modification. This is especially true if the actual purpose of the interface and the typical use differ clearly, e.g. when selecting "LAN (high)" for the internet interface.



When changing the classification of the interface through which SX-GATE is configured, make sure that HTTPS access to SX-GATE remains possible. Otherwise you will no longer be able to access the administration interface with your browser. The console will then be the only way to modify SX-GATE's configuration.

Internet (none)

Typically this option is used for interfaces connected to the Internet. By default, access from the Internet to SX-GATE is denied. The same applies to direct connections from systems in the LAN to the Internet. To allow specific connections from the Internet to SX-GATE, you have to define them on the tab labeled " ... > SX-GATE". Direct connections from LAN to the Internet can be allowed on tab "* > SX-GATE > ... ", however if possible, use the SX-GATE components proxy, mail server, mail client and DNS forwarder instead. These enhance the security of the browser, email and DNS communication of systems in the LAN.

For accepted IPv4 connections from LAN or RAS zones, network address translation (NAT) is applied automatically unless overridden by the rules on tab "* > SNAT". NAT replaces the source address of outbound IP packets with the external IP address of SX-GATE. This will not apply to DS-Lite Internet links and connections forwarded within a bridge.

DMZ (low)

If internet servers are kept in a separate physical network, this network is called a demilitarized zone (DMZ). This is the typical use case of this option. Particularly the LAN networks have unlimited access to servers in the DMZ. In contrast, internet access to the DMZ has to be allowed on tab "* > SX-GATE > ... ".



To restrict DMZ access for the LAN networks, change the corresponding setting on tab "General".

RAS (medium)

By and large, the default policy activated by this option is comparable to "LAN (high)". However it is possible to limit connections from the respective networks to all destinations. With "LAN (high)" only connections to the Internet are restricted.

LAN (high)

Choose this option to activate the least restrictive policy. By default only direct internet access is limited for the respective networks. Access to all other types of interfaces is granted. To impose limitations here, change to the option "RAS (medium)".

Zone/Classification (Trustlevel) of bridge as destination interface

Usually the firewall of a bridge is configured by bridge port in menu "Bridge". As an exception, connections routed into the bridge cannot be configured by port, as at the moment the firewall processes the connection, the destination bridge port has not been determined yet. Also connections initiated by SX-GATE which are routed into the bridge and SNAT rules are not configured by port but for the bridge as a whole.

By selecting one of the firewall zones you determine the default behaviour of the firewall for the connection type mentioned above. Your selection does not affect bridged connections or connections which originate in the bridge. The selected classification may be different from the classification selected for the bridge ports. The following table shows the default behaviour of the firewall. The source refers to the classification of the inbound interface whereas the destination refers to the classification of the bridge. The row labeled "SX-GATE" shows the default policy for connections initiated by SX-GATE.

Source	Destination			
	Internet (none)	DMZ (low)	RAS (medium)	LAN (high)
Internet (none)				
DMZ (low)				
RAS (medium)	Auto SNAT			
LAN (high)	Auto SNAT			
SX-GATE				

	Access denied. Add rules to allow specific connections
	Access denied. Add rules or change default policy to grant access
	Access granted. Restrict by changing the default policy

14.2.2-A General

Description "..."

This field serves for documentation only.

Netflow/IPFIX

Enable this switch to export connections with Netflow/IPFIX, if either their origin or destination is this interface.



In case of a bridge the traffic on all ports is exported.

Default policies

The following table shows and partly even lets you alter the firewall default policy. The defaults depend on the actual zone this interface is in. For the zone assignment, please see option "Zone/Classification (Trustlevel)".

Default policies for routing into bridge

The following table shows and partly even lets you alter the firewall default policy. The defaults depend on the actual zone this interface is in. For the zone assignment, please see option "Zone/Classification (Trustlevel) of bridge as destination interface".

14.2.2-B DNAT > *

On this tab you define portforwarding rules (DNAT). DNAT modifies the destination IP of a connection. This allows for example to establish a direct connection to a server with an internal IP address from the Internet. DNAT rules have to be specified in the connection's inbound interface.



If the destination of the connection after applying the DNAT rules is not SX-GATE itself, you have to activate "IPv4 routing" at "Modules > Firewall > Settings".



A DNAT connection will work only if the new connection target returns the reply packets via SX-GATE. Only then SX-GATE can modify the reply packets so that the client will accept them. If the connection target doesn't route packets back as required, an additional SNAT rule will help.

DNAT (Portforwarding): Source ..., any destination

To add a new entry, please click "New Entry" in the lower left corner of the table. You can use an existing entry as a template: Click the corresponding "Copy" symbol in the last column. You can edit entries by clicking on the pen symbol "Edit". Individual entries are deleted by the thrashcan symbol "Remove". Click the trashcan "Delete selected entries" in the table header to delete all entries you have selected beforehand using the checkboxes at the end of each row. The checkbox in the table header selects all entries. With the arrow buttons "Up" and "Down" you can move an item up or down by one position. To move a row to an other position with Drag'n'Drop, keep the mouse button pressed on the "Drag'n'Drop" symbol right of the arrows. Click the column titles to change the sort order. Please note the import and export buttons at the lower end of the table.



Tables with many entries will not be displayed completely. At the lower right corner a control to change pages will appear instead. Alternatively a grouped display can be selected. There's also an icon to view the complete table in fullscreen mode. This is particularly useful if you need to Drag'n'Drop an entry over many lines.



Rules are evaluated in the given order. The first match applies. Hence more specific rules have to be moved above more general rules. So e.g. a rule for a certain individual IP address must be moved above a rule which refers to the same protocol but an arbitrary IP address.

The following inputs are available:

Active

Use this control to enable or disable a rule at any time. Select date and time to configure a temporary firewall rule which is active until that point of time has been reached.

Log

You can enable logging with this switch. For TCP connections only the initial packet will be written to the log. For all other IP protocols every packet is logged.



You should enable logging only for diagnostic purposes or for rules which are not used frequently. Otherwise your log files may grow rapidly.

Protocol

Select one of the protocols from the list. Each protocol represents a set of IP protocol and port definitions. You will find the details in menu "Definitions > Protocols". This is also where you can extend the list with your own protocol definitions.

Application control works only partially here as DNAT rules have to redirect the very first packet of a connection. With TCP, the first packet transmits no payload, so the application is always unknown at this early stage. With other IP protocols like e.g. UDP the first data packet may include enough information, so that at least some protocols can be detected immediately. Anyway, if the application is still unknown, a DNAT rule will apply already if just the IP protocol and port signature of the packet matches. If it should turn out later that the connection does not match the application, the connection is terminated.

Source (...)

If you leave these fields blank, the rule will apply to any source IP. To grant access for a single client only, please enter its IP address. To give access for a whole network, specify the network address and its corresponding netmask (e.g. 192.168.0.0/24). To configure a rule for multiple individual clients or networks, define a new group in menu "Definitions > IP objects" or select an entry from the list of available groups.

You can also filter the source by MAC address. Refer to objects of type "Host" that you must create in menu "Definitions > IP objects" beforehand. If in such an object only the MAC address has been configured, the rule will check the source by MAC only, regardless if it's IPv4 or IPv6. If an additional IP has been given, the rule will apply only if both, MAC address and IP address match. If the object includes an IPv4 but no IPv6 address, the rule applies to IPv4 packets only and vice versa.



You can combine multiple objects of type "Host" to a group, so a single rule can refer to multiple MAC addresses and MAC/IP combinations.

Policy

Access may either be allowed or forbidden. When denying a connection, SX-GATE will silently discard the IP packet.

Dest.

If you leave these fields blank, the rule will apply to any destination IP. To grant access to a single server only, please enter its IP address. To give access to a whole network, specify the network address and its corresponding netmask (e.g. 192.168.0.0/24). To configure a rule for multiple individual clients or networks,

define a new group in menu "Definitions > IP objects" or select an entry from the list of available groups.



You must not enter an address here if a dynamic IP is assigned to SX-GATE.

to IP

Please enter the new destination address here. This may be an IP of SX-GATE (except 127.0.0.1) or likewise the IP of any other system. Even for "discard" rules an address has to be specified, however the actual value is not considered.

You can establish a static 1:1 mapping between two networks by entering a network address with a corresponding netmask. For example the entry "10.0.0.0/24" will replace the first three octets of any destination IP with "10.0.0", so e.g. the destination IP "192.168.1.254" is mapped to "10.0.0.254".



It is not possible to rewrite the destination port at the same time. You must not enter a "Port".

Port

Leave blank to keep the original destination port. Specify the new destination port otherwise.

Period

You may want to enable certain rules only on specific weekdays during a certain period of time. Here you can assign one of the periods defined in menu "Definitions > Periods".

DoS

If you like you can also activate the Denial-of-Service protection by the dynamic firewall. For TCP the value refers to the maximum number of connections per source IP. For all other protocols you specify the number of packets per source IP.

Comment

Use this field for documentation. Up to 14 characters from this field will be included in the log if logging is enabled for this rule.

14.2.2-C Transp. proxy

Some SX-GATE services can act as a transparent proxy. This allows the use of the proxy with all its benefits without having to reconfigure the clients. The checkboxes on this screen will activate firewall rules to redirect certain connections to the corresponding SX-GATE proxy.



Make sure that the respective proxy service is actually running.

These rules will apply to the connections of all clients connected to the selected interface regardless of source or destination IP. To redirect connections only if specific addresses are involved, you have to configure rules on tab "DNAT > *" instead.

As an example, the redirection to SX-GATE's web proxy will give you an idea which firewall rules are associated with the respective switches. Let's assume SX-GATE's IP address is 192.168.0.254. Connections to any destination's port 80 (HTTP) have to be redirected to SX-GATE's web proxy on port 8082. The DNAT rule "HTTP:*->*>192.168.0.254(8082)" will do this.

Not transparent proxying for connections to

Connections to certain destinations (e.g. internal networks) may be excluded from transparent proxying.



Connections to IP addresses of SX-GATE are always automatically excluded from transparent proxying.

port 80 (HTTP) to web proxy

This checkbox enables transparent access to SX-GATE's web proxy. Connections to any destination's port 80 will be redirected to the web proxy. There's generally no proxy authentication with transparent proxying.



This option is not available if transparent proxying has been disabled in the web proxy configuration.

no content filtering

Select this option to redirect the connections to web proxy port 8083, bypassing the content filter. You may choose this option for a network with low protection needs if the content filter repeatedly causes unexpected problems. But make sure that the firewall denies direct access and access via proxy to networks with higher protection needs.



This option is not available if the content filter is disabled or its configuration does not allow bypassing.

enabled

This setting will redirect the connections to local port 8082. Both, the URL and the content filter will be used if enabled.

port 443 (HTTPS) to web proxy

This checkbox enables transparent HTTPS access to SX-GATE's web proxy. Connections to any destination's port 443 will be redirected to the web proxy. There's generally no proxy authentication with transparent proxying.



This option is not available if transparent proxying has been disabled in the web proxy configuration.

no content filtering

Select this option to redirect the connections to web proxy port 8446, bypassing the content filter. This is useful if the content filter breaks SSL connections but it's not possible to install the proxy CA on devices of a certain network, e.g. an employee wifi with private end devices (BYOD).



This option is not available if the content filter is disabled or its configuration does not allow bypassing.

enabled

This setting will redirect the connections to local port 8445. Both, the URL and the content filter will be used if enabled.

port 21 (FTP) to FTP proxy

Analogical to the previous option, this switch will redirect connections to port 21 to SX-GATE's FTP proxy (port 2121).

port 5060 (voice over IP SIP) to SIP proxy

This switch affects packets corresponding to the Voice over IP protocol SIP. Regardless of the destination IP, packets to TCP and UDP port 5060 will be delivered to the IP of SX-GATE and so to the SIP proxy.

port 110 (POP3) to POP3/SMTP proxy

This option redirects connections to an Internet IP on TCP port 110 via SX-GATE's POP3 proxy (port 8110).

port 25 (SMTP) to

Enable this option to intercept direct SMTP connections to the Internet and redirect them to a service on SX-GATE. From the technical point of view, the destination IP of connections to port 25 will be replaced by SX-GATE's IP.

mail relay server

Select this option to redirect the connection to SX-GATE's mail relay server. All further processing is done by SX-GATE, just as if the sender didn't try a direct Internet connection but delivered straight to SX-GATE.

SMTP proxy

This will forward the mail to SX-GATE's POP3/SMTP proxy (port 8110), which in turn connects to the originally addressed mail server. If enabled, SX-GATE's SMTP proxy will perform a virusscan on the outbound mail. However the actual processing of the message is done by the mail server as predetermined by the sender.

port 53 (DNS) to DNS forwarder

Use this checkbox to pass DNS packets to SX-GATE's caching name server. Both, TCP and UDP packets to port 53 will be affected.

14.2.2-D ... > SX-GATE

This tab addresses connections to SX-GATE. The destination is one of the applications SX-GATE offers.

Input rules: Source ..., destination SX-GATE

To add a new entry, please click "New Entry" in the lower left corner of the table. You can use an existing entry as a template: Click the corresponding "Copy" symbol in the last column. You can edit entries by clicking on the pen symbol "Edit". Individual entries are deleted by the trashcan symbol "Remove". Click the trashcan "Delete selected entries" in the table header to delete all entries you have selected beforehand using the checkboxes at the end of each row. The checkbox in the table header selects all entries. With the arrow buttons "Up" and "Down" you can move an item up or down by one position. To move a row to an other position with Drag'n'Drop, keep the mouse button pressed on the "Drag'n'Drop" symbol right of the arrows. Click the column titles to change the sort order. Please note the import and export buttons at the lower end of the table.



Tables with many entries will not be displayed completely. At the lower right corner a control to change pages will appear instead. Alternatively a grouped display can be selected. There's also an icon to view the complete table in fullscreen mode. This is particularly useful if you need to Drag'n'Drop an entry over many lines.



Rules are evaluated in the given order. The first match applies. Hence more specific rules have to be moved above more general rules. So e.g. a rule for a certain individual IP address must be moved above a rule which refers to the same protocol but an arbitrary IP address.

The following inputs are available:

Active

Use this control to enable or disable a rule at any time. Select date and time to configure a temporary firewall rule which is active until that point of time has been reached.

Log

You can enable logging with this switch. For TCP connections only the initial packet will be written to the log. For all other IP protocols every packet is logged.



You should enable logging only for diagnostic purposes or for rules which are not used frequently. Otherwise your log files may grow rapidly.

Protocol

Select one of the protocols from the list. Each protocol represents a set of IP protocol and port definitions. You will find the details in menu "Definitions > Protocols". This is also where you can extend the list with your own protocol definitions.

Source (...)

If you leave these fields blank, the rule will apply to any source IP. To grant access for a single client only, please enter its IP address. To give access for a whole network, specify the network address and its corresponding netmask (e.g. 192.168.0.0/24). To configure a rule for multiple individual clients or networks, define a new group in menu "Definitions > IP objects" or select an entry from the list of available groups.

You can also filter the source by MAC address. Refer to objects of type "Host" that you must create in menu "Definitions > IP objects" beforehand. If in such an object only the MAC address has been configured, the rule will check the source by MAC

only, regardless if it's IPv4 or IPv6. If an additional IP has been given, the rule will apply only if both, MAC address and IP address match. If the object includes an IPv4 but no IPv6 address, the rule applies to IPv4 packets only and vice versa.



You can combine multiple objects of type "Host" to a group, so a single rule can refer to multiple MAC addresses and MAC/IP combinations.

Policy

Access may either be allowed or forbidden. When denying a connection, SX-GATE can either silently discard the IP packet or reject it with an "administratively prohibited" ICMP reply message. The latter indicates the reason for the connection failure to the sender.

Period

You may want to enable certain rules only on specific weekdays during a certain period of time. Here you can assign one of the periods defined in menu "Definitions > Periods".

DoS

If you like you can also activate the Denial-of-Service protection by the dynamic firewall. For TCP the value refers to the maximum number of connections per source IP. For all other protocols you specify the number of packets per source IP.

Comment

Use this field for documentation. Up to 14 characters from this field will be included in the log if logging is enabled for this rule.

14.2.2-E * > SX-GATE > ...

This tab addresses connections SX-GATE is forwarding, i.e. SX-GATE acts as a router. This always involves two interfaces: The inbound interface, where SX-GATE receives the connections first packet and the outbound interface, where SX-GATE forwards the packet. SX-GATE itself is neither source nor destination of the connection.



In SX-GATE, forwarding rules always have to be configured in the outbound interface.

Forwarding rules: Any source, destination ...

To add a new entry, please click "New Entry" in the lower left corner of the table. You can use an existing entry as a template: Click the corresponding "Copy" symbol in the last column. You can edit entries by clicking on the pen symbol "Edit". Individual entries are deleted by the trashcan symbol "Remove". Click the trashcan "Delete selected entries" in the table header to delete all entries you have selected beforehand using

the checkboxes at the end of each row. The checkbox in the table header selects all entries. With the arrow buttons "Up" and "Down" you can move an item up or down by one position. To move a row to an other position with Drag'n'Drop, keep the mouse button pressed on the "Drag'n'Drop" symbol right of the arrows. Click the column titles to change the sort order. Please note the import and export buttons at the lower end of the table.



Tables with many entries will not be displayed completely. At the lower right corner a control to change pages will appear instead. Alternatively a grouped display can be selected. There's also an icon to view the complete table in fullscreen mode. This is particularly useful if you need to Drag'n'Drop an entry over many lines.



Rules are evaluated in the given order. The first match applies. Hence more specific rules have to be moved above more general rules. So e.g. a rule for a certain individual IP address must be moved above a rule which refers to the same protocol but an arbitrary IP address.

The following inputs are available:

Active

Use this control to enable or disable a rule at any time. Select date and time to configure a temporary firewall rule which is active until that point of time has been reached.

Log

You can enable logging with this switch. For TCP connections only the initial packet will be written to the log. For all other IP protocols every packet is logged.



You should enable logging only for diagnostic purposes or for rules which are not used frequently. Otherwise your log files may grow rapidly.

Protocol

Select one of the protocols from the list. Each protocol represents a set of IP protocol and port definitions. You will find the details in menu "Definitions > Protocols". This is also where you can extend the list with your own protocol definitions.

Source zone

Use this setting to restrict the rule to connections originating in a specific zone.

Source IP/network

If you leave these fields blank, the rule will apply to any source IP. To grant access for a single client only, please enter its IP address. To give access for a whole network, specify the network address and its corresponding netmask (e.g. 192.168.0.0/24). To configure a rule for multiple individual clients or networks, define a new group in menu "Definitions > IP objects" or select an entry from the list of available groups.

You can also filter the source by MAC address. Refer to objects of type "Host" that you must create in menu "Definitions > IP objects" beforehand. If in such an object only the MAC address has been configured, the rule will check the source by MAC only, regardless if it's IPv4 or IPv6. If an additional IP has been given, the rule will apply only if both, MAC address and IP address match. If the object includes an IPv4 but no IPv6 address, the rule applies to IPv4 packets only and vice versa.



You can combine multiple objects of type "Host" to a group, so a single rule can refer to multiple MAC addresses and MAC/IP combinations.

Policy

Access may either be allowed or forbidden. When denying a connection, SX-GATE can either silently discard the IP packet or reject it with an "administratively prohibited" ICMP reply message. The latter indicates the reason for the connection failure to the sender.

Dest. (...)

If you leave these fields blank, the rule will apply to any destination IP. To grant access to a single server only, please enter its IP address. To give access to a whole network, specify the network address and its corresponding netmask (e.g. 192.168.0.0/24). To configure a rule for multiple individual clients or networks, define a new group in menu "Definitions > IP objects" or select an entry from the list of available groups.

Period

You may want to enable certain rules only on specific weekdays during a certain period of time. Here you can assign one of the periods defined in menu "Definitions > Periods".

DoS

If you like you can also activate the Denial-of-Service protection by the dynamic firewall. For TCP the value refers to the maximum number of connections per source IP. For all other protocols you specify the number of packets per source IP.

Comment

Use this field for documentation. Up to 14 characters from this field will be included in the log if logging is enabled for this rule.

14.2.2-F * > SX-GATE > ...

This tab is available on bridge interfaces only. It addresses connections routed into the bridge from outside the bridge. When the firewall processes these packets, unfortunately the target bridge port has not been determined yet. So these rules cannot be configured by bridge port but only for the bridge as a whole.

Forwarding rules: source: any interface except bridge ports, destination: bridge ...

To add a new entry, please click "New Entry" in the lower left corner of the table. You can use an existing entry as a template: Click the corresponding "Copy" symbol in the last column. You can edit entries by clicking on the pen symbol "Edit". Individual entries are deleted by the trashcan symbol "Remove". Click the trashcan "Delete selected entries" in the table header to delete all entries you have selected beforehand using the checkboxes at the end of each row. The checkbox in the table header selects all entries. With the arrow buttons "Up" and "Down" you can move an item up or down by one position. To move a row to an other position with Drag'n'Drop, keep the mouse button pressed on the "Drag'n'Drop" symbol right of the arrows. Click the column titles to change the sort order. Please note the import and export buttons at the lower end of the table.



Tables with many entries will not be displayed completely. At the lower right corner a control to change pages will appear instead. Alternatively a grouped display can be selected. There's also an icon to view the complete table in fullscreen mode. This is particularly useful if you need to Drag'n'Drop an entry over many lines.



Rules are evaluated in the given order. The first match applies. Hence more specific rules have to be moved above more general rules. So e.g. a rule for a certain individual IP address must be moved above a rule which refers to the same protocol but an arbitrary IP address.

The following inputs are available:

Active

Use this control to enable or disable a rule at any time. Select date and time to configure a temporary firewall rule which is active until that point of time has been reached.

Log

You can enable logging with this switch. For TCP connections only the initial packet will be written to the log. For all other IP protocols every packet is logged.



You should enable logging only for diagnostic purposes or for rules which are not used frequently. Otherwise your log files may grow rapidly.

Protocol

Select one of the protocols from the list. Each protocol represents a set of IP protocol and port definitions. You will find the details in menu "Definitions > Protocols". This is also where you can extend the list with your own protocol definitions.

Source zone

Use this setting to restrict the rule to connections originating in a specific zone.

Source IP/network

If you leave these fields blank, the rule will apply to any source IP. To grant access for a single client only, please enter its IP address. To give access for a whole network, specify the network address and its corresponding netmask (e.g. 192.168.0.0/24). To configure a rule for multiple individual clients or networks, define a new group in menu "Definitions > IP objects" or select an entry from the list of available groups.

You can also filter the source by MAC address. Refer to objects of type "Host" that you must create in menu "Definitions > IP objects" beforehand. If in such an object only the MAC address has been configured, the rule will check the source by MAC only, regardless if it's IPv4 or IPv6. If an additional IP has been given, the rule will apply only if both, MAC address and IP address match. If the object includes an IPv4 but no IPv6 address, the rule applies to IPv4 packets only and vice versa.



You can combine multiple objects of type "Host" to a group, so a single rule can refer to multiple MAC addresses and MAC/IP combinations.

Policy

Access may either be allowed or forbidden. When denying a connection, SX-GATE can either silently discard the IP packet or reject it with an "administratively prohibited" ICMP reply message. The latter indicates the reason for the connection failure to the sender.

Dest. (...)

If you leave these fields blank, the rule will apply to any destination IP. To grant access to a single server only, please enter its IP address. To give access to a whole network, specify the network address and its corresponding netmask (e.g. 192.168.0.0/24). To configure a rule for multiple individual clients or networks,

define a new group in menu "Definitions > IP objects" or select an entry from the list of available groups.

Period

You may want to enable certain rules only on specific weekdays during a certain period of time. Here you can assign one of the periods defined in menu "Definitions > Periods".

DoS

If you like you can also activate the Denial-of-Service protection by the dynamic firewall. For TCP the value refers to the maximum number of connections per source IP. For all other protocols you specify the number of packets per source IP.

Comment

Use this field for documentation. Up to 14 characters from this field will be included in the log if logging is enabled for this rule.

14.2.2-G SX-GATE > ...

This tab addresses connections initiated by SX-GATE itself.



Besides system functions like storing backups on some server, outbound connections includes those established by SX-GATE's proxies.

Restricting SX-GATE's outbound connections makes sense if for example SX-GATE separates two networks which must not have access to each other. Direct connections between the two networks can be prevented by an appropriate configuration of forwarding rules. However if access to the proxy servers of SX-GATE is allowed, these could be abused to get indirect access to the other network. With this control you can restrict these outbound connections.

Output rules: Source SX-GATE, destination ...

To add a new entry, please click "New Entry" in the lower left corner of the table. You can use an existing entry as a template: Click the corresponding "Copy" symbol in the last column. You can edit entries by clicking on the pen symbol "Edit". Individual entries are deleted by the trashcan symbol "Remove". Click the trashcan "Delete selected entries" in the table header to delete all entries you have selected beforehand using the checkboxes at the end of each row. The checkbox in the table header selects all entries. With the arrow buttons "Up" and "Down" you can move an item up or down by one position. To move a row to an other position with Drag'n'Drop, keep the mouse button pressed on the "Drag'n'Drop" symbol right of the arrows. Click the column titles to change the sort order. Please note the import and export buttons at the lower end of the table.



Tables with many entries will not be displayed completely. At the lower right corner a control to change pages will appear instead. Alternatively a grouped display can be selected. There's also an icon to view the complete table in fullscreen mode. This is particularly useful if you need to Drag'n'Drop an entry over many lines.



Rules are evaluated in the given order. The first match applies. Hence more specific rules have to be moved above more general rules. So e.g. a rule for a certain individual IP address must be moved above a rule which refers to the same protocol but an arbitrary IP address.

The following inputs are available:

Active

Use this control to enable or disable a rule at any time. Select date and time to configure a temporary firewall rule which is active until that point of time has been reached.

Log

You can enable logging with this switch. For TCP connections only the initial packet will be written to the log. For all other IP protocols every packet is logged.



You should enable logging only for diagnostic purposes or for rules which are not used frequently. Otherwise your log files may grow rapidly.

Protocol

Select one of the protocols from the list. Each protocol represents a set of IP protocol and port definitions. You will find the details in menu "Definitions > Protocols". This is also where you can extend the list with your own protocol definitions.

Policy

Access may either be allowed or forbidden. When denying a connection, SX-GATE can either silently discard the IP packet or reject it with an "administratively prohibited" ICMP reply message. The latter indicates the reason for the connection failure to the sender.

Dest. (...)

If you leave these fields blank, the rule will apply to any destination IP. To grant access to a single server only, please enter its IP address. To give access to a whole network, specify the network address and its corresponding netmask (e.g. 192.168.0.0/24). To configure a rule for multiple individual clients or networks,

define a new group in menu "Definitions > IP objects" or select an entry from the list of available groups.

DoS

If you like you can also activate the Denial-of-Service protection by the dynamic firewall. For TCP the value refers to the maximum number of connections per source IP. For all other protocols you specify the number of packets per source IP.

Comment

Use this field for documentation. Up to 14 characters from this field will be included in the log if logging is enabled for this rule.

14.2.2-H * > SNAT

On this tab you define Network-Address-Translation rules (NAT, SNAT). SNAT modifies the source IP of a connection. This is necessary when IP packets with an internal source IP have to be forwarded to the Internet. SNAT can also be used to set a specific sender address for certain services if multiple Internet IPs are assigned to SX-GATE.



In most cases it is not necessary to configure anything here. The default behaviour is "automatic SNAT", i.e. NAT will apply only on interfaces classified as "Internet", and only to IPv4 connections originating in the LAN or RAS zone. As an exception there's no automatic SNAT on DS-Lite links.

SNAT: Any source, destination ...

To add a new entry, please click "New Entry" in the lower left corner of the table. You can use an existing entry as a template: Click the corresponding "Copy" symbol in the last column. You can edit entries by clicking on the pen symbol "Edit". Individual entries are deleted by the trashcan symbol "Remove". Click the trashcan "Delete selected entries" in the table header to delete all entries you have selected beforehand using the checkboxes at the end of each row. The checkbox in the table header selects all entries. With the arrow buttons "Up" and "Down" you can move an item up or down by one position. To move a row to an other position with Drag'n'Drop, keep the mouse button pressed on the "Drag'n'Drop" symbol right of the arrows. Click the column titles to change the sort order. Please note the import and export buttons at the lower end of the table.



Tables with many entries will not be displayed completely. At the lower right corner a control to change pages will appear instead. Alternatively a grouped display can be selected. There's also an icon to view the complete table in fullscreen mode. This is particularly useful if you need to Drag'n'Drop an entry over many lines.



Rules are evaluated in the given order. The first match applies. Hence more specific rules have to be moved above more general rules. So e.g. a rule for a certain individual IP address must be moved above a rule which refers to the same protocol but an arbitrary IP address.

The following inputs are available:

Active

Use this checkbox to enable or disable a rule at any time.

Log

You can enable logging with this switch. For TCP connections only the initial packet will be written to the log. For all other IP protocols every packet is logged.



You should enable logging only for diagnostic purposes or for rules which are not used frequently. Otherwise your log files may grow rapidly.

Protocol

Select one of the protocols from the list. Each protocol represents a set of IP protocol and port definitions. You will find the details in menu "Definitions > Protocols". This is also where you can extend the list with your own protocol definitions.

Application control settings will be ignored.

Source zone

Use this setting to restrict the rule to connections originating in a specific zone or to connections established by SX-GATE itself.

Source IP/network

If you leave these fields blank, the rule will apply to any source IP. To grant access for a single client only, please enter its IP address. To give access for a whole network, specify the network address and its corresponding netmask (e.g. 192.168.0.0/24). To configure a rule for multiple individual clients or networks, define a new group in menu "Definitions > IP objects" or select an entry from the list of available groups.

It is not possible to filter the source of SNAT rules by MAC address. MAC addresses in objects will be ignored.

NAT

This switch controls Network Address Translation (NAT, SNAT). With SNAT, SX-GATE will replace the original source IP with its own IP address.

Automatic NAT will only apply to IPv4 connections originating in LAN or RAS zones with an Internet destination, except for DS-Lite Internet links.

It is possible to associate a specific NAT IP address with each rule. This way you can create a static mapping between an internal and an external IP address if SX-GATE has multiple Internet IP addresses. If you do not impose an IP, SX-GATE will automatically use the interface's primary IP.



You must not enter an address here if a dynamic IP is assigned to SX-GATE.

You can even establish a static 1:1 mapping between two networks by entering a network address with a corresponding netmask. For example the entry "10.0.0.0/24" will replace the first three octets of any source IP with "10.0.0", so e.g. the source IP "192.168.1.254" is mapped to "10.0.0.254".

Dest. (...)

If you leave these fields blank, the rule will apply to any destination IP. To grant access to a single server only, please enter its IP address. To give access to a whole network, specify the network address and its corresponding netmask (e.g. 192.168.0.0/24). To configure a rule for multiple individual clients or networks, define a new group in menu "Definitions > IP objects" or select an entry from the list of available groups.

Comment

Use this field for documentation. Up to 14 characters from this field will be included in the log if logging is enabled for this rule.

14.2.2-I Options

Automatic blocking of suspicious IPs (dynamic firewall)

The firewall continuously registers connection attempts to blocked ports, connection rates exceeding the limits specified in firewall rules, portscans and also pings or traceroutes by source IP. If a threshold is exceeded for an IP address, it may be automatically blocked for a certain period of time.

Block privat IP addresses (RFC-1918 and RFC-4193)

If this switch is activated, all packets that run via this interface will be checked for IP addresses from the following networks: 192.168.0.0/255.255.0.0, 172.16.0.0/255.240.0.0 and 10.0.0.0/255.0.0.0 as well as fc00::/7. All inbound and

outbound packets with corresponding source or destination addresses will be discarded.

Fake reply to inbound Traceroute and ICMP-Ping

When this option is active, the firewall will reply to inbound ICMP echo-request regardless of the actual destination IP. Incoming packets with a low TTL value may indicate an inbound traceroute. Also these packets will be answered by the firewall. For the sender of the traceroute it appears, that SX-GATE itself is the destination of the traceroute.



If SX-GATE is used as a firewall protecting a network with Internet IP addresses (e.g. a DMZ), this feature can be used to hide the internal network structure and the actually active servers to a certain extend.

14.2.3 Bridge

If there are any bridge interfaces, you can configure the firewall for each bridge port in this menu. This included in particular DNAT rules, access to SX-GATE services from within the bridge and firewall rules for bridged traffic, i.e. connections forwarded from one bridge port to an other. For each bridge port the firewall zone must be selected to determine the default behaviour of the firewall.



No port based configuration is available for connections routed from other interfaces (or bridges) into a bridge. The same applies to connections initiated by a SX-GATE service and SNAT rules. Please configure these settings in menu "Policies".



Imprudent changes of settings in this menu can affect the system security of SX-GATE and of all networks protected by SX-GATE.

A table gives you an overview of the available objects. If multiple columns are displayed you can change the sort order by clicking the column title. If there are more than 20 entries, a navigation bar will appear below the bottom right hand corner of the table. You can switch between a grouped view or a pager. The full screen mode allows you to see all entries at the same time. Pick an entry by clicking its title in the left column. A pencil icon or a trashcan in the right column allow you to rename or delete an entry.

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

14.2.3-A General.....	400
14.2.3-B DNAT > *.....	400
14.2.3-C Transp. proxy.....	403
14.2.3-D ... > SX-GATE.....	406
14.2.3-E * > Bridge >	408
14.2.3-F Options.....	410

Zone/Classification (Trustlevel) of the bridge port

Use this control to define the base configuration of the firewall for the selected bridge port. The setting applies to bridged connections, connections to SX-GATE services and to connections routed from within the bridge into a different interface (or bridge).

The following table shows the default behaviour of the firewall. The source refers to the classification of the inbound port whereas the destination refers to the classification of the outbound port (bridged connections) or the outbound interface (connections routed from within the bridge into a different interface or bridge). The column labeled "SX-GATE" shows the default policy for connections to SX-GATE. No SNAT is applied to bridged traffic. The annotation "Auto SNAT" applies to routed connections only.

Source	Destination				
	Internet (none)	DMZ (low)	RAS (medium)	LAN (high)	SX-GATE
Internet (none)					
DMZ (low)					
RAS (medium)	Auto SNAT				
LAN (high)	Auto SNAT				

	Access denied. Add rules to allow specific connections
	Access denied. Add rules or change default policy to grant access
	Access granted. Restrict by changing the default policy

14.2.3-A General

Description "..."

This field serves for documentation only.

Default policies

The following table shows and partly even lets you alter the firewall default policy. The defaults depend on the actual zone this interface is in. For the zone assignment, please see option "Zone/Classification (Trustlevel) of the bridge port".

14.2.3-B DNAT > *

On this tab you define portforwarding rules (DNAT). DNAT modifies the destination IP of a connection. This allows for example to establish a direct connection to a server with an internal IP address from the Internet. DNAT rules have to be specified in the connection's inbound interface.



If the destination of the connection after applying the DNAT rules is not SX-GATE itself, you have to activate "IPv4 routing" at "Modules > Firewall > Settings".



A DNAT connection will work only if the new connection target returns the reply packets via SX-GATE. Only then SX-GATE can modify the reply packets so that the client will accept them. If the connection target doesn't route packets back as required, an additional SNAT rule will help.

DNAT (Portforwarding): Source ..., any destination

To add a new entry, please click "New Entry" in the lower left corner of the table. You can use an existing entry as a template: Click the corresponding "Copy" symbol in the last column. You can edit entries by clicking on the pen symbol "Edit". Individual entries are deleted by the thrashcan symbol "Remove". Click the trashcan "Delete selected entries" in the table header to delete all entries you have selected beforehand using the checkboxes at the end of each row. The checkbox in the table header selects all entries. With the arrow buttons "Up" and "Down" you can move an item up or down by one position. To move a row to an other position with Drag'n'Drop, keep the mouse button pressed on the "Drag'n'Drop" symbol right of the arrows. Click the column titles to change the sort order. Please note the import and export buttons at the lower end of the table.



Tables with many entries will not be displayed completely. At the lower right corner a control to change pages will appear instead. Alternatively a grouped display can be selected. There's also an icon to view the complete table in fullscreen mode. This is particularly useful if you need to Drag'n'Drop an entry over many lines.



Rules are evaluated in the given order. The first match applies. Hence more specific rules have to be moved above more general rules. So e.g. a rule for a certain individual IP address must be moved above a rule which refers to the same protocol but an arbitrary IP address.

The following inputs are available:

Active

Use this control to enable or disable a rule at any time. Select date and time to configure a temporary firewall rule which is active until that point of time has been reached.

Log

You can enable logging with this switch. For TCP connections only the initial packet will be written to the log. For all other IP protocols every packet is logged.



You should enable logging only for diagnostic purposes or for rules which are not used frequently. Otherwise your log files may grow rapidly.

Protocol

Select one of the protocols from the list. Each protocol represents a set of IP protocol and port definitions. You will find the details in menu "Definitions > Protocols". This is also where you can extend the list with your own protocol definitions.

Application control works only partially here as DNAT rules have to redirect the very first packet of a connection. With TCP, the first packet transmits no payload, so the application is always unknown at this early stage. With other IP protocols like e.g. UDP the first data packet may include enough information, so that at least some protocols can be detected immediately. Anyway, if the application is still unknown, a DNAT rule will apply already if just the IP protocol and port signature of the packet matches. If it should turn out later that the connection does not match the application, the connection is terminated.

Source (...)

If you leave these fields blank, the rule will apply to any source IP. To grant access for a single client only, please enter its IP address. To give access for a whole network, specify the network address and its corresponding netmask (e.g. 192.168.0.0/24). To configure a rule for multiple individual clients or networks, define a new group in menu "Definitions > IP objects" or select an entry from the list of available groups.

You can also filter the source by MAC address. Refer to objects of type "Host" that you must create in menu "Definitions > IP objects" beforehand. If in such an object only the MAC address has been configured, the rule will check the source by MAC only, regardless if it's IPv4 or IPv6. If an additional IP has been given, the rule will apply only if both, MAC address and IP address match. If the object includes an IPv4 but no IPv6 address, the rule applies to IPv4 packets only and vice versa.



You can combine multiple objects of type "Host" to a group, so a single rule can refer to multiple MAC addresses and MAC/IP combinations.

Policy

Access may either be allowed or forbidden. When denying a connection, SX-GATE will silently discard the IP packet.

Dest.

If you leave these fields blank, the rule will apply to any destination IP. To grant access to a single server only, please enter its IP address. To give access to a whole network, specify the network address and its corresponding netmask (e.g. 192.168.0.0/24). To configure a rule for multiple individual clients or networks, define a new group in menu "Definitions > IP objects" or select an entry from the list of available groups.



You must not enter an address here if a dynamic IP is assigned to SX-GATE.

to IP

Please enter the new destination address here. This may be an IP of SX-GATE (except 127.0.0.1) or likewise the IP of any other system. Even for "discard" rules an address has to be specified, however the actual value is not considered.

You can establish a static 1:1 mapping between two networks by entering a network address with a corresponding netmask. For example the entry "10.0.0.0/24" will replace the first three octets of any destination IP with "10.0.0", so e.g. the destination IP "192.168.1.254" is mapped to "10.0.0.254".



It is not possible to rewrite the destination port at the same time. You must not enter a "Port".

Port

Leave blank to keep the original destination port. Specify the new destination port otherwise.

Period

You may want to enable certain rules only on specific weekdays during a certain period of time. Here you can assign one of the periods defined in menu "Definitions > Periods".

DoS

If you like you can also activate the Denial-of-Service protection by the dynamic firewall. For TCP the value refers to the maximum number of connections per source IP. For all other protocols you specify the number of packets per source IP.

Comment

Use this field for documentation. Up to 14 characters from this field will be included in the log if logging is enabled for this rule.

14.2.3-C Transp. proxy

Some SX-GATE services can act as a transparent proxy. This allows the use of the proxy with all its benefits without having to reconfigure the clients. The checkboxes on this screen will activate firewall rules to redirect certain connections to the corresponding SX-GATE proxy.



Make sure that the respective proxy service is actually running.

These rules will apply to the connections of all clients connected to the selected interface regardless of source or destination IP. To redirect connections only if specific addresses are involved, you have to configure rules on tab "DNAT > *" instead.

As an example, the redirection to SX-GATE's web proxy will give you an idea which firewall rules are associated with the respective switches. Let's assume SX-GATE's IP address is 192.168.0.254. Connections to any destination's port 80 (HTTP) have to be redirected to SX-GATE's web proxy on port 8082. The DNAT rule "HTTP:*->*>192.168.0.254(8082)" will do this.

Not transparent proxying for connections to

Connections to certain destinations (e.g. internal networks) may be excluded from transparent proxying.



Connections to IP addresses of SX-GATE are always automatically excluded from transparent proxying.

port 80 (HTTP) to web proxy

This checkbox enables transparent access to SX-GATE's web proxy. Connections to any destination's port 80 will be redirected to the web proxy. There's generally no proxy authentication with transparent proxying.



This option is not available if transparent proxying has been disabled in the web proxy configuration.

no content filtering

Select this option to redirect the connections to web proxy port 8083, bypassing the content filter. You may choose this option for a network with low protection needs if the content filter repeatedly causes unexpected problems. But make sure that the firewall denies direct access and access via proxy to networks with higher protection needs.



This option is not available if the content filter is disabled or its configuration does not allow bypassing.

enabled

This setting will redirect the connections to local port 8082. Both, the URL and the content filter will be used if enabled.

port 443 (HTTPS) to web proxy

This checkbox enables transparent HTTPS access to SX-GATE's web proxy. Connections to any destination's port 443 will be redirected to the web proxy. There's generally no proxy authentication with transparent proxying.



This option is not available if transparent proxying has been disabled in the web proxy configuration.

no content filtering

Select this option to redirect the connections to web proxy port 8446, bypassing the content filter. This is useful if the content filter breaks SSL connections but it's not possible to install the proxy CA on devices of a certain network, e.g. an employee wifi with private end devices (BYOD).



This option is not available if the content filter is disabled or its configuration does not allow bypassing.

enabled

This setting will redirect the connections to local port 8445. Both, the URL and the content filter will be used if enabled.

port 21 (FTP) to FTP proxy

Analogical to the previous option, this switch will redirect connections to port 21 to SX-GATE's FTP proxy (port 2121).

port 5060 (voice over IP SIP) to SIP proxy

This switch affects packets corresponding to the Voice over IP protocol SIP. Regardless of the destination IP, packets to TCP and UDP port 5060 will be delivered to the IP of SX-GATE and so to the SIP proxy.

port 110 (POP3) to POP3/SMTP proxy

This option redirects connections to an Internet IP on TCP port 110 via SX-GATE's POP3 proxy (port 8110).

port 25 (SMTP) to

Enable this option to intercept direct SMTP connections to the Internet and redirect them to a service on SX-GATE. From the technical point of view, the destination IP of connections to port 25 will be replaced by SX-GATE's IP.

mail relay server

Select this option to redirect the connection to SX-GATE's mail relay server. All further processing is done by SX-GATE, just as if the sender didn't try a direct Internet connection but delivered straight to SX-GATE.

SMTP proxy

This will forward the mail to SX-GATE's POP3/SMTP proxy (port 8110), which in turn connects to the originally addressed mail server. If enabled, SX-GATE's SMTP proxy will perform a virusscan on the outbound mail. However the actual processing of the message is done by the mail server as predetermined by the sender.

port 53 (DNS) to DNS forwarder

Use this checkbox to pass DNS packets to SX-GATE's caching name server. Both, TCP and UDP packets to port 53 will be affected.

14.2.3-D ... > SX-GATE

This tab addresses connections to SX-GATE. The destination is one of the applications SX-GATE offers.

Input rules: Source ..., destination SX-GATE

To add a new entry, please click "New Entry" in the lower left corner of the table. You can use an existing entry as a template: Click the corresponding "Copy" symbol in the last column. You can edit entries by clicking on the pen symbol "Edit". Individual entries are deleted by the trashcan symbol "Remove". Click the trashcan "Delete selected entries" in the table header to delete all entries you have selected beforehand using the checkboxes at the end of each row. The checkbox in the table header selects all entries. With the arrow buttons "Up" and "Down" you can move an item up or down by one position. To move a row to an other position with Drag'n'Drop, keep the mouse button pressed on the "Drag'n'Drop" symbol right of the arrows. Click the column titles to change the sort order. Please note the import and export buttons at the lower end of the table.



Tables with many entries will not be displayed completely. At the lower right corner a control to change pages will appear instead. Alternatively a grouped display can be selected. There's also an icon to view the complete table in fullscreen mode. This is particularly useful if you need to Drag'n'Drop an entry over many lines.



Rules are evaluated in the given order. The first match applies. Hence more specific rules have to be moved above more general rules. So e.g. a rule for a certain individual IP address must be moved above a rule which refers to the same protocol but an arbitrary IP address.

The following inputs are available:

Active

Use this control to enable or disable a rule at any time. Select date and time to configure a temporary firewall rule which is active until that point of time has been reached.

Log

You can enable logging with this switch. For TCP connections only the initial packet will be written to the log. For all other IP protocols every packet is logged.



You should enable logging only for diagnostic purposes or for rules which are not used frequently. Otherwise your log files may grow rapidly.

Protocol

Select one of the protocols from the list. Each protocol represents a set of IP protocol and port definitions. You will find the details in menu "Definitions > Protocols". This is also where you can extend the list with your own protocol definitions.

Source (...)

If you leave these fields blank, the rule will apply to any source IP. To grant access for a single client only, please enter its IP address. To give access for a whole network, specify the network address and its corresponding netmask (e.g. 192.168.0.0/24). To configure a rule for multiple individual clients or networks, define a new group in menu "Definitions > IP objects" or select an entry from the list of available groups.

You can also filter the source by MAC address. Refer to objects of type "Host" that you must create in menu "Definitions > IP objects" beforehand. If in such an object only the MAC address has been configured, the rule will check the source by MAC only, regardless if it's IPv4 or IPv6. If an additional IP has been given, the rule will apply only if both, MAC address and IP address match. If the object includes an IPv4 but no IPv6 address, the rule applies to IPv4 packets only and vice versa.



You can combine multiple objects of type "Host" to a group, so a single rule can refer to multiple MAC addresses and MAC/IP combinations.

Policy

Access may either be allowed or forbidden. When denying a connection, SX-GATE can either silently discard the IP packet or reject it with an "administratively prohibited" ICMP reply message. The latter indicates the reason for the connection failure to the sender.

Period

You may want to enable certain rules only on specific weekdays during a certain period of time. Here you can assign one of the periods defined in menu "Definitions > Periods".

DoS

If you like you can also activate the Denial-of-Service protection by the dynamic firewall. For TCP the value refers to the maximum number of connections per source IP. For all other protocols you specify the number of packets per source IP.

Comment

Use this field for documentation. Up to 14 characters from this field will be included in the log if logging is enabled for this rule.

14.2.3-E * > Bridge > ...

This tab addresses connections SX-GATE is forwarding from one bridge port to another. SX-GATE itself is neither source nor destination of the connection.



In SX-GATE, forwarding rules always have to be configured in the outbound port.

Bridging rules: Source: any bridge port, destination: bridge port ...

To add a new entry, please click "New Entry" in the lower left corner of the table. You can use an existing entry as a template: Click the corresponding "Copy" symbol in the last column. You can edit entries by clicking on the pen symbol "Edit". Individual entries are deleted by the thrashcan symbol "Remove". Click the trashcan "Delete selected entries" in the table header to delete all entries you have selected beforehand using the checkboxes at the end of each row. The checkbox in the table header selects all entries. With the arrow buttons "Up" and "Down" you can move an item up or down by one position. To move a row to an other position with Drag'n'Drop, keep the mouse button pressed on the "Drag'n'Drop" symbol right of the arrows. Click the column titles to change the sort order. Please note the import and export buttons at the lower end of the table.



Tables with many entries will not be displayed completely. At the lower right corner a control to change pages will appear instead. Alternatively a grouped display can be selected. There's also an icon to view the complete table in fullscreen mode. This is particularly useful if you need to Drag'n'Drop an entry over many lines.



Rules are evaluated in the given order. The first match applies. Hence more specific rules have to be moved above more general rules. So e.g. a rule for a certain individual IP address must be moved above a rule which refers to the same protocol but an arbitrary IP address.

The following inputs are available:

Active

Use this control to enable or disable a rule at any time. Select date and time to configure a temporary firewall rule which is active until that point of time has been reached.

Log

You can enable logging with this switch. For TCP connections only the initial packet will be written to the log. For all other IP protocols every packet is logged.



You should enable logging only for diagnostic purposes or for rules which are not used frequently. Otherwise your log files may grow rapidly.

Protocol

Select one of the protocols from the list. Each protocol represents a set of IP protocol and port definitions. You will find the details in menu "Definitions > Protocols". This is also where you can extend the list with your own protocol definitions.

Source zone

Use this setting to restrict the rule to connections originating in a specific zone.

Source IP/network

If you leave these fields blank, the rule will apply to any source IP. To grant access for a single client only, please enter its IP address. To give access for a whole network, specify the network address and its corresponding netmask (e.g. 192.168.0.0/24). To configure a rule for multiple individual clients or networks, define a new group in menu "Definitions > IP objects" or select an entry from the list of available groups.

You can also filter the source by MAC address. Refer to objects of type "Host" that you must create in menu "Definitions > IP objects" beforehand. If in such an object only the MAC address has been configured, the rule will check the source by MAC only, regardless if it's IPv4 or IPv6. If an additional IP has been given, the rule will apply only if both, MAC address and IP address match. If the object includes an IPv4 but no IPv6 address, the rule applies to IPv4 packets only and vice versa.



You can combine multiple objects of type "Host" to a group, so a single rule can refer to multiple MAC addresses and MAC/IP combinations.

Policy

Access may either be allowed or forbidden. When denying a connection, SX-GATE can either silently discard the IP packet or reject it with an "administratively prohibited" ICMP reply message. The latter indicates the reason for the connection failure to the sender.

Dest. (...)

If you leave these fields blank, the rule will apply to any destination IP. To grant access to a single server only, please enter its IP address. To give access to a whole network, specify the network address and its corresponding netmask (e.g. 192.168.0.0/24). To configure a rule for multiple individual clients or networks,

define a new group in menu "Definitions > IP objects" or select an entry from the list of available groups.

Period

You may want to enable certain rules only on specific weekdays during a certain period of time. Here you can assign one of the periods defined in menu "Definitions > Periods".

DoS

If you like you can also activate the Denial-of-Service protection by the dynamic firewall. For TCP the value refers to the maximum number of connections per source IP. For all other protocols you specify the number of packets per source IP.

Comment

Use this field for documentation. Up to 14 characters from this field will be included in the log if logging is enabled for this rule.

14.2.3-F Options

Automatic blocking of suspicious IPs (dynamic firewall)

The firewall continuously registers connection attempts to blocked ports, connection rates exceeding the limits specified in firewall rules, portscans and also pings or traceroutes by source IP. If a threshold is exceeded for an IP address, it may be automatically blocked for a certain period of time.

Block privat IP addresses (RFC-1918 and RFC-4193)

If this switch is activated, all packets that run via this interface will be checked for IP addresses from the following networks: 192.168.0.0/255.255.0.0, 172.16.0.0/255.240.0.0 and 10.0.0.0/255.0.0.0 as well as fc00::/7. All inbound and outbound packets with corresponding source or destination addresses will be discarded.

Fake reply to inbound Traceroute and ICMP-Ping

When this option is active, the firewall will reply to inbound ICMP echo-request regardless of the actual destination IP. Incoming packets with a low TTL value may indicate an inbound traceroute. Also these packets will be answered by the firewall. For the sender of the traceroute it appears, that SX-GATE itself is the destination of the traceroute.



If SX-GATE is used as a firewall protecting a network with Internet IP addresses (e.g. a DMZ), this feature can be used to hide the internal network structure and the actually active servers to a certain extend.

14.3 DHCP

SX-GATE can provide a DHCP server for Ethernet, VLAN, and WLAN interfaces. For the directly attached networks SX-GATE can hand out both, IPv4 and IPv6 addresses. Click on the interface name to configure. For IPv4 the DHCP server can also be used for networks using a DHCP relay. Click "Indirect subnets" next to the interface name to configure. Alternatively SX-GATE can run a DHCP relay for IPv4. Again, click the interface name to configure.

A table gives you an overview of the available objects. If multiple columns are displayed you can change the sort order by clicking the column title. If there are more than 20 entries, a navigation bar will appear below the bottom right hand corner of the table. You can switch between a grouped view or a pager. The full screen mode allows you to see all entries at the same time. Pick an entry by clicking its title in the left column. A pencil icon or a trashcan in the right column allow you to rename or delete an entry.

14.3.1

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

14.3.1-A Dynamic IPv4 ranges.....	412
14.3.1-B Static IPv4 addresses.....	413
14.3.1-C Network parameters.....	413
14.3.1-D Windows parameters.....	414
14.3.1-E More parameters.....	415
14.3.1-F Custom options.....	415
14.3.1-G DHCPv4 relay.....	415
14.3.1-H Dynamic IPv6 ranges.....	416
14.3.1-I Static IPv6 addresses.....	416
14.3.1-J DHCPv6 network parameters.....	417

DHCPv4

Please select the DHCPv4 mode.

Server

In this mode SX-GATE will assign the IP address.

Relay

In this mode SX-GATE will forward DHCP queries to a DHCP server in another network.

14.3.1-A Dynamic IPv4 ranges

Dynamically assigned IP ranges

Here you can specify the IP addresses which SX-GATE will assign to devices requesting an IP by DHCP. Please make sure that none of the addresses entered here is already statically assigned to a device in the network. This could lead to conflicts with double IP addresses.



You may set the network part of the IP addresses to "0" to specify them in relation to the interface's primary subnet. So e.g. if the primary subnet is 192.168.0.0/24, the range "0.0.0.100-0.0.0.199" actually means "192.168.0.100-192.168.0.199".



All listed address ranges must belong to the primary IP subnet of the selected interface.

Lease time

Using the lease time, you can define how long an allocated address is to be reserved for a device. Select a low value if it frequently occurs that devices are linked with the LAN for a short time.

SX-GATE is backup DHCP server (secondary)

Activate this option if you want to use SX-GATE as secondary DHCP-server.



If you unnecessarily configure the DHCP server as a secondary, the start up time of workstations will be longer. If more than one primary DHCP server is active, the server that replies faster will assign the IP configuration. Depending on the behaviour of the servers, disruptions or interferences may occur.

In contrast to a primary DHCP server, SX-GATE as secondary will not reply immediately when a device asks for an IP address. SX-GATE will only reply when a few seconds have passed and the device continues to demand the IP address. In this case SX-GATE assumes that the primary DHCP server is not available and will thus assign an IP address.



Please make sure that the IP address ranges assigned by the primary and the secondary DHCP servers do not overlap. As the primary server is not aware of the existence of a secondary, overlapping may result in a conflict.

14.3.1-B Static IPv4 addresses

Statically assigned IPv4 addresses

In this screen you can direct the DHCP server to always assign a specific IP address to a certain device. The device will be identified by the hardware address of its network adapter (MAC address). To add a static address mapping, please type the desired IP address, a name and the MAC address of the device into the respective fields. You may set the network part of the IP address to "0" to specify it in relation to the interface's primary subnet. So e.g. if the primary subnet is 192.168.0.0/24, the IP "0.0.0.200" actually means "192.168.0.200". The name is intended for your reference, so you can specify an arbitrary value. The MAC address is to be stated in hexadecimal form with the single bytes separated by colons (e.g. 0a:43:94:fc:83:0e).



If the network adapter of one of the devices listed here is replaced, the MAC address of the device will change. Adjust the corresponding entry accordingly.



The fixed addresses must not overlap with the IP ranges of dynamically assigned addresses. On the other hand each address must belong to the primary IP subnet of the selected interface.

14.3.1-C Network parameters

Most of the setting of this screen refer to SX-GATE. That's why the corresponding values are used by default. However you can alter these settings if required.

Domainname

This option determines which domainname will be assigned to DHCP clients.

Gateway (Router)

The default gateway used by DHCP clients is configured by this value.

DNS 1

The SX-GATE DHCP-Server will assign this IP address as primary name server.

DNS 2

Optionally you can enter a secondary name server. It will be considered by the clients whenever the primary DNS is not available or answers with a delay. You can specify your provider's DNS server for example, or a DNS server within your LAN.

14.3.1-D Windows parameters

The settings on this screen are useful for Microsoft Windows networks. However it is not mandatory to specify any of the values.

Web-Proxy Auto-Discovery URL

Most browsers are able to automatically detect the web proxy configuration using Web-Proxy Auto-Discovery (WPAD). The browser needs to download a config file from a web server. Publishing via DHCP is one of the methods WPAD specifies to determine the URL of this config file. Yet only Microsoft Internet Explorer supports this distribution method, provided that DHCP is enabled. An alternative DNS based solution can be enabled in menu "Modules > HTTP server". This is supported by all major browsers and does not require DHCP.

Enter the config file's URL here. The SX-GATE configuration server provides such a config file which you should use if the browsers must use SX-GATE as web proxy. However if it does not suit your needs you may as well enter the URL of your own config file.

WINS 1

Here you can specify the primary WINS server. WINS is required by Windows to resolve hostnames in multi-subnetted networks.

WINS 2

Here you can enter a secondary WINS server.

NetBIOS nodetype

Here you can determine the NetBIOS nodetype. This option controls the usage of WINS and broadcast packets by Windows clients.

14.3.1-E More parameters

NTP server 1

Enter the IP address of an NTP time server which can be used by the clients to synchronize their system time.

NTP server 2

Optionally you can enter a second NTP server.

BOOTP Server IP address

Enter the IP address of the server which offers the boot image.

BOOTP file

Enter the name of the boot image.

14.3.1-F Custom options

Custom DHCP options

To meet specific demands, you can define your own options here. Only some elementary data types are available.



To get a list of IP addresses or numbers, enter multiple values separated by comma.

14.3.1-G DHCPv4 relay

DHCP server addresses

Enter the IP addresses of the DHCP servers to relay DHCP queries to.



Please make sure that a route exists on the DHCP servers that sends packets to the client network via SX-GATE.

The relay server uses the "Link Selection" field of DHCP option 82 (Agent Information) to indicate the IP range from which the DHCP server has to pick the IP for the DHCP client. The field "Relay Agent IP" (giaddr) contains the IP of the interface the relay server uses to contact the DHCP server.



It may be necessary to configure the IP range of this SX-GATE interface in the DHCP server in addition to the IP range for the DHCP clients to enable support for this configuration in the DHCP server.

14.3.1-H Dynamic IPv6 ranges

Dynamically assigned IP range

Here you can specify the IP addresses which SX-GATE will assign to devices requesting an IP by DHCP. Please make sure that none of the addresses entered here is already statically assigned to a device in the network. This could lead to conflicts with double IP addresses.



The address range must belong to the primary IP address range of the selected interface.

The prefix may be based on a dynamic prefix SX-GATE requested from your provider. Therefore you can also select from the list of prefixes defined in menu "Definitions > IP objects" when adding a new entry. In said menu you can also add entries of type "IPv6 prefix" yourself to e.g. subdivide the prefix SX-GATE received.

Valid lifetime

Using the lease time, you can define how long an allocated address is to be reserved for a device. Select a low value if it frequently occurs that devices are linked with the LAN for a short time.

14.3.1-I Static IPv6 addresses

Statically assigned IPv6 addresses

In this screen you can direct the DHCP server to always assign a specific IPv6 address to a certain device. The device will be identified by the hardware address of its network adapter (MAC address). To add a static address mapping, please type the desired IP address, a name and the MAC address of the device into the respective fields. The name is intended for your reference, so you can specify an arbitrary value. The MAC address is to be stated in hexadecimal form with the single bytes separated by colons (e.g. 0a:43:94:fc:83:0e).



If the network adapter of one of the devices listed here is replaced, the MAC address of the device will change. Adjust the corresponding entry accordingly.

If the device is actually a router you can even assign an IPv6 prefix for distribution further downstream. SX-GATE will automatically configure the required route for the prefix.



The prefix must not overlap with other local networks. In particular the IPv6 address assigned to the router must not be part of the assigned prefix.

Both, the assigned IPv6 address and the prefix may be based on a dynamic prefix SX-GATE requested from your provider. Therefore you can also select from the list of IPv6 addresses and prefixes defined in menu "Definitions > IP objects" when adding a new entry. Please add entries of type "IPv6 address" or "IPv6 prefix" as appropriate to subdivide the prefix SX-GATE received from the provider.

14.3.1-J DHCPv6 network parameters

Most of the setting of this screen refer to SX-GATE. That's why the corresponding values are used by default. However you can alter these settings if required.

DNS 1

The SX-GATE DHCP-Server will assign this IP address as primary name server.

DNS 2

Optionally you can enter a secondary name server. It will be considered by the clients whenever the primary DNS is not available or answers with a delay. You can specify your provider's DNS server for example, or a DNS server within your LAN.

14.3.2 - Indirect subnets

Networks connected to SX-GATE via a router can also receive their IPv4 configuration from SX-GATE's DHCP server. A DHCP relay on the router is required to forward DHCP requests to SX-GATE. Add the indirectly connected networks here to configure the corresponding DHCP parameters.

A table gives you an overview of the available objects. If multiple columns are displayed you can change the sort order by clicking the column title. If there are more than 20 entries, a navigation bar will appear below the bottom right hand corner of the table.

You can switch between a grouped view or a pager. The full screen mode allows you to see all entries at the same time. Pick an entry by clicking its title in the left column. A pencil icon or a trashcan in the right column allow you to rename or delete an entry. Add new objects by clicking "New Entry" below the table on the left.

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

14.3.2-A Dynamic IPv4 ranges	418
14.3.2-B Static IPv4 addresses	419
14.3.2-C Network parameters	420
14.3.2-D Windows parameters	420
14.3.2-E More parameters	421
14.3.2-F Custom options	421

14.3.2-A Dynamic IPv4 ranges

Comment

This field can be used for documentation purposes.

Dynamically assigned IP ranges

Here you can specify the IP addresses which SX-GATE will assign to devices requesting an IP by DHCP. Please make sure that none of the addresses entered here is already statically assigned to a device in the network. This could lead to conflicts with double IP addresses.



You may set the network part of the IP addresses to "0" to specify them in relation to the subnet. So e.g. if the subnet is 192.168.0.0/24, the range "0.0.0.100-0.0.0.199" actually means "192.168.0.100-192.168.0.199".



All listed address ranges must belong to the configured subnet.

Lease time

Using the lease time, you can define how long an allocated address is to be reserved for a device. Select a low value if it frequently occurs that devices are linked with the LAN for a short time.

SX-GATE is backup DHCP server (secondary)

Activate this option if you want to use SX-GATE as secondary DHCP-server.



If you unnecessarily configure the DHCP server as a secondary, the start up time of workstations will be longer. If more than one primary DHCP server is active, the server that replies faster will assign the IP configuration. Depending on the behaviour of the servers, disruptions or interferences may occur.

In contrast to a primary DHCP server, SX-GATE as secondary will not reply immediately when a device asks for an IP address. SX-GATE will only reply when a few seconds have passed and the device continues to demand the IP address. In this case SX-GATE assumes that the primary DHCP server is not available and will thus assign an IP address.



Please make sure that the IP address ranges assigned by the primary and the secondary DHCP servers do not overlap. As the primary server is not aware of the existence of a secondary, overlapping may result in a conflict.

14.3.2-B Static IPv4 addresses

Statically assigned IPv4 addresses

In this screen you can direct the DHCP server to always assign a specific IP address to a certain device. The device will be identified by the hardware address of its network adapter (MAC address). To add a static address mapping, please type the desired IP address, a name and the MAC address of the device into the respective fields. You may set the network part of the IP address to "0" to specify it in relation to the interface's primary subnet. So e.g. if the primary subnet is 192.168.0.0/24, the IP "0.0.0.200" actually means "192.168.0.200". The name is intended for your reference, so you can specify an arbitrary value. The MAC address is to be stated in hexadecimal form with the single bytes separated by colons (e.g. 0a:43:94:fc:83:0e).



If the network adapter of one of the devices listed here is replaced, the MAC address of the device will change. Adjust the corresponding entry accordingly.



The fixed addresses must not overlap with the IP ranges of dynamically assigned addresses. On the other hand each address must belong to the primary IP subnet of the selected interface.

14.3.2-C Network parameters

Most of the setting of this screen refer to SX-GATE. That's why the corresponding values are used by default. However you can alter these settings if required.

Domainname

This option determines which domainname will be assigned to DHCP clients.

Gateway (Router)

The default gateway used by DHCP clients is configured by this value.

DNS 1

The SX-GATE DHCP-Server will assign this IP address as primary name server.

DNS 2

Optionally you can enter a secondary name server. It will be considered by the clients whenever the primary DNS is not available or answers with a delay. You can specify your provider's DNS server for example, or a DNS server within your LAN.

14.3.2-D Windows parameters

The settings on this screen are useful for Microsoft Windows networks. However it is not mandatory to specify any of the values.

Web-Proxy Auto-Discovery URL

Most browsers are able to automatically detect the web proxy configuration using Web-Proxy Auto-Discovery (WPAD). The browser needs to download a config file from a web server. Publishing via DHCP is one of the methods WPAD specifies to determine the URL of this config file. Yet only Microsoft Internet Explorer supports this distribution method, provided that DHCP is enabled. An alternative DNS based solution can be enabled in menu "Modules > HTTP server". This is supported by all major browsers and does not require DHCP.

Enter the config file's URL here. The SX-GATE configuration server provides such a config file which you should use if the browsers must use SX-GATE as web proxy.

However if it does not suit your needs you may as well enter the URL of your own config file.

WINS 1

Here you can specify the primary WINS server. WINS is required by Windows to resolve hostnames in multi-subnetted networks.

WINS 2

Here you can enter a secondary WINS server.

NetBIOS nodetype

Here you can determine the NetBIOS nodetype. This option controls the usage of WINS and broadcast packets by Windows clients.

14.3.2-E More parameters

NTP server 1

Enter the IP address of an NTP time server which can be used by the clients to synchronize their system time.

NTP server 2

Optionally you can enter a second NTP server.

BOOTP Server IP address

Enter the IP address of the server which offers the boot image.

BOOTP file

Enter the name of the boot image.

14.3.2-F Custom options

Custom DHCP options

To meet specific demands, you can define your own options here. Only some elementary data types are available.



To get a list of IP addresses or numbers, enter multiple values separated by comma.

14.4 DNS

14.4.1 Settings

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

14.4.1-A Provider DNS.....	422
14.4.1-B Client access.....	423
14.4.1-C Response policy.....	424
14.4.1-D Dynamic DNS.....	424

14.4.1-A Provider DNS

Ask the following forwarding Nameservers first

DNS queries for addresses SX-GATE cannot answer authoritatively will be forwarded to name servers in the Internet. SX-GATE should first pass the DNS query to the name servers of your provider, which can be filled in here. If multiple servers are available they will be asked in order of their speed of response.



If you do not specify any name server here, SX-GATE will always forward queries to the so-called root name servers. In this case, name resolution will usually take considerably longer.

Use specified forwarding name servers only

This option allows you to control whether SX-GATE is allowed to send queries to the Internet root name servers when the provider DNS is not available or answering with a significant delay. If SX-GATE is situated behind an upstream firewall, this behaviour is often not desired. Enable this option in this case. If no provider DNS has been specified, this option is without effect.

Obtain nameservers automatically if possible

When enabled and SX-GATE is connected to the Internet with an ADSL dial-up link or if it uses DHCP, it will obtain the DNS automatically. This applies to the default route interface only.



Automatically assigned DNS addresses have precedence over manually configured DNS. SX-GATE will fallback to the configured addresses if no dial-up DNS can be obtained.

14.4.1-B Client access

Local IP addresses

This setting affects both, the DNS forwarder function of SX-GATE (DNS proxy) and the name server feature. Forwarding DNS queries to the Internet (recursion) is restricted to local IPs, which limits the use of SX-GATE as DNS proxy to internal clients. Information from non-public DNS zones will be served only to local IP addresses.

DNSSec validation

Enable this switch and SX-GATE's DNS forwarder will validate all replies using DNSSec.



This will increase memory, CPU and network bandwidth consumption.

Deny answers with private IPs

Enable this switch to prevent DNS rebinding attacks. Forwarding of DNS answers with private IPs from the networks 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, fe80::/10 and fc00::/7 will be denied.

Log all DNS queries

With this switch you can log every request processed by the SX-GATE DNS. This can be especially useful with dial-up Internet connections to detect misconfigured computers in your LAN which repeatedly trigger an Internet connection with senseless DNS queries.



Due to the often high frequency of DNS queries, activated logging can influence the system performance. Furthermore the size of the logfiles and correspondingly the occupied harddisk usage may increase rapidly. Thus it is not recommended to activate this option permanently.

14.4.1-C Response policy

Override or block DNS replies

Here you can override or block DNS replies. The actual values you have to specify depend upon the selected type.

A/AAAA/CNAME

Depending on the type of entry in the "Target" field the name is mapped to an IPv4 address, IPv6 address or an other DNS name respectively. If you leave "Target" empty, the reply will indicate that the queried name does not exist.

To overwrite a reverse lookup (PTR), enter the IP address as "DNS name" using the ".in-addr.arpa" or ".ip6.arpa" format. As "Target" you can enter the hostname or nothing.

MX

Specifies the mail server for a domain. Enter the mail domain (the part behind the @ of an email address) in the first field. In the second field you have to specify the hostname of a mail server. The number specifies the priority. The MX entry with the lowest priority will be tried first. If the corresponding mail server is not available, the mail servers with higher priority will be used. If there are multiple MX entries with the same priority for the same domain, the client will choose a random entry. On failure it will try the next address.

NS

Defines a name server for a domain. Specify the domain in the first and the name of the DNS in the second field. If multiple entries are defined for the same domain, the client will make a random selection. If the corresponding DNS is not available, it will try the next address.

SRV

Specify the server for a specific service. The entry must begin with "_servicename._protocol" (e.g. "_sip._udp"). The corresponding value starts with the UDP or TCP port number followed by a space character and the actual server name (e.g. "5060 www.example.com").

TXT

Allows you to enter an arbitrary text.

14.4.1-D Dynamic DNS

With dynamic DNS it is possible to address a device which it is connected to the Internet with a dynamic IP address. So with dynamic DNS you can access the services offered by SX-GATE despite of its dynamic IP address. Dynamic DNS uses ordinary hostnames (fully qualified domain names, FQDN) to address a device. Dynamic DNS is offered by many different providers. Some offer this service for free, others charge for it.



It takes a few seconds or even minutes until a new IP address becomes available via dynamic DNS.

If SX-GATE gets a dynamic IP address itself (ADSL interface with dynamic IP or Ethernet interface with IP address assigned via DHCP), please configure dynamic DNS in settings of the respective interface of menu "Modules > Network > Interfaces". SX-GATE will then update its dynamic DNS record once a new dial-up connection is established or when the IP changes.

If SX-GATE is situated behind a NAT router and it's the NAT router that actually gets the dynamic IP, the NAT router must forward inbound connections to SX-GATE (DNAT, portforwarding, exposed host). You should configure dynamic DNS in the NAT router, as only the NAT router knows its current dynamic IP. Only if this is not possible you may consider to configure dynamic DNS in SX-GATE menu "Modules > DNS > Settings". SX-GATE will then try to figure out the current dynamic IP of the NAT router at regular intervals, using an Internet based service.

Protocol

Unfortunately there's no standard protocol for updating dynamic DNS records. SX-GATE offers a bunch of different protocols. Please consult your dynamic DNS provider, which protocol is used and if SX-GATE supports it.

Update server of the DNS provider

Here you have to specify the server which accepts and processes the IP address update messages. This server may be different to the webserver of the dynamic DNS provider.

Update URL

Here you have to specify the update URL (aka "direct URL") for updating the dynamic IP address. The URL may have the placeholders <host>, <ipaddr>, <username> and <password> that will be substituted by the dynamic DNS name, the IP address, the username and the password, i.e.: `http://dynupdate.exampledyndns.com/nic/update?hostname=<domain>&myip=<ipaddr>`

Dynamic DNS hostname of SX-GATE

Usually the providers allow you to manage multiple dynamic DNS names with a single user account. Therefore you have to supply SX-GATE's complete dynamic DNS name here (including the domain).

Login

No dynamic DNS updates without authentication. Please enter the login for the corresponding account here.

Password

Finally you have to specify the password for the dynamic DNS account.

URL to obtain the Internet IP

Enter the URL of an Internet service that reports the external IP (e.g. checkip.dyndns.org). SX-GATE will then enter this IP in dynamic DNS.

Time interval to check for IP change

SX-GATE will check for a changed external IP in the time interval you configure here.



While it is of course desirable to check very frequently, access to the Internet service for obtaining the external IP might be rate limited.



On a cluster only the current master node will update dynamic DNS.

Update now

Check live if DynDNS update is working.

14.4.2 Zones

A table gives you an overview of the available objects. If multiple columns are displayed you can change the sort order by clicking the column title. If there are more than 20 entries, a navigation bar will appear below the bottom right hand corner of the table. You can switch between a grouped view or a pager. The full screen mode allows you to see all entries at the same time. Pick an entry by clicking its title in the left column. A pencil icon or a trashcan in the right column allow you to rename or delete an entry. Add new objects by clicking "New Entry" below the table on the left.

Type of zone

Here you can add a new DNS zone for which SX-GATE will be the authoritative name server. DNS queries for these zones will not be forwarded to name servers in the Internet but answered by the DNS of SX-GATE.

IPv4 reverse lookup zone

Usually a reverse lookup zone is defined for complete class A, B or C networks (netmasks 255.0.0.0, 255.255.0.0 or 255.255.255.0). To specify a zone of one of these classes, please enter only the significant parts of the IP address. Some examples:

Class A: 10.0.0.0/255.0.0.0 (10.in-addr.arpa.)

Input: 10

Class B: 10.5.0.0/255.255.0.0 (5.10.in-addr.arpa.)

Input: 10.5

Class C: 10.5.0.0/255.255.255.0 (0.5.10.in-addr.arpa.)

Input: 10.5.0



If your provider made a so called "classless in-addr.arpa delegation" according to RFC 2317, you might have to enter something different here. Keep in mind, that the actual zone name differs from the name you enter here. The order of the components delimited by dots is always inverted.

IPv6 reverse lookup zone

Please enter only the significant parts of the IPv6 prefix. If the prefix doesn't end with a colon or a four-digit hexadecimal number you might have to add leading zeros (e.g. either "2001:0db8" or "2001:db8:" instead of "2001:db8").

Network: fd00::/8 (d.f.ip6.arpa.)

Input: "fd"

Network: fd00::/12 (0.d.f.ip6.arpa.)

Input: "fd0"

Network: 2001:db8::/32 (8.b.d.0.1.0.0.2.ip6.arpa.)

Input: "2001:db8:" or "2001:0db8". Entering "2001:db8" would be wrong as it refers to 2001:db80/28.

Network: 2001:db8::/64 (0.0.0.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa.)

Input: "2001:db8:0:0:" or "2001:db8:0:0000". Wrong would be e.g. "2001:db8:." (refers to 2001:db8::/112) or "2001:db8:0:0" (refers to 2001:db8::/52).

14.4.2.1 domain

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

14.4.2.1-A Entries.....	428
14.4.2.1-B SOA.....	430
14.4.2.1-C NS.....	431
14.4.2.1-D MX.....	431
14.4.2.1-E Access control.....	431
14.4.2.1-F Forwarders.....	432

Type

Please select SX-GATE's role for the DNS zone.

Master

The entries in the zone file have to be configured on SX-GATE in this case. SX-GATE is the start of authority (SOA) for this zone.

Slave

In this mode, SX-GATE mirrors the contents of a DNS zone. The contents cannot be modified on SX-GATE. To be able to perform zone transfers, the address of the master name server has to be supplied on tab "Access control".

Forward

In contrast to the previous options, SX-GATE is not authoritative for the zone but rather forwards queries to an other name server.

14.4.2.1-A Entries

Userdefined entries

Here you can define entries for the selected zone. To specify NS and MX records for the zone itself please use the tabs specifically provided for these entries.



DNS entries can be specified absolute or relative. An entry which ends with a dot is considered to be absolute (e.g. "www.example.com."). A relative entry has no trailing dot. The current zone will be appended automatically to this entry. If for instance the current zone is "example.com", you only need to enter "www" to define "www.example.com.". Entering "www.example.com" (without trailing dot) is not what you actually want, as it defines "www.example.com.example.com.".

The values you have to specify for a new entry depend upon the selected type.

A

Maps a name to an IP address. Specify the relative or absolute name in the first input field and the IP address in the second. If a name resolves to more than one IP address, the client will select a random one. On failure it will try the next address.

AAAA

Equivalent of "A", but for IPv6 addresses.

CAA

Let's you specify which CAs are authorized to issue certificates for a host or domainname. CAA records are only queried by CAs when issuing a new certificate to reduce the risk of mis-use. Enter the host or domainname in the first field and the CA domain in the second field. Ask your CA which entry it expects. Enter a semicolon instead of a CA domain to deny issuing certificates for a host or domain. To specify multiple CAs you can add multiple CAA records per host or domain.

If only the CA name or a semicolon has been specified in the second field an "issue" entry is generated which affects issuing ordinary certificates. This is equivalent to entering "issue ca.example.com" or "issue ;". To control issuing wildcard certificates, enter "issuewild" followed by a blank and the CA domain or a semicolon (e.g. "issuewild ca.example.com" or "issuewild ;"). Enter "iodef" followed by a blank and an URL to receive a report in case of a policy violation (e.g. "iodef mailto:hostmaster@example.com").

CNAME

Defines an alias for a name. Enter the alias in the first field and an existing name in the second. Both fields may contain either relative or absolute names.

MX

Specifies the mail server for a domain. Enter the mail domain (the part behind the @ of an email address) in the first field. In the second field you have to specify the hostname of a mail server. You can use absolute or relative names in both input fields. The number specifies the priority. The MX entry with the lowest priority will be tried first. If the corresponding mail server is not available, the mail servers with higher priority will be used. If there are multiple MX entries with the same priority for the same domain, the client will choose a random entry. On failure it will try the next address.

NS

Defines a name server for a domain. Specify the domain in the first and the name of the DNS in the second field. Both values may be either an absolute or a relative name. If multiple entries are defined for the same domain, the client will make a random selection. If the corresponding DNS is not available, it will try the next address.

SRV

Specify the server for a specific service. The entry must begin with "_servicename._protocol" (e.g. "_sip._udp"). The corresponding value starts with the UDP or TCP port number followed by a space character and the actual server name (e.g. "5060 www.example.com.).

TXT

Allows you to enter an arbitrary text.

The "TTL" controls how long an entry may be cached. If not specified the default value is used which can be configured on tab "SOA".

14.4.2.1-B SOA

Each DNS zone must provide a Start Of Authority record which contains administrative settings. Some of them can be configured here.

Start of authority servername

This option determines the hostname of the primary DNS for the selected zone. Usually a DNS zone is mirrored by secondary name servers. The value you configured here won't be changed on the mirrors, so it is possible to determine the primary name server which is responsible for the entries of the zone.

Start of authority email

Here you have to specify the email address of the administrative contact for the selected zone.

Incremented serial number

Every DNS zone must provide a strictly ascending serial number. With this number, secondary DNS servers decide whether the entries of a zone file have been updated and therefore a zone transfer is required. The serial number will be incremented automatically by SX-GATE after each modification. Nevertheless you can influence the serial number by specifying a value yourself.



If the local serial number is lower than on the mirrors it can cause inconsistencies. Check the serials especially after restoring a backup.

Default TTL

Configure how long entries from this zone may be cached.

14.4.2.1-C NS

Specify all authoritative primary and secondary name server for the selected zone. This will add the respective NS records to the zone file. The server names can be specified relative to the current zone (e.g. "ns") or as an absolute name. An absolute name ends with a dot (e.g. "ns.example.com.").

14.4.2.1-D MX

Specify all mail servers (mail exchanger) for the email domain which corresponds to the selected zone. This will add the respective MX records to the zone file. The server names can be specified relative to the current zone (e.g. mail) or as an absolute name. An absolute name ends with a dot (e.g. mail.example.com.).

The number specifies the priority. The MX entry with the lowest priority will be tried first. If the corresponding mail server is not available, the mail servers with higher priority will be used.

14.4.2.1-E Access control**Master**

This option is only available when SX-GATE acts as a secondary server (slave) for this zone. Please specify from which name server SX-GATE can download the zone file.

Public zone

DNS queries on this zone will always be answered if the query was sent from an internal IP address. These are defined at "Modules > DNS > Settings" on tab "Client access". If the records of the selected zone have to be available to anybody in the Internet, you have to declare the zone to be "public" by activating this switch.



To enable DNS requests from the Internet to the SX-GATE name server, you most likely have to modify the firewall policy to accept incoming packets on port 53 for the protocols UDP and TCP.

Allow zone transfer for IP

If this zone has to be mirrored by secondary name servers, you have to add their IP addresses here. SX-GATE will accept a zone transfer only if it is requested by one of the IPs listed here.

14.4.2.1-F Forwarders

Forward queries to name server

Queries to the currently selected zone will be forwarded to the name servers you enter here. This allows you to resolve individual domains via a custom DNS instead of using the ISP's DNS or the Internet root servers.



Only clients which are allowed to send recursive queries will be permitted. Please refer to "Modules > DNS > Settings", tab "Client access".

Besides adding IP addresse, you can also refer to DNS ip objects.

14.4.2.2 IPv4 reverse lookup zone

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

14.4.2.2-A Entries.....	433
14.4.2.2-B SOA.....	434
14.4.2.2-C NS.....	435
14.4.2.2-D Access control.....	435
14.4.2.2-E Forwarders.....	435

Type

Please select SX-GATE's role for the DNS zone.

Master

The entries in the zone file have to be configured on SX-GATE in this case. SX-GATE is the start of authority (SOA) for this zone.

Slave

In this mode, SX-GATE mirrors the contents of a DNS zone. The contents cannot be modified on SX-GATE. To be able to perform zone transfers, the address of the master name server has to be supplied on tab "Access control".

Forward

In contrast to the previous options, SX-GATE is not authoritative for the zone but rather forwards queries to an other name server.

14.4.2.2-A Entries

Userdefined entries

Here you can define entries for the selected zone. To specify NS records for the zone itself please use the tab specifically provided for these entries.

The values you have to specify for a new entry depend upon the selected type.

PTR

Maps an IP address to a name.

In the first field you have to supply the numbers missing in the zone name to form a complete IP address. If you have to specify more than one number, you have to enter them in reverse order. If for example you want to define a PTR record for the address "172.16.5.10" in the zone file "172.16", you have to enter "10.5". Due to the relative addressing (no trailing dot) this value will automatically expand to "10.5.16.172.in-addr.arpa.".

The second field will take the hostname which corresponds to this address.

NS

Defines a name server for a reverse lookup zone.

In the first field you have to fill in the zone for which you want to add a NS record. Enter the name relative to the currently selected zone. If you have to specify more than one number, keep in mind that you have to enter them in reversed order. If for example you want to define a nameserver for "10.16.5" in zone "10", you have to type "5.16", as in fact you want to define "5.16.10.in-addr.arpa.". Due to the relative addressing (no trailing dot with "5.16") the entry will automatically expand to "5.16.10.in-addr.arpa.".

The second field will take the hostname of the name server. If multiple entries are defined for the same domain, the client will make a random selection. If the corresponding DNS is not available, it will try the next address.

The "TTL" controls how long an entry may be cached. If not specified the default value is used which can be configured on tab "SOA".

Automatically add missing PTR entries

All addresses which have not been mapped to hostnames by manually specifying a PTR record can be supplemented automatically.



This feature is not available for class A zones.

using hostname

This option will determine the hostname of the automatically added entries. For a class C network, the last number of the respective IP address will be added to the value specified here. For a class B network an additional dash and the last but one number of the IP will be appended.

and domain

Finally this control allows you to determine the domain which will be appended automatically to the generated hostnames.

14.4.2.2-B SOA

Each DNS zone must provide a Start Of Authority record which contains administrative settings. Some of them can be configured here.

Start of authority servername

This option determines the hostname of the primary DNS for the selected zone. Usually a DNS zone is mirrored by secondary name servers. The value you configured here won't be changed on the mirrors, so it is possible to determine the primary name server which is responsible for the entries of the zone.

Start of authority email

Here you have to specify the email address of the administrative contact for the selected zone.

Incremented serial number

Every DNS zone must provide a strictly ascending serial number. With this number, secondary DNS servers decide whether the entries of a zone file have been updated and therefore a zone transfer is required. The serial number will be incremented automatically by SX-GATE after each modification. Nevertheless you can influence the serial number by specifying a value yourself.



If the local serial number is lower than on the mirrors it can cause inconsistencies. Check the serials especially after restoring a backup.

Default TTL

Configure how long entries from this zone may be cached.

14.4.2.2-C NS

Specify all authoritative primary and secondary name server for the selected zone. This will add the respective NS records to the zone file. Use the absolute addressing scheme with a trailing dot (e.g. "ns.example.com.").

14.4.2.2-D Access control**Master**

This option is only available when SX-GATE acts as a secondary server (slave) for this zone. Please specify from which name server SX-GATE can download the zone file.

Public zone

DNS queries on this zone will always be answered if the query was sent from an internal IP address. These are defined at "Modules > DNS > Settings" on tab "Client access". If the records of the selected zone have to be available to anybody in the Internet, you have to declare the zone to be "public" by activating this switch.



To enable DNS requests from the Internet to the SX-GATE name server, you most likely have to modify the firewall policy to accept incoming packets on port 53 for the protocols UDP and TCP.

Allow zone transfer for IP

If this zone has to be mirrored by secondary name servers, you have to add their IP addresses here. SX-GATE will accept a zone transfer only if it is requested by one of the IPs listed here.

14.4.2.2-E Forwarders**Forward queries to name server**

Queries to the currently selected zone will be forwarded to the name servers you enter here. This allows you to resolve individual address ranges via a custom DNS instead of using the ISP's DNS or the Internet root servers.



Only clients which are allowed to send recursive queries will be permitted. Please refer to "Modules > DNS > Settings", tab "Client access".

Besides adding IP addresses, you can also refer to DNS IP objects.

14.4.2.3 IPv6 reverse lookup zone

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

14.4.2.3-A Entries.....	436
14.4.2.3-B SOA.....	437
14.4.2.3-C NS.....	438
14.4.2.3-D Access control.....	438
14.4.2.3-E Forwarders.....	439

Type

Please select SX-GATE's role for the DNS zone.

Master

The entries in the zone file have to be configured on SX-GATE in this case. SX-GATE is the start of authority (SOA) for this zone.

Slave

In this mode, SX-GATE mirrors the contents of a DNS zone. The contents cannot be modified on SX-GATE. To be able to perform zone transfers, the address of the master name server has to be supplied on tab "Access control".

Forward

In contrast to the previous options, SX-GATE is not authoritative for the zone but rather forwards queries to another name server.

14.4.2.3-A Entries

Userdefined entries

Here you can define entries for the selected zone. To specify NS records for the zone itself please use the tab specifically provided for these entries.

The values you have to specify for a new entry depend upon the selected type.

PTR

Maps an IP address to a name.

In the first field you have to supply the numbers missing in the zone name to form a complete IP address. You can either use normal IPv6 address syntax or you have to use the PTR record syntax (reverse order of digit, separated by dots). If for example you want to define a PTR record in zone 2001:db8:0:0: for the address 2001:db8::1, you could take on of the following entries: ":1", "0:0:0:1" or "1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0".

The second field will take the hostname which corresponds to this address.

NS

Defines a name server for a reverse lookup zone.

In the first field you have to fill in the zone for which you want to add a NS record. Enter the name relative to the currently selected zone. If you have to specify more than one number, keep in mind that you have to enter them in reversed order, separated by dots. If for example you want to delegate a nameserver for "2001:db8:0:1::/64" in zone 2001:db8:0:, you have to type "1.0.0.0", as in fact you want to delegate "1.0.0.0.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa.". Due to the relative addressing (no trailing dot with "1.0.0.0") the current zone (0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa.) is appended automatically.

The second field will take the hostname of the name server. If multiple entries are defined for the same domain, the client will make a random selection. If the corresponding DNS is not available, it will try the next address.

The "TTL" controls how long an entry may be cached. If not specified the default value is used which can be configured on tab "SOA".

14.4.2.3-B SOA

Each DNS zone must provide a Start Of Authority record which contains administrative settings. Some of them can be configured here.

Start of authority servername

This option determines the hostname of the primary DNS for the selected zone. Usually a DNS zone is mirrored by secondary name servers. The value you configured here won't be changed on the mirrors, so it is possible to determine the primary name server which is responsible for the entries of the zone.

Start of authority email

Here you have to specify the email address of the administrative contact for the selected zone.

Incremented serial number

Every DNS zone must provide a strictly ascending serial number. With this number, secondary DNS servers decide whether the entries of a zone file have been updated

and therefore a zone transfer is required. The serial number will be incremented automatically by SX-GATE after each modification. Nevertheless you can influence the serial number by specifying a value yourself.



If the local serial number is lower than on the mirrors it can cause inconsistencies. Check the serials especially after restoring a backup.

Default TTL

Configure how long entries from this zone may be cached.

14.4.2.3-C NS

Specify all authoritative primary and secondary name server for the selected zone. This will add the respective NS records to the zone file. Use the absolute addressing scheme with a trailing dot (e.g. "ns.example.com.").

14.4.2.3-D Access control

Master

This option is only available when SX-GATE acts as a secondary server (slave) for this zone. Please specify from which name server SX-GATE can download the zone file.

Public zone

DNS queries on this zone will always be answered if the query was sent from an internal IP address. These are defined at "Modules > DNS > Settings" on tab "Client access". If the records of the selected zone have to be available to anybody in the Internet, you have to declare the zone to be "public" by activating this switch.



To enable DNS requests from the Internet to the SX-GATE name server, you most likely have to modify the firewall policy to accept incoming packets on port 53 for the protocols UDP and TCP.

Allow zone transfer for IP

If this zone has to be mirrored by secondary name servers, you have to add their IP addresses here. SX-GATE will accept a zone transfer only if it is requested by one of the IPs listed here.

14.4.2.3-E Forwarders

Forward queries to name server

Queries to the currently selected zone will be forwarded to the name servers you enter here. This allows you to resolve individual address ranges via a custom DNS instead of using the ISP's DNS or the Internet root servers.



Only clients which are allowed to send recursive queries will be permitted. Please refer to "Modules > DNS > Settings", tab "Client access".

Besides adding IP addresses, you can also refer to DNS ip objects.

14.5 Mail Server

14.5.1 POP/IMAP server

SX-GATE offers a mailbox to every member of group "system-mail". To have mails delivered into a SX-GATE mailbox, at least one domain with "Deliver to SX-GATE mailbox" must be configured.

This service provides access to SX-GATE's mail accounts with POP3 and IMAP4. While POP3 provides access to the inbox only, IMAP4 offers much more features like e.g. managing your mail in folders on the server.



You can also use the SX-GATE groupware to access mailboxes, provided the groupware extension is installed.

POP3 (port 110)

Access to the inbox is not encrypted from the beginning. However if the mail client supports the appropriate protocol extensions, an encrypted connection can be negotiated.

POP3 encrypted (port 995)

Inbox access is encrypted from the beginning.

IMAP4 (Port 143)

Connections to this service are not encrypted from the beginning. However if the mail client supports the appropriate protocol extensions, an encrypted connection can be negotiated.

IMAP4 encrypted (port 993)

Here the connection is encrypted from the beginning.

Enforce encryption

Enable this option to require an upgrade to an encrypted connecting when using the unencrypted ports 110 or 143. Clients refusing to encrypt will be rejected.

TLS protocol

Select the encryption strength.



The actual encryption parameters associated with each option are updated from time to time.

outdated

For compatibility with older devices, AES ciphers using the discouraged Cipher Block Chaining (CBC) and the obsolete hash SHA1 will be enabled when selecting this option. The minimum TLS version is 1.0.

compatibel

Select this option for wide compatibility with older client systems. This will enable the obsolete hash SHA1. The minimum TLS version is 1.2.

contemporary

Only halfway recent client systems will be supported when selecting this option. At least TLS 1.2 is required. It is a good choice for security.

maximum

Requires TLS 1.3. Make sure that all clients support TLS 1.3 before selecting this option.

Local email mailboxes can be scanned for viruses on a regular basis. In this way, viruses that were not detected by antivirus signatures when the email arrived can be found.



A functional virusscanner must be installed on SX-GATE if you want to use this feature. The virus scanner licenses are not included with SX-GATE and must be purchased separately. Further information about supported or already installed scanners can be found in the menu "Modules > Virusscanner". The installation of a virusscanner also has to be made there.

14.5.2 SMTP settings

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

14.5.2-A Provider relay.....	442
14.5.2-B Delivery parameters.....	446
14.5.2-C PGP / SMIME.....	448
14.5.2-D Relay control.....	448
14.5.2-E Receiving filters.....	450
14.5.2-F Resource limits.....	453
14.5.2-G Archiving / Milter.....	455

14.5.2-A Provider relay

SMTP Relay Server for outgoing emails

With this control you determine how outgoing emails will be forwarded. SX-GATE can deliver directly to the recipient's mail server. The address of this mail server is determined by DNS. If you specify the name or IP of a mail relay server (smarthost) here, outgoing emails will always be forwarded to this server. The relay server is responsible for further delivery.



This setting will not affect emails addressed to domains which SX-GATE delivers to local mailboxes or forwards to specific (internal) mail servers.

Using a relay server is recommended if you are connected to the Internet via a dial-up link. If the direct connection to the recipient's mail server is rather bad, the relay server has to retry the delivery, so the dial-up link won't be stressed unnecessarily. Furthermore some mail servers won't accept emails sent from a dynamic IP address.

Relay Server port

If the relay server doesn't accept connections on standard port 25, you can fill in the required port here (usually 465 or 587).

Protocol

There's no need to change this setting unless the relay server requires SMTPS on a non-standard port, i.e. not on port 465.

Authenticationmethod

The SMTP auth credentials can be transmitted using different methods. Use this control to force one of them. If SX-GATE may choose one of the methods, it will prefer the MD5 based algorithms as the password won't be send in clear.



Not every relay server supports all of these methods. If you force the usage of a method which is not supported by the relay, SX-GATE will not be able to authenticate itself. The relay server might then refuse delivery of emails.

Microsoft 365 OAUTH2

For sending outbound emails via a Microsoft 365 account using the OAuth2 authentication scheme, SX-GATE uses the "client credentials flow". You need to create an application with an application password for SX-GATE in Entra ID (formerly Azure Active Directory). SMTP Authentication permission has to be granted to the application. SX-GATE uses a single user account for sending mails, so all senders have to grant "SendAs" permission to this user. With its application ID and password, SX-GATE will then be able to get a short-lived access token, which in turn allows sending mails via the configured user account.

The steps in detail:

Register application

Login to Microsoft Azure with an administrator account (<https://portal.azure.com>).

Select "Microsoft Entra ID", then "Manage > App registrations".

Click "New registration" and assign a name of your choice. Leave the other settings unchanged and click "Register".

In the menu on the left, click "Certificates & secrets" and then "Client secrets". Issue a new application password by clicking "New client secret" and "Add".

Copy the generated password in column "Value" immediately by clicking the copy icon behind the password. It will no longer be possible to copy the password at a later point in time. Paste the password into the SX-GATE mail server's oauth2 configuration or temporarily store it in a safe place to paste it later into SX-GATE.

Now click "Manage > API permissions" in the menu on the left, then "Add a permission". Select "APIs my organization uses" and type "Office" into the search field. Select "Office 365 Exchange Online" and click "Application permissions". Open the section "SMTP" and check "SMTP.SendAsApp". Close the window with "Add permissions". Finally click "Grant admin consent for DOMAINNAME".

Now click "Overview" in the menu on the left and copy the values "Application (client) ID" and "Directory (tenant) ID" into the oauth2 configuration of the SX-GATE mail server or store the values to configure SX-GATE later.

Leave the App registration by clicking "Home" in the upper left corner.

Select "Microsoft Entra ID" again, but this time choose "Manage > Enterprise Applications". Copy the "Object ID" of the application you just registered for later use. The "Application ID" is also displayed here again. You will need both values in a moment when configuring Exchange.

Grant access in Exchange

SX-GATE uses just one single account for sending mails. After you decided, which account to use, you should check in "Microsoft 365 admin center" (<https://admin.microsoft.com>), if "Authenticated SMTP" has been granted for this account. Click on the account below "Users > Active Users", then "Mail" and check the permissions below "Email apps".

Now step through all other users and groups and grant "SendAs" permission for the account used to send mails.

Configure credentials in SX-GATE

If you haven't done so already, paste the values you copied earlier into the OAuth2 configuration of the SX-GATE mail client.

Enter the account you picked for sending mails as "SMTP-Auth login". It is not necessary to enter the corresponding password, as SX-GATE can login with its application password.

SMTP-Auth login

If authentication with SMTP-Auth is required for using the relay server of your provider, you can provide the username and password in the corresponding input fields. If you leave these fields blank, authentication is disabled.



SMTP-Auth relates to outgoing mails and has nothing to do with the user login that is required to retrieve mails from your provider's POP3 server. If SMTP-Auth is really required by the mail relay, the credentials can however be identical to those used for the POP3 server.



According to the standard, SMTP-Auth is a "hop-to-hop" authentication. Thus it involves only the two systems directly connected. In this case the relay server asks the SX-GATE mail server to authenticate itself and not e.g. the user who wrote the email. Therefore SX-GATE usually uses one specific login for SMTP-Auth. Different credentials depending on the sender of the mail are possible, but may be subject to limitations (see "Authentication by email address of sender" below).

As a rule, a mail relay server will insist on authentication, if it is not operated by your Internet access provider. In this case we recommend that you insert the relay server of the ISP over which you are connected to the Internet.



It is recommended to use the mail relay server offered by your Internet access provider. Usually authentication is not required in this case. In addition, the email transfer to the relay server is not affected by bottlenecks within the Internet. So delivery is generally faster.

Tenant

Enter your Entra ID tenant name or ID.

OAuth2 client ID

Enter the client ID you have registered in Entra ID for the SX-GATE mail server.

Secret OAuth2 client key

Enter the application password you have generated in the Azure Active Directory for the SX-GATE mail server.



The Azure AD application password has a limited validity period. Please remember to issue a new application password in time and copy it to SX-GATE.

Authentication with Certificate

Alternatively or in addition to password authentication, SX-GATE can identify itself to other mail servers with a client certificate if the connection is encrypted.

Select one of the keys managed in menu System > Certificate manager > Keyring".

Authentication by email address of sender

If the provider insists that the credentials used for authenticating an outbound mails must match the sender address, you can enter credentials by sender address here. The sender address is the so-called "Envelope From" as shown in the SX-GATE maillog.



In some situations (e.g. undeliverable mail) or by some features (e.g. out-of-office replay) mails with an empty sender address are sent (the so-called SMTP null reverse-path). The provider relay might refuse to accept these mails and they are either silently discarded or trigger a notification mail to the local administrator. If this is the case, please switch zu direct delivery of outbound mails or change to a provider offering a full-featured SMTP relay.

14.5.2-B Delivery parameters

Forward outgoing emails

Outgoing emails can be forwarded immediately or they can be added to a queue first. In this case the mails will be sent all together the next time the queue is processed. This is particularly useful with dial-up Internet connections to save connection fees.

Process send queue every

This and the following option control, when emails waiting in the SX-GATE mail queue will be processed. An email is queued if the previous attempt to deliver the mail failed or if deferred delivery has been configured.



At least one of the two options must be enabled and functional. Otherwise emails will be queued forever.

The mail queue will be processed by the mail server in the interval configured here. So this value specifies the minimum period of time a mail will wait in the queue until the next attempt to deliver it is made.

Process send queue on Internet dial-in

Activate this option if SX-GATE is directly connected to the Internet using an ADSL dial-up link. Each time a new dial-up connection is established, an attempt is made to deliver the emails waiting in the queue.



If SX-GATE has no direct PPP dial-up Internet connection, this option is without effect.

Notify sender, if mail cannot be delivered within

If the mail server cannot deliver an email while processing the queue and this email has been waiting in the queue longer than the period of time configured here, the sender will be notified. The notification will be sent only once per email.



Notifications will be sent while processing the send queue. So the actual period of time until such a notification is delivered may be longer than the period you configured here. Please coordinate this option with the time interval specified for processing the queue.

Return mail as undeliverable, if mail cannot be sent within

This option is quite similar to the previous one. However an email will be returned to the sender as undeliverable, if it was queued longer than configured here and SX-GATE is still not able to forward it. Also this time limit will only be checked while processing the queue.



The actual period of time until a non delivery report is sent may differ from the configured value. See the previous option for details.

HELO/EHLO name

Configure which hostname SX-GATE uses with the HELO/EHLO command when sending an email. Either use a static name or let SX-GATE dynamically pick a name by DNS reverse lookup on the outbound connection's source IP.



In case of dynamic lookup SX-GATE will always use its hostname as configured in System > Setup for connections via device eth0.

Sender for SX-GATE mails

SX-GATE generates emails like e.g. status reports or notifications. With this control you can configure the sender address that SX-GATE will use for these mails. Enter either a full email address or just a domain. If you enter a domain, the part before the @ sign is unchanged (usually "root").

14.5.2-C PGP / SMIME

The PGP/SMIME filter helps to enforce that emails to certain recipients have to be encrypted. If a user forgets to encrypt a mail, SX-GATE will refuse to accept it. Mails must be at least partially encrypted, using PGP (GPG) or S/MIME. As an exception, emails with an empty sender address as often used in e.g. error notifications, delivery status notification and out-of-office replies will always be accepted.



Only outbound emails will be tested.

PGP / SMIME filter

This switch enables or disables the filter.

Block unencrypted mails sent to mail address and domains

Email to recipients listed here must always be encrypted. You can enter individual recipient addresses or complete mail domains (e.g. "user@example.com" or "example.com").

14.5.2-D Relay control

It is crucial that only internal IP addresses are allowed to send mails to the Internet, unless authorized by e.g. authentication. Otherwise SX-GATE will likely be abused as an "open relay server" by SPAM mail senders.



Independent of the source IP it is always possible to send emails to addresses within the local recipient domains. This includes both, domains delivered to SX-GATE mailboxes and domains forwarded to specific (internal) mails servers. Also Authentication is never required in these cases.

Local IP addresses

With this control you can define which IP addresses are considered to be "local". Unless restricted by other options, only the addresses included here will be able to relay mails to the Internet offhand.



You should never grant this right to any IP.



The SX-GATE groupware, if installed, has its own IP address which is always treated as a "local" IP, even if it is not listed here.

You can also use this feature to allow Internet mails only for some systems while all others may only send internal mails. Here, the IP address of the system which sends the mail to SX-GATE is decisive. The following options allow you to allow Internet mail per user.

SMTP-Auth required for local users

If this switch is active, SX-GATE will not relay emails to the Internet, if the mail was sent from a local IP address without authentication. Local IP addresses are those listed at "Local IP addresses" above.



The switch also enables SMTP authentication in the SX-GATE Groupware, if it is installed.

Use this feature to allow the delivery of emails to the Internet only for specific local users. You can give the SMTP-Auth privilege to groups at "System > User administration > Groups".

Always propose SMTP-Auth

When enabled, both, external and internal clients can authenticate themselves. Usually external clients are not allowed to relay emails to the Internet via the SX-GATE mail server. Activate this switch to allow it for certain users after successful authentication. As described in the previous option, the group administration determines, which users are actually authorized. Internal users might have to authenticate themselves when outbound emails are to be signed by the "S/MIME gateway" module.

Mail clients should use the submission ports 465 or 587 to submit mails to the SMTP server. In this case it is sufficient to enable authentication on the submission ports only. If the submission ports are not reachable from the Internet, this would even increase the overall security, as user credentials cannot be probed in this case.

on submission ports only

Enable this option if authentication should only be possible on the submission ports 465 and 587.

also on Port 25

Enable this option if authentication should also be possible on port 25.

Accept only encrypted user authentication

Activate this switch if SMTP-Auth passwords should never be transmitted in clear. In this case, the SMTP-Auth methods PLAIN and LOGIN can only be used if the SMTP connection itself is TLS encrypted.



SMTP-Auth is affected in both directions. For outgoing connections (provider relay server requires authentication) as well as for incoming connections (mail relay to Internet only for authenticated clients).

Submission port 465 (SMTPS)

Enables submission port 465. Connections to this port are always encrypted

Submission port 587

Enables submission port 587. Connections to this port are initially unencrypted. If the SX-GATE configuration permits, the connection can be upgraded to an encrypted connection upon request of the client (STARTTLS).

14.5.2-E Receiving filters***Suppress disposition notifications***

Whenever a user opens an email requesting a return receipt in form of a Message Disposition Notification (MDN), the mail program will usually ask for the user's confirmation to send it. If the user agrees, the mail program will return an email indicating that the mail has been opened to the sender. Most mail programs can be configured to always ignore or always send disposition notifications.

Enable this options and SX-GATE will remove those headers from inbound mail, requesting for an MDN. So an administrator can suppress MDNs regardless of the actual settings in the users' email programs.



This option does not affect Delivery Status Notifications (DSNs).

Tag mails received from external

The email sender as displayed to the user ("From" and "Sender" header) can be forged easily. Some users could be fooled by an email using e.g. the sender address of the manager. With this option enabled, the subject of emails received from an external sender can be tagged. Authenticated connections and connections from IPs listed

below "Local IP addresses" in menu "Modules > Mail Server > SMTP settings" on tab "Relay control" do not count as external.

if faking sender from local domain

Use this setting to tag the email subject only if one of the local domains is found in the sender address. The text "*****FAKE***** [Sender]" will be put in front of the subject.



If a local user sends an email to a mailinglist, the returned email is expected to be tagged wrongfully.



Enable this option only if all emails with local sender domains are always sent to the Internet via local systems (SX-GATE or internal mailserver).

Verify internal addresses in advance

When this option is enabled, SX-GATE will contact the internal mail server for every email it receives to verify if it is willing to accept a message for the given recipients. This is checked before the actual message body is transmitted to SX-GATE, so mails to non-existent recipients will be rejected before wasting bandwidth.



This feature applies to all recipient domains SX-GATE forwards to an internal mail server.



Address verification also applies to mails SX-GATE retrieves from a POP or IMAP server. If the internal mail server refuses delivery, the mail is usually silently discarded.

using SMTP

This is the most simple approach which works with almost all mail servers. For each inbound mail SX-GATE opens an SMTP connection to the internal mail server and The received sender and recipient addresses are forwarded to it. Depending on the replies of the internal mail server, the sender is then either allowed to continue with the transmission of the email or the mail is rejected.



With this method you can even make use of any capability your internal mail server offers to reject sender addresses.



Make sure that the internal mail server immediately rejects unknown recipient addresses. The following paragraph describes how to enable this in Microsoft Exchange.

In Microsoft Exchange you will have to enable recipient filtering first. Install the Antispam Agents by searching and starting the script "Install-AntispamAgents" that you will find in a subfolder below the Exchange program folder. Since Exchange 2013 an additional HubTransport connector of type "Internet" is also required. Configure the connector to grant anonymous access. We recommend to allow access from SX-GATE's IP only. If the Windows firewall is enabled, you will also have to add a rule there to grant access to the new connector. Finally enter the port number of the new connector on SX-GATE as "SMTP port for verification".

using LDAP (Active Directory)

The requested recipient addresses will be looked up in an Active Directory (attribute "proxyAddresses"). The necessary parameters for LDAP access have to be configured in menu "System > User administration > Settings".

Accept mail if verification is not possible

With this option disabled, SX-GATE reports a temporary SMTP failure if the verification is not possible as the required service is unavailable. When using SMTP to verify the address, temporary failures reported by the internal server (e.g. due to insufficient storage space) are simply forwarded. So in both cases the mail will remain on the sending system, which will usually retry delivery later. SX-GATE will accept the mail only after it successfully verified it with the internal mail server.

Enable this option and SX-GATE will accept the mail without verification in both situations. SX-GATE will queue the mail if the internal mail server is unreachable. SX-GATE will return the mail to its sender if the internal mail server refuses to accept it (e.g. due to an invalid recipient address) or the queue time limit has expired (setting "Return mail as undeliverable, if mail cannot be sent within" on tab "Delivery parameters").

SMTP port for verification

Address verification can use a different port than the actual mail delivery.

Test LDAP connection

With this button you can test if email addresses can be found in Active Directory.

Emails to unknown local recipients

If a mail is addressed to a local domain, but there is no corresponding user or group, SX-GATE can refuse the delivery. The system which tried to deliver the mail is responsible to notify the sender in this case. Alternatively you can deliver mail to unknown recipients to a specific local user mailbox or distributor (group). You can not enter a complete mail address (with "@" and domain) in this case. Please specify the username (login) or the name of the group instead.



You cannot refuse the delivery of emails which have been retrieved from a POP server by SX-GATE's mail client. Emails will be delivered to the administrator if you select this option anyway.

Block mails sent from mail address, mail domains or IP address

SX-GATE will refuse to accept emails from addresses listed here. It is possible to specify the following types of entries:

A complete email address (e.g. spam@example.com)

Emails from this sender will be rejected. Note that the so called "envelope from" will be compared here and not the from header which is usually displayed by mail client programs.

A Domain (e.g. example.com)

In this case SX-GATE won't accept emails from any sender within this domain and subdomains. For example emails from spam@example.com and info@www.example.com would be denied.

Besides checking the email address, SX-GATE will lookup the IP address of the SMTP connections source in the DNS. If the hostname is within the blocked domain, the mail won't be accepted either. Let's assume the connection source is the IP 169.254.254.20 and DNS reveals that this IP corresponds to the hostname 254-20.ppp-pool.example.com. In this case the mail would be blocked as well.

An IP address

Emails will be blocked if the source IP of the SMTP connection is listed here.



In the maillog of SX-GATE the "envelop from" and the source IP of every email is logged. Search in the log for the line which contains the source information of an email ("from="). "from=" provides the "envelope from" and the source IP of the SMTP connection is listed as "relay=".



For emails which have been retrieved from a POP server by the SX-GATE mail client, the source IP of the connection is always SX-GATE itself (127.0.0.1, localhost). Therefore you can only deny emails based on the "envelope from".

14.5.2-F Resource limits

On this tab you can configure various limits which help to protect SX-GATE and downstream systems from being overloaded. The restrictions apply to all SMTP

connections accepted by SX-GATE. It does not matter if a mail client program or an other mail server establishes the connection. Usually all restrictions apply already before the actual email contents are transmitted.

Maximum number of concurrent connections

This setting limits the total number of incoming connections. This includes connections from internal LAN workstations as well as connections originating somewhere in the Internet. The limit is meant to protect SX-GATE from overload conditions.

Maximum number of concurrent connections per IP

With this option you can limit the number of simultaneous connections per source IP. It keeps individual servers from overloading the SX-GATE mail server.

In contrast to the previous option, only connections from external addresses will be monitored. So this setting won't have any effect if e.g. SX-GATE polls a POP server for emails. This option requires SX-GATE to receives emails directly per SMTP.



External addresses are all IPs which are not listed below "Local IP addresses" on tab "Relay control".

Maximum number of connections per IP and minute

Just like the previous setting, also this option limits the number of connections per source IP, but this time the total number of connections per minute. Again only external senders are affected.

Maximum number of recipients per message

When this limit is reached, SX-GATE will reject every additional recipient, indicating a transient error. A new delivery attempt has to be started for the remaining recipients.

Maximum permitted size of an email

The SMTP protocol was not designed for the transmission of lots of megabytes of data. Therefore many mail servers will only accept mails up to a certain size or will terminate the transfer after a certain period of time. Thus it is highly recommend that also the SX-GATE SMTP mail server imposes a reasonable upper limit for the size of emails.

Maximum permitted size of email headers

If emails are rejected due to oversized headers, you can adjust the acceptable size here.

14.5.2-G Archiving / Milter

The milter interface allows SX-GATE to connect with an external, milter-enabled email filtering product via network. In particular the milter interface is the best way to integrate an email archiving solution.

If no such product is available, SX-GATE could automatically deliver a copy of each mail to an additional recipient. It makes no difference if this recipient is a SX-GATE mailbox, an address on an internal mailserver or even in the Internet. The archive feature can be configured independently for inbound and outbound emails.



If a SX-GATE mailbox is used to receive a copy of every mail it must be flushed regularly. SX-GATE's POP3/IMAP4 server is not designed to be used as a long-term archive system.



Please obey the data protection and privacy acts. Enabling this feature could be subject to legal constraints or might even be prohibited by law.

Archive recipient for outbound mails

Fill in the email address which will receive a copy of every outbound email.



The sender's IP address is considered to distinguish between inbound and outbound emails. To be outbound, the origin must be an internal IP as configured on tab "Relay control". Authenticated emails are always outbound.

Archive recipient for inbound mails

Fill in the email address which will receive a copy of every inbound email. You may use the same address as for outbound email.



The recipient will be added after the mail passed the virusscan module. Hence infected emails won't be included in the archive. Both, the attachment and the relay SPAM filter might modify the original mail before it is forwarded to the archive recipient. If the relay SPAM filter decides to discard the mail, the archive recipient won't receive a copy.

External milter

You can make SX-GATE contact an external milter while processing mail. Select the stage of processing which suits best to the purpose of the filter.

Address of Milter

Enter the hostname or IP address of the external Milter.

Port of the Milter application

The milter's TCP port goes in here.

14.5.3 SPAM/Virus/Malware

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

14.5.3-A Sanity checks.....	456
14.5.3-B Greylisting.....	459
14.5.3-C SPF/DMARC filter.....	464
14.5.3-D Virusscan.....	466
14.5.3-E MIME filter.....	466
14.5.3-F MIME filter rules.....	470
14.5.3-G MIME filter options.....	472
14.5.3-H Relay SPAM filter.....	474
14.5.3-I SPAM scores.....	477
14.5.3-J SPAM modules.....	478
14.5.3-K SPAM settings.....	481

14.5.3-A Sanity checks

The check you can control on this tab are meant to relieve the malware and SPAM filters by rejecting some unwanted contents beforehand. The tests apply to all SMTP connections accepted by SX-GATE. It does not matter if a mail client program or an other mail server establishes the connection. An email which violates one of these checks will already be rejected before the actual payload is being transmitted.

Protection against automated mailers

Many SPAM and virus mails are distributed by rather simple routines, trying to deliver as many emails as possible in a very short time. This protective function makes use of this fact. Normally a mail server sends a greeting message as soon as a new connection has been established. The peer waits for the greeting and sends back a greeting message.

When enabling this feature, SX-GATE sends its greeting with a very short delay. If the client didn't wait for it, but started to send a batch of commands immediately, the connection is rejected.



This feature will affect connections from external addresses only. External addresses are all IPs which are not listed below "Local IP addresses" in menu "Modules > Mail Server > SMTP settings" on tab "Relay control". So SX-GATE needs to receive emails directly per SMTP. There won't be any effect if emails are retrieved from a POP server.



This feature may also affect regular emails.

Check HELO/EHLO

This option enables a sanity check on the hostname part of the welcome message, presented by the sending system. The hostname must include at least one dot and may not be equal to SX-GATE's hostname. Otherwise the mail will be rejected.



This check is not performed for authenticated connections and connections from IPs listed below "Local IP addresses" in menu "Modules > Mail Server > SMTP settings" on tab "Relay control". Also emails retrieved from a POP server are not affected.

Check reverse DNS

Enable this option to test the DNS information provided for the source IPs of incoming connections. Often home PCs are abused for SPAM delivery. Many of these fail to pass the reverse DNS check.



Neither authenticated nor local connections will be affected by this check. Mails retrieved from a POP3 server won't be tested either.

for existence

Select this mode to reject emails if no reverse DNS entry exists.

forward confirmed

A reverse DNS entry must exist here, too, but in addition it must be forward-confirmed. That is, the hostname returned from the reverse lookup is resolved

back to an IP by an other DNS query. If this IP differs from the original IP, the mail is rejected.



This feature sets high expectations in terms of DNS configuration. Regular emails may be affected in individual cases.

Check sender domain

With this option you activate a verification of the domain part of the sender address for each incoming mail.



This feature might also affect legitimate emails which by mistake use a misconfigured sender address. This sometimes occurs with computer generated emails of badly configured online registrations or shopping systems.

for existence

An email won't be accepted if its sender domain doesn't exist in DNS.

for valid mailserver

In this mode SX-GATE additionally determines the IP address of the mail server for this domain. In case it is invalid, delivery is refused. The test is not performed on connections from internal source IPs.

If DNS reports a permanent error when resolving the sender domain (e.g. domain does not exist), SX-GATE's mail server will refuse delivery. The sender which may be a user's mail client program or an other mail server is in charge of dealing with the error.



If it's the SX-GATE mail client which tried to deliver a mail retrieved from a POP server, the mail will be discarded without notice. As the sender domain is invalid, returning an error to the sender makes no sense. Delivery to the local administrator contradicts the purpose of defeating SPAM.

However DNS might also report a temporary problem resolving the sender domain (e.g. name server unreachable). There are two different behaviours, depending on whether the SX-GATE mail client has been enabled in the configuration or not. If it is not used, the SX-GATE mail server will refuse delivery with a temporary error. Depending on its configuration, the sending mail server might retry delivery later before notifying the sender. If the DNS problem has been solved in the meantime, the mail will be accepted. If in contrast the SX-GATE mail client is enabled, emails will be accepted despite of

temporary DNS errors. This keeps the SX-GATE mail client from retrieving the same mail over and over again if the reported temporary DNS error is in fact a permanent one.

Reject mails sent with own domain as sender

Many unsolicited emails use the recipient domain also in the sender address. With this option inbound emails will be rejected if the sender address contains one of the local domains. This check is not performed for authenticated connections and connections from IPs listed below "Local IP addresses" in menu "Modules > Mail Server > SMTP settings" on tab "Relay control". Also emails retrieved from a POP server are not affected.



This option checks the so called "Envelope From" and not the "From" header as displayed to the user. See option "Tag mails received from external" in menu "Modules > Mail Server > SMTP settings" on tab "Receiving filters" for a "From" header check.



Enable this option only if all emails with local sender domains are always sent to the Internet via local systems (SX-GATE or internal mailserver).

14.5.3-B Greylisting

Greylisting tries to defeat virus and SPAM mails already before the actual contents are transmitted. The system load caused by virus scanner and spam filter will be reduced, however greylisting is by no means a replacement for both of them. Greylisting takes advantage of the fact that often only one attempt is made to deliver a virus or SPAM mail. If this attempt fails, no retransmission is tried and so the email has been intercepted before it has even been transmitted.



Greylisting only makes sense if incoming emails are delivered directly to SX-GATE with SMTP. Particularly if emails are polled from a POP server, greylisting is useless.

With greylisting enabled, SX-GATE will collect the sender and the recipient address of an incoming email. It will then terminate the connection with a temporary error. The actual contents of the email have not been transmitted at that stage. Usually the instance trying to deliver an incoming email is a mail relay server and not the sender's mail client program. Hence the sender of an email will not become aware of the delay. As SX-GATE indicated a temporary problem, the sending relay server will retry delivery at a later point in time. This is the vital difference in comparison with the behaviour of many spammers and most viruses.

Three parameters control the greylisting. After a configurable minimum period of time, SX-GATE will start to accept retransmissions. The retransmission has to occur within a time limit determined by an other parameter. Meanwhile an email originating from the same source IP and with the same sender and recipient addresses will be accepted at once. If there is no retransmission, the corresponding entry will be deleted. Otherwise it is auto-whitelisted for a configurable period of time. Every use will reset the timeout of the corresponding whitelist entry.

This strategy will quickly develop a database of "well known communication relationships". An email using a registered combination of source IP, sender and recipient will be accepted immediately. In contrast an email will be delayed if is unknown or it timed out.



It depends on the configuration of the sending relay server when and how often it will retry delivery. SX-GATE has no influence on this. In most cases the retransmission will take place in less then an hour. However longer delays are possible. It is even possible that some servers will not retry at all. However in this case the sender is usually notified. There is also a builtin whitelist of important servers which are known not to retransmit.

To avoid unwanted delays, greylisting can be disabled for certain senders or recipients. Greylisting will never be effective for

- connections from a local source IP address (see "Local IP addresses" in menu "Modules > Mail Server > SMTP settings" on tab "Relay control")
- connections from IP addresses included in the builtin whitelist of servers known to perform no retransmissions
- emails retrieved from POP servers
- authenticated connections (SMTP auth)

Working method

This switch will enable greylisting. As described above, greylisting is useful if incoming mails are directly delivered with SMTP. Hence for at least one local domain the Internet DNS mail exchanger (MX) must point to SX-GATE's external IP address.



Any backup MX entries need to be removed from DNS. This does not apply to backup servers which do not accept emails while SX-GATE is alive. Backup servers which apply greylisting themselves are acceptable, too. Adapt the greylist timings to those of the backup.



A setup where incoming emails are forwarded to SX-GATE through an upstream mail relay is not suitable for greylisting. However switching to direct delivery shouldn't be a problem in this case.

check DNS blacklist

This is the most tolerant greylisting mode. Hence it can be enabled without problems on most SX-GATEs, provided the prerequisites for greylisting are met. Once an incoming connection has been established, SX-GATE looks up the source IP in several realtime databases of known SPAM senders and dynamic IP addresses. Only when this lookup succeeds, greylisting will be imposed.

Exchange2k/catch-all mode

This option has been included for two special cases. When selected, the sender of each outbound email will be whitelisted as recipient for inbound mail. Each succeeding outbound mail will renew the clearance, otherwise it will expire after the period of time configured in "Timeout after last use". The run-in phase of this configuration is very short, as every local user has to send but a single mail.



Important local email addresses which are rarely or even never used as the sender address of outbound mail should be added manually to the "Recipient whitelist".



Do not select this option if your setup does not correspond to one of the following. Otherwise greylisting will be of little avail.

Select this option if SX-GATE forwards emails to an internal Microsoft Exchange server release 2000 or older. These servers are not able to reject emails to unknown local recipients beforehand. Instead every mail is accepted and, if the recipient does not exist, a non-delivery response is returned to the sender. So the number of mails to process will almost double, which may have a significant impact on the whole infrastructure. Even worse, in case of a SPAM mail, the non-delivery report is often sent to a faked or non-existent address, which leads to even more annoyance. SX-GATE's particular greylisting mode can help to reduce the amount of non-delivery reports, as every mail which has been addressed to an unknown local recipient has to overcome greylisting.



From Exchange 2003 on it is able to reject emails to unknown local recipients immediately and SX-GATE can check this before accepting an inbound mail. For more information please check the option "Verify internal addresses in advance" in menu "Modules > Mail Server > SMTP settings" on tab "Receiving filters".

The second use case are so called "catch-all" email domains. Here, when no local user is associated with the actual recipient address, the mail is delivered to a dedicated mailbox or group account. The majority of emails here is most likely SPAM to random recipient addresses. The best solution to this problem is probably to get rid of the catch-all behaviour. If this is an option and SX-GATE forwards mails to an internal mail server, please switch to menu "Modules > Mail Server > SMTP settings", tab "Receiving filters", enable "Verify internal addresses in advance" and disable the catch-all feature in the configuration of the internal mail server. If SX-GATE hosts the catch-all mailbox, you can disable it with the option "Emails to unknown local recipients" on the same tab. If however you must continue with a catch-all setup, this greylisting option will help to reduce both, SX-GATE's workload and the amount of SPAM.

permit mail partners

Basically every inbound email has to pass greylisting in this mode. However SX-GATE will extract the sender and recipient of each outbound email and whitelist the reverse address combination for inbound mails. So replies and also any further message exchange using the same addresses is no longer subject to delays. The actual sender IP is not considered. Each outgoing email with the same address combination will refresh the clearance. If it is no longer used, it will expire in accordance with "Timeout after last use".



While an effort is made to avoid delays for correspondence initiated by a local user, initial submissions of a remote user will be deferred. Therefore it is crucial to manually add important sender and recipient addresses to "Recipient whitelist" and "Recipient whitelist" respectively. Explain the prospective delays to the local users, as the delays will particularly hit in the early stages.

always active

This setting enables "pure" greylisting. Each inbound mail will be delayed, except the combination of its IP, sender and recipient is already known.



To avoid annoyance we highly recommend to explain the prospective delays to the local users and fill out the "Recipient whitelist" and the "Recipient whitelist" in advance.

Accept delivery after at least

If a combination of source IP, sender and recipient is not known by the greylist, this parameter controls after how many minutes subsequent connections using the same combination will be accepted. So a retransmission will not succeed until this minimum delay has passed off.



If a retransmission occurs beforehand it will be aborted with a temporary error, too. However this will not prolong the time remaining until it is unblocked.

Timeout of unused entries

This parameter determines how long SX-GATE will accept an initial retransmission. If none occurs, the combination of source IP, sender and recipient will become unrecognized again. A low value will help to keep the internal database small and it will also reduce the risk that a connection is considered to be a retransmission by mistake. On the other hand delivery of requested emails might fail.



Relay servers which retry delivery after longer periods of time will not be able to deliver emails to SX-GATE if the chosen value is too low.

Timeout after last use

After a retransmission, the corresponding combination of source IP, sender and recipient will be stored in the automatic whitelist. The whitelisting will expire after the period of time determined by this parameter. However each new email will reset this timer.

Sender whitelist

This list will accept IP addresses and DNS names of mail servers. The greylist module will always accept emails if the connection's source IP is whitelisted. It is also possible to insert email addresses of individual senders or a complete email domain. To whitelist all the emails from the "example.com" domain, please enter "*@example.com".



Keep in mind that the sender address of an email can be faked easily. Greylisting will check the envelope address only.

Recipient whitelist

To make sure that certain recipients will never be delayed, you can add the corresponding addresses here. To disable greylisting for a whole domain, use an asterisk (e.g. `"*@example.com"`).

14.5.3-C SPF/DMARC filter

SPF is the acronym for "Sender Policy Framework". The owner of a domain can publish a DNS record indicating that only specific servers are permitted to send emails for the domain, i.e. all emails from this domain have to be sent or relayed through these servers. The recipient can lookup the SPF details in DNS and reject non-compliant emails. Both, the HELO name and the envelope sender is checked. The HELO name is the hostname used by the sending system to introduce itself. The envelope sender is the sender address used by the SMTP protocol and does not have to be the same address as displayed by the recipient's mail application. SPF can help defending SPAM and malware sent with forged sender address.



If you decide to publish a restrictive SPF entry for your own domains, the filter will also reject inbound emails pretending to be sent from your own domain. If SX-GATE directly delivers outbound emails, you should make sure that it uses a valid HELO name. It can be configured in menu "Modules > Mail Server > SMTP settings" on tab "Delivery parameters". Instead of publishing an SPF entry for your own domain you could enable option "Reject mails sent with own domain as sender" on tab "Sanity checks".



SPF may cause problems with emails forwarded by a third part. Please carefully consider the information provided for option "Accepted hosts".

DMARC is the acronym for "Domain-based Message Authentication, Reporting and Conformance" and is meant to mitigate the latter problem. It combines SPF and DKIM (DomainKeys Identified Mail). A domain owner who wants to protect his domain with DMARC must sign outbound mails with DKIM, publish the public DKIM key in DNS and add SPF and DMARC policies to his DNS domain. The mailserver of a recipient checks both, SPF and DKIM of an inbound mail. The DMARC check is successful if either the SPF or the DKIM check succeeds whereby the domain in the mail's "From" header

must fulfill the following additional condition: In case of SPF, the domain is compared with the domain from the SMTP envelope from, in case of DKIM with the domain from the DKIM signature. Both domains must be equal, however most DMARC policies allow subdomains, too.

The SPF/DMARC filter checks inbound emails only. So it won't check emails received from IPs from the list "Local IP addresses" in menu "Modules > Mail Server > SMTP settings" on tab "Relay control". Authenticated emails are never checked.



SPF/DMARC can only be effective if inbound emails are delivered directly to SX-GATE with SMTP. Particularly if emails are polled from a POP server, the filter is useless.

Check SPF/DMARC

Enable the check with this switch.

SPF only

Select this option to check SPF only and that already before the mail body is actually transmitted.

DMARC or SPF

Enables the DMARC check. If an SPF policy but no DMARC policy has been published for a domain, an SPF check is performed.

Accepted hosts

The SPF/DMARC filter won't process inbound emails from IPs configured as "Local IP addresses" on tab "Relay control" in menu "Modules > Mail Server > SMTP settings". However it is often necessary to whitelist additional addresses:

Backup MX

If a backup MX is configured for your own domain, SX-GATE must accept emails it receives from the backup MX without filtering. This is because the backup MX is not an authorized sender in the terms of SPF for the sender domain.



If a backup MX is used it also has to perform an SPF/DMARC check. Otherwise it will be used to bypass SX-GATE's SPF/DMARC filter and render it useless. You might want to drop the backup MX.

Own external systems

If you have configured a restrictive SPF entry for your own domain, you might have to enter some of your own external systems here. This is the case if the system sends e.g. status reports or critical warnings by mail and uses your own protected domain as sender.

14.5.3-D Virusscan

Virusscan enabled

Activate this switch to scan all incoming and outgoing emails which pass the SX-GATE mail server for viruses. As an exception, email generated on the system level of SX-GATE like e.g. status reports and backups will not be checked. However emails sent by SX-GATE extensions, such as, in particular, the groupware extension, will be scanned.



A functional virusscanner must be installed on SX-GATE if you want to use this feature. The virus scanner licenses are not included with SX-GATE and must be purchased separately. Further information about supported or already installed scanners can be found in the menu "Modules > Virusscanner". The installation of a virusscanner also has to be made there.

If a virus is found, the infected email will temporarily be stored in the "virusmails" quarantine directory. Only the user "admin" is able to access this directory via the console, secure shell or FTP. Furthermore, if the detected virus is a makro virus or the EICAR virusscanner testpattern, the sender of the mail will be notified.

Mail notification when virus found

If requested, an administrator will be informed by email of every discovered virus. The notification will give details of the infected email.

14.5.3-E MIME filter

All options on this screen refer to email in MIME format. MIME is commonly used to compose HTML emails and emails with attachments.



Please note that automatically modifying emails may be subject to legal constraints or might even be prohibited by law.

Some of the features distinguish between inbound and outbound emails. An email is outbound, if the source IP of the corresponding connection is part of the list "Local IP addresses" in menu "Modules > Mail Server > SMTP settings" on tab "Relay control". Authenticated emails are always regarded as local.



None of the filter options will apply to SX-GATE system mails.

Attachment filter

Enable this feature to look for unwanted kinds of email attachments. Outbound emails with unwanted attachments will be rejected. For inbound emails this is possible, too. However, usually a quarantine procedure will apply for inbound emails. This includes temporarily storing unwanted attachments in a quarantine area which is available via menu "Monitoring > Mail server". Quarantined attachments will be re-scanned by the installed virus scanners after each signature update. Note that quarantined items will be deleted without further notice after the "Storage time" configured below has been reached.

Activating this filter in addition to the virusscanner absolutely makes sense. A virusscanner can only detect known viruses or viruses which can be identified due to certain well known characteristics or patterns. Therefore the attachment filter can enhance the overall security.

incoming mails only

Enable this option if you want to look for unwanted attachments in inbound emails only.

incoming and outgoing mails

Use this setting to filter any email passing SX-GATE's mail server. While the filtering behaviour for inbound emails is configurable, outbound emails with unwanted attachments will always be rejected.

Scan ZIP/RAR archives

Enable this switch to include the contents of ZIP and RAR archives when scanning for files with blocked names. If an archive contains at least one restricted file or not only permitted files, the whole archive is not permitted.



No other archive types are supported by this function. Archive inspection is non-recursive, i.e. archives inside of archives will not be scanned.

Scan TNEF files (winmail.dat)

Enable this switch to include the contents of TNEF files (winmail.dat) when scanning for files with blocked names. If a TNEF file contains at least one restricted file or not only permitted files, the whole archive is not permitted.



No other file types are supported by this function. Inspection is non-recursive, i.e. TNEF files inside of TNEF files will not be scanned.



If the "Quarantine mode for inbound emails" is set to "remove attachment" the entire E-Mail will be withheld regardless.

Quarantine mode for inbound emails

Determine how to deal with emails containing unwanted attachments.

If one of the quarantine options has been selected, an administrator can inspect filtered attachments in menu "Monitoring > Mail server" and forward them to the recipients anytime. In addition, you can configure option "User access to quarantine area" to send the recipients a link which grants them access to the quarantine directory if certain conditions are met.

remove attachment

When this option is selected, unwanted attachments in an email will be replaced by a reference text. The modified email will then be delivered to its recipients.

The advantage of this setting is that the recipients immediately receive as much of the original email as possible. For the administrator this setting will become the more time consuming one, if he often has to unquarantine attachments and forward them to the recipients, because each attachment has to be downloaded and forwarded manually.

retain email

Here the whole email is quarantined. A notification email will be sent to all recipients.



If "Quarantine mode for inbound emails" is enabled, following the link of an email which has been sent to multiple recipients will trigger delivery to all recipients.

The advantage of this option is that the signature of signed email won't be destroyed. For the administrator, delivery of a quarantined email is just a single click.

reject email; no quarantine

Select this option to reject emails with unwanted attachments completely. Neither the recipients nor the administrator will be notified. The sending system is responsible for notifying the sender that the email cannot be delivered.



We strongly recommend not to use this option if SX-GATE retrieves emails from a provider mail server with POP or IMAP. In this case SX-GATE would generate an undeliverable response which would affect third parties in case of forged sender addresses.

Tag for subject of affected mails

The subject of an email which was retained or from which attachments were removed can be prefixed with a tag like e.g. "*** CAREFUL ***" or "[FILTERED]".

User access to quarantine area

To relieve the administrator, recipients can be allowed to access the quarantine area themselves under certain conditions. Depending on the setting "Quarantine mode for inbound emails" the recipient will either get links for downloading quarantined attachments or a link to trigger delivery of a quarantined email. When following the link the user will receive an error message, if a virus has been found in the mail or if not all of the requirements configured here have been met yet.



The recipients won't receive a link to attachments or emails with attachments from the list "Dangerous attachments" or for office documents with makros if "Office documents are dangerous" is enabled.

no

With this option, recipients won't have access to the quarantine area.

immediately

The recipients may access the quarantine area anytime, even if no re-scan with updated virus scanner patterns has taken place yet.

after next virusscanner signature update

Here the recipients must wait until the quarantine area has been scanned with updated virus scanner patterns. The administrator can still access the quarantine area anytime via administration interface.



The virus scanner vendors publish new signatures at irregular intervals. It's not important when SX-GATE will check for new signatures, but that updated signatures are actually available.

earliest after

In addition to a re-scan with updates virus scanner patterns, an email must have been quarantined for the configured amount of time before access is granted to recipients. If several hours have been configured it is likely that multiple re-scans with updates virus patterns take place.

Hostname in link

If option "User access to quarantine area" is enabled, users will receive emails with HTTPS links to access quarantined files or mails. You can configure the hostname or IP address used in the link here. The clients must be able to reach the SX-GATE reverse proxy via this address. In the reverse proxy configuration access to the quarantine directory must be enabled.

Mail notification upon each quarantined email

An administrator can be informed about every email which is either retained or quarantined in parts.

Storage time

Number of days email attachments or emails will be stored in the quarantine folder before they are deleted at around midnight.

14.5.3-F MIME filter rules

The settings on this tab determine if and which attachments will be objected. The order of the input elements corresponds to the order the attachments will be checked.

Office documents are dangerous

Enable this feature to detect and object office documents with macros. The detection is independent of the actual filename. Archives will be scanned recursively. The list "Trusted senders" does not apply.



Only an administrator may access attachments which have been quarantined due to this list.

Dangerous attachments

All attachments with an extension or MIME type listed here will always be objected, regardless of any exceptions configured below like e.g. "Trusted senders". Enter potentially dangerous filename extensions here.



Only an administrator may access attachments which have been quarantined due to this list.

It makes no difference, if you specify an extension as e.g. "exe", ".exe" or "*.exe". All three formats refer to the extension "exe". SX-GATE tests each attachment, if its filename ends with a dot, followed by one of stated extensions. These are compared case insensitive.

You may also add MIME types like e.g. "application/zip" to the list. An asterisk serves as a placeholder (e.g. "application/*"). The configured MIME types are compared with the "Content-Type" as specified for each email attachment.

Trusted senders

The restrictions of options "Dangerous attachments" and "Office documents are dangerous" apply, otherwise any attachment of senders in this list may pass. Any restrictions configured in the settings below don't apply to these senders.

You can add a complete email address (e.g. user@example.com) to prevent filtering attachments from this specific address. Add only the domain part of the address (e.g. example.com) to accept any attachment from senders in the entire domain.

Office documents are unwanted

Enable this feature to detect and object office documents with macros. The detection is independant of the actual filename. Archives will be scanned recursively.

Accepted attachments

This setting is only available if "All other attachments are: unwanted" has been configured. Only those attachments ending with one of the filename extensions listed here will be accepted. All other attachments will be objected.

It makes no difference, if you specify an extension as e.g. "pdf", ".pdf" or "*.pdf". All three formats refer to the extension "pdf". SX-GATE tests each attachment, if its filename ends with a dot, followed by one of stated extensions. These are compared case insensitive.

You may also add MIME types like e.g. "image/png" to the list. An asterisk serves as a placeholder (e.g. "image/*"). The configured MIME types are compared with the "Content-Type" as specified for each mail attachment.

Unwanted attachments

This setting is only available if "All other attachments are: allowed" has been configured. Email attachments with filename extensions listed here will be objected. All other attachments may pass.

It makes no difference, if you specify an extension as e.g. "zip", ".zip" or "*.zip". All three formats refer to the extension "zip". SX-GATE tests each attachment, if its filename ends with a dot, followed by one of stated extensions. These are compared case insensitive.

You may also add MIME types like e.g. "application/zip" to the list. An asterisk serves as a placeholder (e.g. "application/*"). The configured MIME types are compared with the "Content-Type" as specified for each email attachment.

All other attachments are

Here you can configure the default behaviour of the filter.

14.5.3-G MIME filter options

On this screen some additional MIME filter features are available which can be used even if the attachment filter is disabled.



Please note that automatically modifying emails may be subject to legal constraints or might even be prohibited by law.

Some of the features distinguish between inbound and outbound emails. An email is outbound, if the source IP of the corresponding connection is part of the list "Local IP addresses" in menu "Modules > Mail Server > SMTP settings" on tab "Relay control". Authenticated emails are always regarded as local.



None of the filter options will apply to SX-GATE system mails.

Don't modify signed mails

The signature of an email becomes invalid if the contents of the mail are modified. Enable this switch and mails signed with PGP or S/MIME will pass the filter unchecked. The following options are affected:

Inbound emails

"Attachment filter" on tab "MIME filter" if "Quarantine mode for inbound emails" is set to "remove attachment".

The options "Defang HTML messages" and "Remove redundant HTML parts" below

"Tag mails received from external" in menu "Modules > Mail Server > SMTP settings" on tab "Receiving filters".

Outbound emails

"Disclaimer" in the domain configuration below menu "Modules > Mail Server > Domains"



Please keep in mind that this option provides a simple way for an attacker to bypass the aforementioned filters.

Defang HTML messages

HTML formatted emails can be abused in various ways. Exploiting vulnerabilities of the user's mail client, web bugs used by spammers to collect addresses of users who open SPAM, phishing mails trying to get confidential information like passwords - just to mention a few.

Enable this option to defeat most of these dangers. SX-GATE will then scan for critical HTML elements and rename them. The user's mail client will then no longer recognize these elements, so the user is quite safe. For people who are familiar with HTML it is however easy to recognize the original contents. Even without HTML knowledge the original document can be reconstructed. Just erase every occurrence of the text "DEFANGED_" in the document.



This filter will be applied to incoming emails only.



Attached HTML files will be filtered, too. Send HTML files in archives to make sure these will not be altered.

enabled

Select this option to defang HTML in emails. Tags which are used to embed active contents and form elements will be affected. The same applies to scripting and unknown HTML elements. References to external resources which trigger unnoticeable actions are filtered, too. The target of links will be removed if it refers to active components.

all-out

In addition to the measures described for option "enabled", with this setting all references and any link target will become unusable.

Remove redundant HTML parts

Some mail programs can be configured to send the contents of every email twice, as plain text and in HTML. Both parts are denoted as alternative contents (multipart/

alternative). The recipient's mail client will choose according to its capabilities and configuration which part it is going to display.

To automatically remove the HTML part of alternative contents you can enable this switch.



Only inbound emails will be filtered. Pure HTML emails will not be affected.



The removed HTML part will not be quarantined. There's no way to restore it. No notification will be sent to the administrator either.

Use this option to save bandwidth if e.g. mobile clients will be retrieving emails. In addition local users will be protected from unwanted side effects of HTML mails without the risk of losing information, as one can expect identical text contents in both parts of a regular email. Note however that this will not apply to many SPAM mails or advertising.



In the text part there will be no formatting like e.g. colours or different font sizes. Links will not be clickable, except the user's mail client provides an automatic link detection. Furthermore external resources loaded by an HTML mail while opening it will be missing, too. This is however a nonserious bad practice (web bugs).



The quality of the SPAM filter results may be reduced for emails which have been altered by this feature.

14.5.3-H Relay SPAM filter

A SPAM mail is an unsolicited email, usually with dubious origin. The SPAM mail filter tries to detect these emails and can be configured to tag these mails or refuse to accept them.

The SPAM mail filter of SX-GATE classifies emails by identifying typical phrases and other attributes indicating an unsolicited email. SX-GATE contains a database of checks to perform and all matches result in a score which in turn allows filtering emails. Characteristics indicating a SPAM mail will add a value to the score while other

characteristics indicating that it's not a SPAM mail will subtract a certain value. The higher the final score, the more likely it's a SPAM mail.



Emails exceeding the size of 1MB will not be classified to save system resources. However this is not a drawback, as a SPAM mail is usually very small.

A few headers will be added to each email examined by the SPAM mail filter. The header "X-Spam-Status" shows the final score (hits=...) and give the name of the matches (tests=...). This allows the recipient of the mail to check the score of any mail. The header "X-Spam-Level" will contain one "x" per scored point (e.g. "X-Spam-Level: xxx" for a score between 3.0 and 3.99). This header allows automatic sorting in the user's mail client.



Most mail clients will display only the most important headers by default. Usually the full header information is available after selecting a specific menu option.

SX-GATE's SPAM mail filter can be activated at two different places: In the user administration individually for each mailbox or here on tab "Relay SPAM filter" in equal measure for every recipient.



All the other SPAM related tabs here in menu "Mail Server" affect both ways of SPAM filtering.

If SX-GATE forwards emails to an other (internal) mail server, you have to activate the SPAM filter in relay mode here on this tab. If however SX-GATE keeps the mailboxes for your domains, both ways of SPAM filtering are possible.



The user specific SPAM filter will be disabled when activating the relay SPAM filter.

To activate the SPAM filter in relay mode you have to enable at least one of the thresholds. In this mode it examines every incoming email while passing the SX-GATE mail server. It is not possible to assign different thresholds to different users.



To differentiate incoming from outgoing emails, SX-GATE will consider the source IP address of the respective SMTP connection. In menu "Modules > Mail Server > SMTP settings" on tab "Relay control" the parameter "Local IP addresses" determines which IP addresses refer to internal senders. The relay SPAM filter will not analyze their emails. In addition also authenticated mails will not be checked.

Tag an email as SPAM when it is scored more than

If the score exceeds the threshold for tagging an email as SPAM, the subject of the mail is prefixed by the text "***** SPAM *****" and the SPAM score.

Send tagged emails to

Instead of delivering potential SPAM mails to the original recipients, tagged emails can be redirected to a specific address. The email header "X-Spam-Orig-To:" will contain the list of original recipients in this case.



Automatic redirection of emails may be subject to legal constraints or might even be prohibited by law.

Refuse to accept mails when score exceeds

Exceeding this threshold, SX-GATE's mail server will refuse to accept the email. The sending system in charge of a proper reaction like e.g. notifying the sender or an administrator. If you want to be sure that no requested email gets lost, you should not enable this option. Activate the threshold "Tag an email as SPAM when it is scored more than" instead and make use of the features offered by the mail client programs to sort emails based on header lines.



Emails which have been retrieved from a POP server by SX-GATE's mail client will be silently discarded if the mail server refuses delivery due to the SPAM filter. There will be no notification and it is not possible to undelete the email. The email is lost irrecoverable!



To avoid loss of important emails you should be very carefully when activating this option. You should select a value which is rather to high than to low. Please note that automatically deleting email may be subject to legal constraints or might even be prohibited by law.

14.5.3-I SPAM scores

The settings made on this screen will not only apply to the relay SPAM filter, but also to the user specific SPAM filter as configured in the user administration.

Userdefined SPAM checks

This control allows you to extend the SPAM checks by self-defined rules. First you have to decide to which part of the mail a new rule applies. If the specified pattern is found in a mail, the selected score is accounted.

The following types of SPAM filter rules are available:

Subject

The pattern is looked up in the email's subject.

Sender

This will check the sender of the mail (From header).

Recipient

Use this option to match the recipient (To header).

Message header

Allows you to examine an arbitrary mail header.

Message text

The actual text contents of the email, including the subject, are analyzed when selecting this value.

Raw HTML text

Just like the previous option, but including HTML tags of HTML emails.

Web links

Checks web links (either plain text or HTML links) found in the subject or the message body.

Rule

This setting differs from the previous ones. It allows you to modify the score of SX-GATE's builtin rules. Accordingly you don't specify a search pattern here. Instead you have to supply the internal ID of the rule. The ID together with the original score is listed in the content analysis of mails, that have been marked as SPAM (e.g. "HTML_MESSAGE" or "FORGED_MUA_OUTLOOK").



When the builtin rulesets are updated, internal ID's may change without notice. The rules defined here will not be adjusted.

Search patterns ("matches") are case-insensitive. If the pattern starts/ends with a letter or a digit, the pattern matches only if the pattern is found at the beginning/end of a word. So e.g. the pattern "pace" won't match "spaces" but will match "Learn at your own pace!".

Some characters have a special meaning:

***** (Asterisk)

It represents a sequence of arbitrary characters. The sequence may also be missing. As searching for such a sequence of any length is rather time-consuming, an asterisk matches no more than 30 characters. The pattern "a*d" will match e.g. "ad", "a_d" and "abcd". The asterisk helps you to find patterns within words. So e.g. the pattern "*pace*" will match "spaces".

? (Question mark)

Any single character is matched by a question mark. If for instance "a?d" is looked up, "a_d" is a hit. In contrast "ad" and "abcd" do not apply.

_ (Underscore)

An underscore matches any amount of whitespace characters, i.e. spaces, tabs and new-lines. As an example, "a_d" will match "a d", but not "ad" or "a_d".

Please keep an eye on the configured thresholds when selecting the score for a new rule. For a rule which refers to SPAM mails you have to select a positive value. Negative numbers reduce the probability of matching emails to be classified as SPAM.

SPAM filter whitelist

Of course the SPAM mail filter will not achieve a hit ratio of 100% when classifying emails automatically. If an email was identified as SPAM by mistake, you can add the sender to this list. The SPAM filter will subtract 100 points from the SPAM score of a mail, if the sender is found in this list. Thus all future emails of senders listed here will never be recognised as SPAM.

You can add a complete email address (e.g. user@example.com) to prevent filtering emails from this specific address. If you want to allow every email from a specific domain to pass, add only the domain part of the address (e.g. example.com).

14.5.3-J SPAM modules

The settings made on this screen will not only apply to the relay SPAM filter, but also to the user specific SPAM filter as configured in the user administration.

DNS based lists

Several blacklists are available in the Internet, which contain mail servers known to be the origin of SPAM mails. Another form of blacklists contains web server addresses that are advertised by SPAM mails (URI: URI Black Lists). Links in the message body are checked against these URI Black Lists. Finally there are also whitelists with friendly mail servers.

When analyzing an email, some of these lists can be queried. Each single hit will be rated with a rather moderate value. However when multiple lists indicate potential SPAM, it will have considerable impact on the SPAM score. The reliability of the lists depends on how the entries have been collected. Choose which level of quality will be considered.

few

Select this option if you want to include only verified SPAM sources. Particularly automatically collected lists will not be considered. URI Black Lists are active.

medium

In addition to verified SPAM sources this level will also include addresses collected automatically by SPAM traps.

many

If you choose this option, emails from known dynamic IP addresses will be scored, too.

Razor2 distributed spam filter network

This feature will calculate a fuzzy checksum of some parts of an email and send it to Razor2 servers in the Internet (TCP port 2703). Razor2 provides a database with the checksums of known SPAM. In case of a match, the SPAM score of the mail is increased. The amount depends on the reputation of those, who reported the SPAM mail to the Razor2 system.



Do not activate this feature when your internet connection is a rather expensive dial-up link. For each email, the Razor2 checksum will be sent to the internet, even for internal emails. Thus the dial-up link will be online frequently which results in high expenses.

Enable Bayes filter

If enabled, the SPAM filter autonomically learns additional characteristics of unsolicited mail (SPAM) and requested mail (HAM) while processing inbound emails. Only mails with a score of more than 10 or 0 and less are considered respectively.



At least 200 SPAM mails and 200 HAM mails have to be learned before the Bayes filter is taken into account.

With this feature it also becomes possible to learn unrecognized SPAM and emails which have been tagged as SPAM by mistake. A user account with mail permission (group system-mail) on SX-GATE is required and either IMAP or the SX-GATE groupware must be used to access the mail account.



In the user administration there's an option which makes SX-GATE deliver SPAM into the "SPAM" folder. The folder will be created automatically if necessary. We recommend that you enable this option.

Using IMAP, you will have to add special mail folders. Move unrecognized SPAM into a folder named "SPAM". A copy of mistakenly tagged emails goes into the "HAM" folder.

Just after midnight a brief overview of the folders' contents will be mailed to the corresponding user. At the same time, the Bayes filter will learn the contents of these folders, if enabled. A per user setting in the user administration determines when emails from these folders will be deleted automatically.

OCR for images

Some SPAM mails use images to convey their message, so traditional text analysis will fail. The character recognition tries to identify text in those images. Detecting typical SPAM phrases, the SPAM score is increased by a basic value and a surcharge per suspicious word.



In order to save system resources, the OCR won't be started if the mail's SPAM score is sufficiently high.

English language indicates potential SPAM

The majority of SPAM mails is written in English language. Activate this switch to add some points to the SPAM score of every English email. This will result in a significant increase of the probability that the score of English mails will exceed the configured SPAM filter thresholds.



Use "Userdefined SPAM checks" to change the score of this setting. In the user administration you can even change it individually for every local account. The rule ID is "UNWANTED_LANGUAGE_BODY".



As this rather drastic measure affects all users, they all should agree upon its activation.

Charsets from the Far East indicate potential SPAM

With this switch you can increase the SPAM score of every email which references charsets of Japan, Korea, Thailand or China.

Cyrillic charsets indicate potential SPAM

With this switch you can increase the SPAM score of every Cyrillic email.

14.5.3-K SPAM settings

The settings made on this screen will not only apply to the relay SPAM filter, but also to the user specific SPAM filter as configured in the user administration.

Forward original contents of SPAM emails

With this parameter you can control how a mail will be tagged as SPAM. In any case the prefix "*****SPAM*****" and the SPAM score will be prepended to the email subject.

as attachment

If you select this option, the email will contain a preview to the original contents and a detailed break down of the SPAM score. The original message is enclosed as attachment.

Delivering the original email as attachment is supposed to achieve that selecting the email in the mail client will not trigger any unwanted actions. Depending on the mail client program used, the mere selection of an HTML formatted email may for example trigger the download of images from the Internet as the mail client tries to show a preview of the mail. So the sender of a SPAM mail is unnoticeably informed that the SPAM mail was opened. This will increase the value of this email address for SPAM mail senders and in turn more and more SPAM will be sent to this address.

without modification

With this option the original contents will be forwarded. A break down of the score will be added to the headers of the mail.

Always add detailed report

Email which haven't been classified as SPAM will also include a detailed break down of the SPAM score when this option is enabled. The information is passed as mail header "X-Spam-Report".

Contact email of SPAM administrator

Please specify the address of the SPAM filter administrator here. It will be included in emails which are tagged as SPAM.

14.5.4 Archive

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

14.5.4-A General.....	482
14.5.4-B Users.....	484
14.5.4-C Mail feeds.....	485
14.5.4-D Storage.....	487
14.5.4-E Time stamping.....	488
14.5.4-F Backup.....	489
14.5.4-G Tools.....	490

The mail archive module can be installed in menu "System > Apps". The extension is subject to a fee.

The archive encrypts and stores mails on a network share. It provides a frontend for searching, reading and downloading mails with a web browser.

14.5.4-A General

Four-eyes login for auditors

If enabled, whenever one of the special users "auditor" or "revisor" logs in, this has to be confirmed by entering the "admin" password, too.

Delete option for auditors

In certain situations it might be necessary to delete emails from the archive.

disabled

Manually deleting mails is disabled. Mails will only be deleted after expiration of the archiving period.

after approval

When selected, a request to delete an email has to be accepted or denied by the special user "dataofficer".

enabled

Select this setting if auditors should be able to delete emails right away.

Subfolder support

With the help of this option, a cross-user structuring of the archived mails is possible. In the administration interface of the archive app, the "admin" can create folders and configure rules to automatically file new mails into these. The "admin" can also grant individual users the right to manually move mails into certain folders. The "auditor" user is always allowed to do this for any folder. The "revisor" however may either work with all folders or can be restricted to certain folders. So e.g. a tax auditor can be limited to see the contents of folders with tax relevant mails only.

Default archiving period

A new mail will be deleted from the archive after the period of time you configure here. In the administration interface of the archive app, the "admin" can configure rules for excluding mails from the archive or for using a different period of time, so that e.g. applications are not archived at all or will be deleted after a few weeks.



Changing this value does not affect already archived mails.

Mailheader with additional recipient address

In particular when retrieving mails from a POP or IMAP server, the original SMTP recipient information (envelope recipient) is often no longer available. If you are lucky, a mail header like e.g. "X-Envelope-To:" has been added with the original address. Configure the name of the header here if applicable.



Changing this value does not affect already archived mails.

Mailheader signaling SPAM mail

When archiving a new mail, it will be marked as SPAM if it contains a header which starts with the value configured here.



Changing this value does not affect already archived mails.

Archive sends mails via mail server

The user interface of the archive allows users to send themselves archived mails. The mails are delivered via the mail server configured here.

SMTP-Auth username

Enter the necessary credentials if user authentication is required for sending mails via the mail server. Leave empty otherwise.

14.5.4-B Users

User administration

Select how the administration of users and groups in the archive should take place.



When switching between "SX-GATE user administration" and one of the other options at a later point in time - no matter into which direction - all settings related to users and groups as well as notices and tags will be lost in the app!

User administration of App

With this option user and groups will be managed by "admin" in the administration interface of the archiving app. This offers maximum flexibility at the price of redundant user administration.

SX-GATE user administration

Select this option if SX-GATE is your mail server, i.e. mailboxes and corresponding users already exist on SX-GATE. Users and groups are then automatically available in the archive app, too.



When switching to or from this option at a later point in time, all settings related to users and groups as well as notices and tags will be lost in the app!

Microsoft Exchange (Active Directory)

This is the recommended setting when operating a local Exchange server.



Configure the LDAP parameters for access to the Active Directory in menu System > User administration > Settings".

Reset password for "auditor"

The login "auditor" is a special user for the person which is responsible for the contents of the archive with unrestricted access to all emails.

Reset password for "revisor"

The "revisor" is intended for an external auditor. In the administration interface of the app, the "admin" user can grant unlimited access to all E-Mails for "revisor" or limit access to certain domains or the contents of certain folders.

Reset password for "dataofficer"

This user is required only when deleting mails after approval is enabled. In this case the "dataofficer" must approve deletion requests made by "auditor" or "revisor".

14.5.4-C Mail feeds

Archiving by SX-GATE mail server

We recommend this kind of archiving whenever possible. When enabled, mails will be archived while being processed by the SX-GATE mail server.



To archive mail which are not processed by the SX-GATE mail server additional or alternative ways to archive have to be used. This affects in particular internal mails when using a hosted or an internal mail server.

With this option mails will be stored in an Exchange Journal-like format. The advantage is that it includes the envelope recipients as used e.g. with blind-copy emails (Bcc).

When using the SX-GATE S/MIME gateway, inbound mails will be decrypted before archiving, outbound mails will be archived before encryption.

Otherwise the mail is archived in its original form, as the contents are extracted right after the anti-virus check. In particular the archived mail will not include changes made by the SX-GATE MIME or SPAM filters. Nevertheless, mails marked as SPAM by the relay SPAM filter can also be tagged as SPAM in the archive. Mails held back in the MIME filter quarantine directory will be archived when released. Mails rejected by the MIME or SPAM filters are not archived.



The individual per-user SPAM filter will be called after archiving. So mails will be archived even if the SPAM filter discards them later. There's also no tagging as SPAM of archived mails. So please enable the SX-GATE relay SPAM filter instead of using the per-user SPAM filter.

Archiving by sending mail to domain

The SX-GATE mail server will forward email addressed to the domain configured here to the archive. The local part of the email address (the part in-front-of the @) has no meaning. Use whatever you want. This method of archiving can e.g. be used in combination with the journal feature of Microsoft Exchange servers.

Archiving via DNAT rule in firewall

The previous methods used the SX-GATE mail server to store mails in the archive. With the help of a firewall rule you can instead talk directly to the SMTP server of the archive. Please add a DNAT rule manually which forward the connection to the address displayed here.



Do not make the SMTP server accessible for arbitrary Internet addresses!

Required mail header for archiving

If you configure the name and the value of an email header here, emails delivered to the archive by SMTP will be stored only if they contain a mail header starting with the configured value. This serves as an additional protection if it is possible to address the SMTP service of the archive from less trustworthy networks.



Please pay attention to correct upper and lower case letters of both, header name and value.



Emails without this header will be discarded by the archive and not stored.

You may e.g. filter mails from Microsoft 365 by default domain: "X-OriginatorOrg: ...".

Select key/certificate for STARTTLS

For archiving via DNAT rule the connection can be encrypted with STARTTLS. Please select one of the keys managed in menu "System > Certificate manager > Keyring".

14.5.4-D Storage

The archive consists of the encrypted emails, a database with the meta data and the search index. On this screen you configure where the encrypted emails and the database backup are stored.



We recommend an external storage device like e.g. a NAS.



Make sure that the data stored on the storages is backed up regularly.

Storage volumes

Configure the storages. Add an other storage when running out of space. If a storage is temporarily unavailable, you can disable it.



Never delete a storage when emails have been archived on it or when emails have been archived to a storage with higher ID.



Please contact technical support if you want to merge the contents of multiple storages on one storage.

The special storage "local (only for testing)" is intended for testing purposes only. All data is stored within the device with its rather limited capacity.



When deleting the archive app, all emails and database backups stored on this storage will be lost.

Write to storage

If multiple storages have been configured, select to which storage new mails and the database backup will be written.

14.5.4-E Time stamping

Legal requirements for archiving of mails usually include the duty of proof that the documents have not been altered. SX-GATE uses a time stamping service for this.

For each mail in the archive a checksum is stored in the database to verify that the individual mail has not been modified. However to proof that no one has tampered with the database, an external proof in form of a timestamp is required. So an other checksum is computed over the checksum of multiple mails and then signed by a time stamping service.



It is often required to use certain accredited time stamping services.

Time period for time stamps

Period for requesting new time stamps for newly archived mails. Additionally a new timestamp for 10000 mails is requested every 15 minutes if more than 10000 mails are pending.

URL of time stamp service

Please enter the URL of the currently used time stamping service (e.g. "http://tsa.example.com/" oder "https://ca.example.com/tsa/").

Login

If authentication with a username and a password is required to use the time stamping service, please enter the credentials here. Leave the input fields empty, if no authentication is required.

CA certificates of all time stamp services used so far

The time stamps are verified with the CA certificates entered here. When viewing an email in the archive which has not been time stamped yet, a verification error is displayed. If the list is empty, time stamps will not be checked.



Usually CAs use a dedicated root certificate for their time stamping services which is not part of the "usual" certificate bundles. So please import the required root certificate in menu "System > Certificate manager > CA certificates" first.

Test time stamping configuration

The test gets a time stamp from the configured URL and tries to verify it using the configured CAs.

14.5.4-F Backup

You must backup the following components in order to be able to restore the backup:

Archive key

You can backup the key on this screen

Database with the meta data

Enable the scheduled backup on this screen. The database backup is written to the active storage.

Storages with the encrypted mails and the database backup

Please use external tools to backup this data. To make distributed or internally stored data accessible to an external tool, SX-GATE can mirror all storages to a network share.



There's no backup of the search index. It must be rebuild in case it got lost.

Create backup of archive key

Here you can backup the archive key. If this key should ever get lost, the archive is no longer readable. If the key or its backup should fall into wrong hands, it could be used to read the encrypted mails and the database backup.



The archive key is neither part of the SX-GATE backups nor part of the database backup or any other backup.

Scheduled database backup

The backup is stored on the active storage in the folder "database". A subdirectory is created for each full backup, containing the full backup file and files for associated incremental backups.



The subdirectory of a full backup is deleted from the active storage if it is older than seven days and at least two newer subdirectories with full backups exist.

Plus mirroring of archive and database backup to Windows share

Enable this option to mirror the encrypted mails of all storages and the database backup to a network share. The mirror is updated as part of the automatic database backup. You can also start the process manually.



Use an external tool to backup the data on this share.

Backup database now

Stores an incremental backup of the database. If no full backup is found on the active storage, a full backup is made instead.

Backup archive and database backup now

Mirrors the mails and the database backups of all storages to the configured network share.

14.5.4-G Tools

Update index

The search index is updated automatically every 30 minutes. Trigger an update to find mails in the archive which have just arrived.

Re-create index

With this function the search index is re-created by processing all stored emails.

Import emails from a POP3/IMAP4 server

Use this wizard to import emails from a POP or IMAP server once.

Import emails from a storage

Use this wizard to import emails from one of the storages once. On the storage the mails in eml format must be placed in the folder "import".

Export emails to a storage

You can download smaller numbers of emails from the search interface of the archive. Use the export to a storage if you need to download large amounts or even all emails. On the storage the mails will be stored as eml files in folder "export". An ID which is unique for each email is used as filename. So you can even run the export multiple times with different queries to sum up the results in the export directory.

Selection***Export to storage***

Mails will be exported into folder "export" on the selected storage.

Query

Leave empty to export all mails. To limit the export, please proceed as follows:

- Log in to the archive as "auditor" or "revisor"
- Put the search together
- Right below the search results there's a link labeled "sphinx". Copy the query which is displayed when clicking the link
- Paste the query here

Authorization by user

The password of the user you select here has to be entered to authorize the export.

Check selection***Number of selected mails***

Displays how many mails would be exported in the next step.

14.5.5 TLS Encryption

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

14.5.5-A General.....	492
14.5.5-B Mail server certificate.....	494
14.5.5-C Trusted CAs.....	494

SX-GATE supports the encrypted transmission of mails using the STARTTLS command. However, only the SMTP connection between the SX-GATE mail server and its communication partner will be encrypted.



This option will not assure an end-to-end encryption from the sender to the recipient. Furthermore the authenticity of the email can not be granted.

14.5.5-A General

TLS encryption

Encryption can be forced for certain connections to guarantee the encrypted delivery of emails. If the SX-GATE mail server is configured to prefer encrypted communication, it might be necessary to suppress encryption with certain opposites. You can configure both in this area.

forced when sending to recipient domain

Encryption can be forced when sending mails to a certain recipient domain. Use this setting if the recipient's mail server can change (e.g. because there is a backup mail server operated by the ISP). If the addressed mail server does not support encryption, the mail will be queued. SX-GATE will retry the delivery at a later point in time.

forced on communication with server / client

Supply the IP address or the DNS name (not the mail domain) of a mail server or mail client. In contrast to the previous option, encrypted communication is also enforced on incoming mails. SX-GATE will not accept an unencrypted incoming mail from the corresponding address. If an outgoing mail cannot be delivered encrypted, it will bounce back to the sender as undeliverable.

denied on communication with server / client

Also with this option you have to enter the IP address or the DNS name (not the mail domain) of a mail server or mail client. SX-GATE won't offer encryption for incoming connections from this address. On outgoing connections a corresponding offer will be ignored.

Verify server identity

If encryption is required, this option additionally verifies the certificate presented by the server for outbound mail. It must have been issued by the CA configured on tab "Trusted CAs". Also the server certificate must have been issued to the correct server name.



If disabled and in combination with "forced on communication with server / client", "DANE" will be disabled for outbound connections to the specified mail server. In combination with "denied on communication with server / client", this option has no meaning.

Always try and propose TLS encryption (STARTTLS)

If this switch is activated, SX-GATE will try to send outgoing emails encrypted, whenever the remote SMTP server supports it. Furthermore SX-GATE offers encryption for all incoming connections. In this case, the opposite server or client decides whether it makes use of this option.

TLS protocol

Select the encryption strength. This setting applies to both, sending and receiving mails.



The actual encryption parameters associated with each option are updated from time to time.

outdated

For compatibility with older devices, AES ciphers using the discouraged Cipher Block Chaining (CBC) will be enabled when selecting this option. The minimum TLS version is 1.0.

compatibel

Select this option for wide compatibility with older systems. The minimum TLS version is 1.0.

contemporary

Only halfway recent systems will be supported when selecting this option. At least TLS 1.2 is required. It is a good choice for security, however there is a risk that you may not be able to send mail to or receive mail from certain mailservers if direct communication with arbitrary mailservers on the Internet is required.

maximum

Requires TLS 1.3. This setting is not suitable for direct communication with arbitrary mail systems on the Internet (i.e. direct delivery of inbound or outbound mail via DNS MX record). Make sure that all potential peers support TLS 1.3 before selecting this option.

Verify server certificates with DANE/TLSA

In contrast to HTTPS, server certificates are commonly not validated when a mail server connects to an other mail server, as frequently mail servers have no valid certificate. Using DANE (DNS-based Authentication of Named Entities) the operator of a mail server can publish information in DNS which tells other mail servers that this is a mail server with a verifiable certificate and how to verify it. The goal is to get a connection which is protected against Man-in-the-Middle attacks.



DANE is based on DNSSEC, so DNSSEC validation must be enabled in the SX-GATE DNS server (Menu "Modules > DNS > Settings" on tab "Client access").

If connections to a specific mail server fail due to misconfiguration, you can disable DANE for this server with an entry in table "TLS encryption" above. Add an entry with

"Encryption forced on communication with server / client" but without "Verify server identity".

14.5.5-B Mail server certificate

SX-GATE's mail server presents this certificate to clients and other mail servers which are able to use an encrypted connection when delivering an email to SX-GATE (SMTP STARTTLS). The certificate is also used by the POP3 and IMAP4 servers of SX-GATE to provide encrypted access.

Select key/certificate

Please select one of the keys managed in menu "System > Certificate manager > Keyring".

14.5.5-C Trusted CAs

SX-GATE checks the certificate of the destination server when sending an email via a TLS encrypted connection. SX-GATE will consider all certificates issued by a CA in this list as trusted.



By default, SX-GATE will deliver emails even if the destination server certificate is untrusted. To change this behaviour for specific destinations, please add them to the list "TLS encryption" on tab "General" with option "Verify server identity" enabled.

14.5.6 S/MIME gateway

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

14.5.6-A General.....	495
14.5.6-B Decrypt.....	497
14.5.6-C Verify.....	498
14.5.6-D Sign.....	500
14.5.6-E Encrypt.....	502

The S/MIME gateway allows you to utilise S/MIME automatically towards the outside including a centralized key management. Inbound emails can be decrypted with their signatures checked automatically. The email subject will be tagged to show the result

of these operations. Certificates received as part of a signature can be used to encrypt outbound emails. Outbound emails are signed and encrypted automatically if possible.



Before you start to use this component, you should be aware of its implications. S/MIME should guarantee that the message actually originates from the claimed sender and promises encryption and integrity from end-to-end. All this is only partially true when using an S/MIME gateway as there is no S/MIME protection between the gateway and the internal sender or internal recipient, opening the door for various attacks.

Some particularly critical facts are:

- For the peer there's nothing to indicate the missing end-to-end S/MIME protection.
- Formerly encrypted emails will be stored unencrypted in the mailbox.
- Before an email is signed, the sender should be authenticated. However when an internal mail server is used, direct authentication is usually not possible. Instead the gateway has to trust the sender address as specified in the email.
- Even if TLS encryption is used for internal network communication, man-in-the-middle attacks are usually easy, as certificate verification errors are often ignored.
- The S/MIME gateway requires the private keys of all internal users to be able to sign and decrypt.

14.5.6-A General

On this tab you can control which operations the S/MIME gateway should perform. If you would like to enable verification and encryption, just go ahead. For these operations no prerequisites like private keys are required. However to enable signing and decryption you will have to upload S/MIME keys in menu "System > Certificate manager > Keyring" first. Then you have to add references to the keys. It depends on the application environment where the references have to be made:

You want to use domain certificates for communication with certain recipients

Domain certificates are configured by domain in menu "Modules > Mail Server > Domains".

Outbound mails are directly submitted to SX-GATE

Associate the S/MIME keys with user accounts in the SX-GATE user administration and enable user authentication in the SMTP server (menu "Modules > Mail Server > SMTP settings" on tab "Relay control").

Outbound mails are submitted to an internal mail server

Refer to the S/MIME keys on tab "Sign" and add the IP address of the internal mail server to "Trust sender address when received from". If signing should be disabled, you can add the keys on tab "Decrypt" instead.

Decrypt emails

Enable this option to automatically decrypt emails if SX-GATE has the required key and the recipient address is part of the S/MIME certificate.

Verify signed inbound emails

When enabled, SX-GATE will verify the signatures of inbound emails. In addition to checking the signature as such, this includes checking the certificate. It must be valid, issued by a trusted CA, include email signing as usage attribute and contain the email address of the sender.



Only emails which have either been retrieved from a POP server or received from an external IP address without authentication will be verified. External addresses are all IPs which are not listed below "Local IP addresses" in menu "Modules > Mail Server > SMTP settings" on tab "Relay control".

Sign outbound emails

Outbound emails will be signed when enabled and a number of conditions are met. SX-GATE will never sign emails to local recipients, i.e. emails delivered to a SX-GATE mailbox and emails forwarded to an internal mail server. Emails that have already been signed or encrypted won't be signed, too. Naturally SX-GATE can sign an email only if it has a key matching the sender address. Each key is linked to a user account and to be able to use it, the sender has to authenticate himself. If this is not possible, SX-GATE may trust the sender address as specified in the mail. Only mails SX-GATE receives from server systems which themselves authenticate the sender and make sure the sender information in the mail headers matches the authenticated user should be trusted in that way. There's an IP list where you can add these servers.



You should use this feature only in combination with the "Decrypt emails" option as you will likely receive encrypted emails as soon as you start sending signed emails.

Encrypt emails

SX-GATE will automatically encrypt emails if this option is enabled and it knows an S/MIME certificate for the recipient address. SX-GATE will never encrypt already

encrypted emails and mails delivered to local recipients, i.e. emails delivered to a SX-GATE mailbox and emails forwarded to an internal mail server.

14.5.6-B Decrypt

On this tab you can configure the email decryption process. Check the documentation of tab "General" to learn about the conditions that must be met, so that SX-GATE will decrypt an email.

Tag subject of encrypted mails with

Here you can configure how SX-GATE will tag the subject of emails it has decrypted. First the selected symbol or text will be deleted from the subject of all emails, so the status can't be forged and users can simply reply to marked emails without having to remove the tag from the subject themselves.

UTF-8 symbol ##

It depends on the mail client how the symbol is displayed. Some clients might not show the symbol at all!

Mark decrypted mails as "Confidential"

When enabled, SX-GATE will add a "Sensitivity: company-confidential" header to decrypted emails, so that some mail clients will mark the mail as "Confidential". First the header will be removed from external mails, so the status can't be forged. For internal mails however the header will be kept. If an email already contains a sensitivity header with a different value (e.g. "personal" or "private"), the header is neither deleted nor changed, so the email won't be marked as "Confidential".

S/MIME keys

In addition to any S/MIME keys configured in the user administration, the keys in this list will be used to decrypt inbound emails automatically. The email recipient must match the email address of the certificate.



After removing a key from the list SX-GATE is no longer able to decrypt emails encrypted with this key. These emails will be delivered encrypted. If the key has already been destroyed everywhere it is no longer possible to decrypt the mail.

In the transitional period after a key has been re-newed you will continue to receive mails encrypted with the old certificate for quite a while. This can even happen after the old certificate has expired. When replacing a key-pair in menu "System > Certificate manager > Keyring" the previous key-pair will be kept. The S/MIME gateway will keep using the previous key-pair for decrypting inbound mails.



Only the previous key-pair is kept, not multiple generations of it.

14.5.6-C Verify

On this tab you can configure the signature verification process. Check the documentation of tab "General" to learn more about the verification process and the conditions that must be met.

Drop correct signatures

Signatures may be deleted after successful verification. If any part of the verification process fails, the signature is always kept.

domain signatures only

If there are email communication partners with a domain certificate which is also used for signing, you should remove their signatures. Otherwise the recipient's mail program will complain that the signature doesn't correspond to the sender address.

Convert opaque signed Mails

There are two ways to sign an email: With the signature as an attachment (smime.p7s) or in a binary structure, the so called opaque signature. Some mail clients do not support opaque signed mails. They will display an empty mail with a single attachment (smime.p7m). If you are using problematic mail clients, SX-GATE can automatically convert opaque signed mails into mails with an attached signature.

Use received certificates for encryption

SX-GATE can use the certificates received as part of signatures to send encrypted mails to the peer in the future. For a certificate to become available for encryption, the signature verification process must have been passed without error or there may only be a problem with the certificate as such (expired, unknown CA, wrong key usage attributes). You can view and edit the list of currently approved certificates on tab "Encrypt".

after manual approval

In this mode the certificates will just be stored temporarily. In menu "Monitoring > Mail server" on tab "S/MIME certificates" you can view and approve the certificates for encryption.

automatic if verified without errors

If the verification process has been passed without any errors, the certificate is automatically approved for encryption. If problems occurred with the certificate, manual approval is required.

automatic

Even faulty certificates will be approved for encryption automatically.

Subject tag for signed mails sent on behalf or with domain signatures

Usually the From header contains the sender of an email. As an exception, the actual sender address is provided by the Sender header, if an email was sent on behalf of someone else. Unfortunately some email clients don't display the Sender header and so mislead the recipient into thinking that the person listed in the From header signed the message. To prevent this, SX-GATE will tag the subject with the signer's email address when the email address from the Sender header is not also part of the From header.



As Sender headers are rarely used in practice, you will hardly ever see this tag.

For domain signatures, only the sender domain and not the complete sender address can be assumed to be correct. So e.g. "*"@example.com" is used to mark a domain signature.

Tag subject of signed mails with

Here you can configure how the subject of signed emails will be tagged after SX-GATE checked the signature. First the selected symbols or text will be deleted from the subject of all emails, so the status can't be forged and users can simply reply to marked emails without having to remove the tag from the subject themselves.

UTF-8 symbols

It depends on the mail client how the symbols are displayed. Some clients might not show the symbols at all!

CA certificates

The list of trusted CA certificates can be configured here. You can also enable checking Certificate Revocations Lists (CRLs). Either only the signer's certificate is checked (leaf certificate) or the whole trust chain.

From some email communication partners you might receive signed emails which have not been signed with a purchased certificate but with certificates of their own and thus untrusted CA. SX-GATE will tag these mails with "Untrusted certificate". In order to make the certificate verification process succeed, you can import the CAs of communication partners who regularly send you email. To prevent abuse, the CA has

to be associated with individual email addresses or email domains. The CA will only be used for emails from matching senders.

After you have received the CA certificate from the peer you must upload it in menu "System > Certificate manager > CA certificates" Afterwards add a new entry to this list, associating the CA with the sender addresses.

14.5.6-D Sign

On this tab you can configure the signature process. Check the documentation of tab "General" to learn more about the conditions that must be met, so that SX-GATE will sign an email.

Trust sender address when received from

To prevent abuse, we recommend user authentication and S/MIME keys associated with user accounts for signing. If however an internal mail server is used in addition to SX-GATE, clients often can't directly login to SX-GATE. Add the IP address of the internal mail server to this list if SX-GATE can rely on the sender information (From or Sender header) of emails it receives from this server. Then configure the relevant certificates in "S/MIME keys usable without authentication".



Enable this option only if absolutely necessary. Never enter larger networks like e.g. "INTRANET". Make sure that all systems listed here can guarantee correct sender addresses.



The SX-GATE groupware, if installed, guarantees correct sender addresses and so it is trusted automatically.

S/MIME keys usable without authentication

The keys configured here may be used for signing outbound emails even though the sender didn't authenticate himself. The keys are managed in menu "System > Certificate manager > Keyring".



Please see the note below regarding certificate expiry.

The prerequisite is that SX-GATE receives the mail from an address configured in "Trust sender address when received from". The email address in the "From" or "Sender" header will then be used to find the corresponding key.



This is the typical configuration when users submit outbound mails to an internal mailserver which in turn forwards the mail to SX-GATE. If users submit outbound mails directly to SX-GATE, we recommend to add the certificates in the user administration to associate them with user accounts and use authenticated mail submission instead.

In addition to any S/MIME keys configured in the user administration, the keys in this list will also be used to decrypt inbound emails automatically. The email recipient must match the email address of the certificate.



After removing a key from the list SX-GATE is no longer able to decrypt emails encrypted with this key. These emails will be delivered encrypted. If the key has already been destroyed everywhere it is no longer possible to decrypt the mail.

In the transitional period after a key has been re-newed you will continue to receive mails encrypted with the old certificate for quite a while. This can even happen after the old certificate has expired. This is how SX-GATE supports you in the transition phase: When replacing a key-pair in menu "System > Certificate manager > Keyring" the previous key-pair will be kept. The S/MIME gateway will continue to use it for decrypting inbound mails while the new key-pair is used for both, decrypting and signing mails. So if a certificate is about to expire, please re-new it within the existing entry in the "Keyring" menu. Do not add a new entry. It is not necessary to modify the S/MIME gateway configuration.



Only the previous key-pair is kept, not multiple generations of it.

Don't sign to recipient address/domain

Mails to domains or addresses on this list will not be signed.

Subject command for "don't sign"

If the subject of an email starts with this keyword (including the square brackets), SX-GATE won't sign the mail. The keyword will be removed from the subject.



The subject may start with multiple keywords (e.g. "[NOCRYPT] [NOSIGN] ..."). Only keywords in authenticated emails and emails received from internal IP addresses will be considered and deleted.

14.5.6-E Encrypt

On this tab you can configure the encryption process. Check the documentation of tab "General" to learn more about the conditions that must be met, so that SX-GATE will encrypt an email.

Subject command for "don't encrypt"

If the subject of an email starts with this keyword (including the square brackets), SX-GATE won't encrypt the mail. The keyword will be removed from the subject.



The subject may start with multiple keywords (e.g. "[NOSIGN] [NOCRYPT] ..."). Only keywords in authenticated emails and emails received from internal IP addresses will be considered and deleted.

Subject command for "force encryption"

If the subject of an email starts with this keyword (including the square brackets), SX-GATE must encrypt the mail. The keyword will be removed from the subject. If no suitable key is available for any of the external recipients, delivery is stopped and the mail will be returned to the sender as undeliverable.



The subject may start with multiple keywords (e.g. "[NOSIGN] [CRYPT] ..."). Only keywords in authenticated emails and emails received from internal IP addresses will be considered and deleted.



Encryption is not forced for local recipients (i.e. mailbox on SX-GATE or forwarding to internal mail server).

Force encryption of mails marked as "Confidential"

Some mail clients can mark emails as "Confidential" by setting the additional mail header "Sensitivity: company-confidential". The presence of this header can instruct

SX-GATE that encryption is absolutely necessary for this mail. The header itself is deleted. If no suitable key is available for any of the external recipients, delivery is stopped and the mail will be returned to the sender as undeliverable.



The header is considered and deleted only in authenticated emails and emails received from internal IP addresses.



Encryption is not forced for local recipients (i.e. mailbox on SX-GATE or forwarding to internal mail server).

Delete expired peer certificates after

The system can perform a daily task that deletes expired recipient certificates. The recipient will then receive unencrypted mails. Therefore it is often preferable to keep using an expired certificate for a while.

Enter the number of months after which an expired certificate has to be deleted. Enter "0" to delete expired certificates immediately. Leave empty if you don't want to delete expired certificates automatically.

Edit S/MIME peers

To be able to encrypt emails, an S/MIME certificate must be known for the recipient address. You can upload certificates here, however you might prefer the more or less automatic process which is configured on tab "Verify" and allows SX-GATE to retrieve the information itself from signed emails.

A table gives you an overview of the available objects. If multiple columns are displayed you can change the sort order by clicking the column title. If there are more than 20 entries, a navigation bar will appear below the bottom right hand corner of the table. You can switch between a grouped view or a pager. The full screen mode allows you to see all entries at the same time. Pick an entry by clicking its title in the left column. A pencil icon or a trashcan in the right column allow you to rename or delete an entry. Add new objects by clicking "New Entry" below the table on the left.

Recipient email address

Please enter the email address of an external recipient. You can then upload the certificate of this recipients for automatic S/MIME encryption of emails to this address.



If the recipient is using a domain certificate, you can enter a domainname instead of an individual email address.

S/MIME certificate

State

If you should encounter problems when sending encrypted emails to a specific recipient, you can disable the certificate here.

Source

Shows you if the certificate has been uploaded by an administrator or if it was retrieved from a signed email.

14.5.7 Domains

A table gives you an overview of the available objects. If multiple columns are displayed you can change the sort order by clicking the column title. If there are more than 20 entries, a navigation bar will appear below the bottom right hand corner of the table. You can switch between a grouped view or a pager. The full screen mode allows you to see all entries at the same time. Pick an entry by clicking its title in the left column. A pencil icon or a trashcan in the right column allow you to rename or delete an entry. Add new objects by clicking "New Entry" below the table on the left.

Email domain

Please enter a recipient domain. Mails to this domain are either going to be delivered to a local mailbox on SX-GATE or forwarded to a specific (internal) mail server.

Deliver

For each individual recipient domain you can select one on the following delivery targets:

to SX-GATE mailbox

Mails addressed to a domain of this type will be delivered to a user mailbox or group of SX-GATE.

to internal mail server

Mails addressed to a domain of this type will be delivered to a user mailbox or group of SX-GATE. Select this option to forward inbound emails to a specific internal mailserver. A typical example would be an mail server in the LAN like e.g. Microsoft Exchange which hosts the user mailboxes.

to external mail server

With this option you can route outbound emails via a specific mail server. Only emails from authenticated users and local IPs as configured in menu "Modules > Mail Server > SMTP settings" on tab "Relay control" will be accepted.

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

14.5.7-A Local domain.....	505
14.5.7-B Mail server.....	506
14.5.7-C Virtual recipients.....	507
14.5.7-D Mailrouting.....	508
14.5.7-E Sender addresses.....	509
14.5.7-F Provider relay.....	509
14.5.7-G Disclaimer.....	510
14.5.7-H DKIM.....	511
14.5.7-I S/MIME.....	512

Deliver

to SX-GATE mailbox

Mails addressed to a domain of this type will be delivered to a user mailbox or group of SX-GATE.

to internal mail server

Mails addressed to a domain of this type will be delivered to a user mailbox or group of SX-GATE. Select this option to forward inbound emails to a specific internal mailserver. A typical example would be an mail server in the LAN like e.g. Microsoft Exchange which hosts the user mailboxes.

to external mail server

With this option you can route outbound emails via a specific mail server. Only emails from authenticated users and local IPs as configured in menu "Modules > Mail Server > SMTP settings" on tab "Relay control" will be accepted.

14.5.7-A Local domain

Domain type

The following types are available:

simple domain

In a simple domain, incoming mails will be delivered to users and groups as configured in SX-GATE's user administration.

extended domain

An extended domain allows you to change the recipient address before it is delivered. So you can e.g. deliver emails to info@example.com and info@example.net to different recipients.

alias domain

Select alias domain to process two local domains in exactly the same way. For distributing e.g. mails to example.net like mails to example.com, you would first add example.com as extended domain with distribution rules, then add example.net and make it an alias of example.com.

Process domain just like

Enter the new domain which is to replace the original recipient domain.

14.5.7-B Mail server

Forward emails to

SX-GATE will forward all mails with a recipient address in the currently selected domain to the mail server you enter here.

Backup server

If there is a backup system for the mail server configured above, you can fill in its address here. Then SX-GATE will forward mails to the backup whenever the primary server becomes unavailable. Leave this field empty if there is no backup.

Including subdomains

Enable to forward all subdomains as well.

Server port

If the server doesn't accept connections on standard port 25, you can fill in the required port here (usually 465 or 587).

Protocol

There's no need to change this setting unless the server requires SMTPS on a non-standard port, i.e. not on port 465.

SMTP-Auth login

If authentication with SMTP-Auth is required for using the server, you can provide the username and password in the corresponding input fields. If you leave these fields blank, authentication is disabled.



According to the standard, SMTP-Auth is a "hop-to-hop" authentication. Thus it involves only the two systems directly connected. In this case the relay server asks the SX-GATE mail server to authenticate itself and not e.g. the user who wrote the email. Therefore SX-GATE can only use one specific login for SMTP-Auth. Different credentials depending on the sender of the mail can be configured in menu "SMTP settings".

14.5.7-C Virtual recipients

Mapping of recipient addresses

Usually only the local part (i.e. the part before the "@" character) of the recipient email address is considered when delivering emails to local accounts. If the local part does not correspond to the intended recipient, you can redirect it here. As this configuration is available per domain, each domain can have a different mapping. This is particularly useful if you have multiple domains and you must deliver emails to addresses with the same local part to different recipients, depending on the actual domain. E.g. while mail to "info@example.com" is delivered to account "info" as usual, "info@example.net" could be redirected to account "info_net".



Mappings which are independent of the actual recipient domain should not be configured here, but in the user administration instead. Addressing a user in all local domains by "firstname" and also "firstname.surname" or forwarding the emails for one account to a different address are typical examples of mappings which should go into the user administration.

Insert the original recipient address along with the new destination in this list. It is also possible to refuse delivery. As destination, you can specify an arbitrary internal or external email address. If you enter a complete email address of a local recipient, including the domain part, further mappings may be applied to it. Check this screen in the corresponding domain. If you redirect to an internal address without domain, e.g. the name of a SX-GATE group or a SX-GATE mailbox, mail is delivered straight to it. Of course the configured behaviour of a group or a user's mailbox is preserved. This includes distributing an email to all members of a group or following forwarding rules of a user's mailbox.



Please make sure that no forwarding loops occur. An email address must not be forwarded to itself, neither direct nor indirect.

Delivery of all other addresses *@...

If a local recipient's address does not match any entry in one of the lists on this screen, the mail will be delivered to SX-GATE's users and groups without considering the domain part. How to process unknown recipients has been determined on tab "Local domain". With the help of this control you can determine a different default behaviour for specific domains. It will be applied to all emails with a matching recipient address which is not in the list "Mapping of recipient addresses".

As one option, SX-GATE can refuse delivery to those addresses. But it is also possible to send the respective emails to a certain internal or external email address. Here, the same rules apply as explained in the control above: If you specify an internal address including a domain, the mappings defined on this screen will be applied to the new target first. Omitting the domain part and thus specifying e.g. the name of a SX-GATE group or mailbox, the mail will be delivered directly and processed according to the configuration of the respective group or mailbox. Finally you can enter the special target "***@DOMAIN**", e.g. "***@example.com**". In this case the domain part of matching recipient address will be replaced by the specified new domain. The recipient part before the "@" character remains unaltered. Use this feature if the mapping of a previously defined domain can also be used by an other domain.



Please watch out for forwarding loops. Never forward an email address direct or indirect to itself.

14.5.7-D Mailrouting

E-Mails are usually forwarded to your provider's mail relay server or directly to the mail server of the recipient. Mailrouting allows you to determine per recipient address to which mail server SX-GATE has to forward an email.

Routing of specific recipient addresses

With entries in this area you can route emails for a specific recipient to a non-default mail server. If necessary you can also change the recipient address. You will need two entries for the same original recipient address to alter both, target server and recipient address.



Entries on this tab have precedence over entries configured on other tabs of this screen for the same recipient address.



To avoid mail loops you must make sure that the destination mail server will not forward the mail so that it eventually returns to SX-GATE.

In practice an entry here is only required if multiple mail servers keep the mailboxes for a local domain. In a typical example SX-GATE polls the provider's POP server for local emails. One user however has no access to SX-GATE and must poll the POP server himself. If a local user tries to send an email to this external user, SX-GATE would try to deliver this mail locally. An entry here allows you to forward mail for this recipient to the Internet instead.

14.5.7-E Sender addresses

Mapping of sender addresses

You can change the sender address of emails here. Each entry in the list consists of two values: the address to rewrite and the new value.



Any sender address mapping configured for the rewritten address is ignored. There's no chaining of rewrite actions.

*Rewritten sender of all other addresses *@...*

All sender addresses which don't match an entry in the list above can be rewritten to a specific sender address. If you only want to change the domain part of the sender address, regardless of the actual sender, enter `"*@DOMAIN"`, e.g. `"*@example.com"`. The local part before the `"@"` character is not modified in this case.



Any sender address mapping configured for the rewritten address or in the rewritten domain is ignored.

14.5.7-F Provider relay

Relay server for sender domain "..."

In exceptional cases it might be necessary to send outbound emails via different relay servers, depending on the sender domain.



Some emails such as disposition status notifications or non delivery reports are sent without sender address. Hence these emails will not be forwarded to a domainspecific relay, even if the original mail was related to the domain.

Relay Server port

If the relay server doesn't accept connections on standard port 25, you can fill in the required port here (usually 465 or 587).

Protocol

There's no need to change this setting unless the relay server requires SMTPS on a non-standard port, i.e. not on port 465.

SMTP-Auth login

If authentication with SMTP-Auth is required for using the relay server of your provider, you can provide the username and password in the corresponding input fields. If you leave these fields blank, authentication is disabled.



According to the standard, SMTP-Auth is a "hop-to-hop" authentication. Thus it involves only the two systems directly connected. In this case the relay server asks the SX-GATE mail server to authenticate itself and not e.g. the user who wrote the email. Therefore SX-GATE can only use one specific login for SMTP-Auth. Different credentials depending on the sender of the mail can be configured in menu "SMTP settings".

14.5.7-G Disclaimer

The boilerplate entered here will be appended to every outbound email, passing SX-GATE's mail server. The distinction between inbound and outbound email is based on the values in "Local IP addresses" from menu "Modules > Mail Server > SMTP settings" on tab "Relay control". Authenticated emails are always regarded as outbound.

Manual line-feeds can be used for a basic layout of the boilerplate. When adding the boilerplate to the contents of an HTML mail, an HTML new-line (
) will be inserted instead. In HTML mails the boilerplate is enclosed by tags. It is possible to use arbitrary HTML tags to control the layout of the boilerplate. When appending the boilerplate to a plain text email all HTML tags will be removed (passages between the characters "<" and ">").



Don't use the characters "<" and ">" in the boilerplate's text. Otherwise parts may be stripped off unintentional.

14.5.7-H DKIM

DKIM is the acronym for "DomainKeys Identified Mail" and is applied to outbound emails. A checksum is calculated, including some headers like e.g. "From", "To" and "Subject" and the actual contents of the mail. The checksum is signed and added to the mail as a header. The public key of the key-pair that has been used for signing has to be published in DNS. Recipients of the mail can then use the public key to verify that the signed parts of the mail have not been modified in transit. Furthermore the recipient can assume that the mail has indeed been sent by someone in the domain as given in the sender address.



DKIM requires a DNS entry in the respective domain.

DKIM key

Please select an RSA key, that can be added and maintained in menu "System > Keyring", to enable signing of mails in this domain. Note that it has to be a key of type "RSA key (SSH, DKIM)".



Some systems on the Internet do not yet support RSA keys with more than 2048 bit.

The key should be changed regularly (e.g. once a year). We recommend to add a new entry in the "Keyring" for the new key instead of generating a new key-pair in the existing entry.



Please note the information regarding key change in the documentation of "Name of DNS entry".

Name of DNS entry

DKIM requires a specific DNS entry in the respective domain. It consists of a selector and the text "_domainkey". The selector is an identifier of your choice that you can enter here and should correspond to a specific DKIM key.



When changing the DKIM key once a year, you could include the year number in the selector.

The selector will also be part of the DKIM header that is added to each signed email. A validating system uses the selector and the domain to retrieve the public key from DNS.

Proceed as follows change the DKIM key of a domain:

- Add a new entry of type "RSA key (SSH, DKIM)" in menu "System > Keyring". It is advisable to name the new entry so that it becomes clear that it is used for DKIM and what the corresponding selector will be called. Create the key-pair.
- Add a new DKIM entry to DNS, using a previously unused selector and of course the public key of the new key-pair you just created.
- Wait until the new DKIM entry is available on all authoritative DNS servers of your domain.
- Now select the new key-pair as "DKIM key" and at the same time change the selector in "Name of DNS entry".

Data of DNS entry

The DNS TXT record in the domain must have the value displayed here.



Depending on the administration interface of your DNS server it may be necessary to split this very long entry into multiple parts with a maximum of 255 characters each (e.g. dkim._domainkey TXT "Part1" "Part2" ... "PartX").

14.5.7-I S/MIME

The SX-GATE S/MIME-Gateway supports so-called domain certificates. Normally you would have to buy an individual S/MIME key for each and every sender address. With a domain certificate all outbound emails of one or even multiple local domains are signed with a single key and of course inbound encrypted mails are decrypted with the same key. Which at first sounds tempting has one major disadvantage: A recipient's mail client should display a clear warning whenever the sender email address is not part of the certificate which has been used for a signature.



The concept of domain certificates is not an approved standard. It is only suitable for communicating with peers that have been informed that a domain certificate is used and that have mail software which supports this concept. In practice this is only the case for peers which use an email encryption gateway themselves.

As this isn't a standardized concept anyway, you might want to issue the domain certificate yourself (e.g. using the SX-GATE CA). But of course you could also by an S/MIME certificate. If you can choose the certificate's email address freely, we recommend using an administrative contact.



Technically a domain certificate is just a normal S/MIME certificate like any other. It is just slightly misused. So you don't have to order something special when buying the certificate from a CA. For example it is not necessary to buy a department certificate which is offered by some CAs and which is more expensive than a certificate issued for a natural person.

S/MIME domain key

If SX-GATE acts as an email encryption gateway you can select the S/MIME key to be used as domain certificate to sign outbound and decrypt inbound mails here. The keys are managed in menu "System > Certificate manager > Keyring".



The domain certificate of a peer which is used to verify inbound and encrypt outbound mails has to be configured in menu "Modules > Mail Server > S/MIME gateway" on tab "Encrypt". Click "Edit S/MIME peers" and add an entry for the peer domain (e.g. "example.com").

Outbound emails with the corresponding sender domain (according to From or Sender header) will be signed with the domain certificate if the recipient is listed in "Sign mails to the following recipient addresses and domains", no individual S/MIME key is available for the sender and the email isn't already signed or encrypted.



Please be aware that it is often easy to forge the sender address. This becomes particularly relevant when emails from multiple domains with different owners or purposes are sent via SX-GATE.

Encrypted emails will be decrypted automatically if SX-GATE has the required key and the email recipient domain corresponds with the domain certificate.



After removing the key SX-GATE is no longer able to decrypt emails encrypted with this key. These emails will be delivered encrypted. If the key has already been destroyed everywhere it is no longer possible to decrypt the mail.

In the transitional period after a certificate has been re-newed you will continue to receive mails encrypted with the old key for quite a while. This can even happen after the old certificate has expired. When replacing a key-pair in menu "System > Certificate manager > Keyring" the previous key-pair will be kept. The S/MIME gateway will keep using the previous key-pair for decrypting inbound mails.



Only the previous key-pair is kept, not multiple generations of it.

Sign mails to the following recipient addresses and domains

Enter individual email addresses or complete mail domains of recipients who may receive emails signed with the domain certificate.



If the list is empty, the domain certificate will only be used for decryption, not for signing.

14.6 POP/IMAP Client

14.6.1 Settings

On this tab you can configure when SX-GATE has to poll POP or ETRN servers for new mails. If neither POP nor ETRN servers have been specified, these settings are ineffective. The same applies to POP servers with no mailboxes and ETRN servers with no domains.

Schedule

Here you can configure the time-controlled retrieval of emails.

Check for mail whenever a new PPP connection is established

If SX-GATE is connected to the Internet with a PPP dial-up link, it can automatically trigger the retrieval of mail anytime a new dial-up connection is established.



This option can help to save fees. On the other hand it is not recommended to use this option if the dial-up connection is almost permanently online. The same applies if the Internet connection is rarely used.

Deliver unknown recipients from multi-drop mailboxes to

Emails with an unknown recipient which have been collected from a multi-drop mailbox will be delivered to this address.

14.6.2 Servers

A table gives you an overview of the available objects. If multiple columns are displayed you can change the sort order by clicking the column title. If there are more than 20 entries, a navigation bar will appear below the bottom right hand corner of the table. You can switch between a grouped view or a pager. The full screen mode allows you to see all entries at the same time. Pick an entry by clicking its title in the left column. A pencil icon or a trashcan in the right column allow you to rename or delete an entry. Add new objects by clicking "New Entry" below the table on the left.

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

14.6.2-A OAuth2.....	517
14.6.2-B Mailboxes.....	519
14.6.2-C Multi-drop Parameters.....	519
14.6.2-D Multi-drop Domains.....	520
14.6.2-E Server settings.....	521
14.6.2-F ETRN.....	522

Protocol

Please select the protocol used to access this server. Ask your provider for the correct setting.

POP3

The most commonly used way to retrieve emails is by using the POP3 protocol. With POP3, emails are kept in mailboxes that can be accessed with a username and a password. You can retrieve emails from a mailbox at the provider and deliver it to a specific local user or group (single-drop). An other possibility is to retrieve the emails from a mailbox and have SX-GATE deliver it to the recipient deduced from the headers of the mail (multi-drop).

Microsoft 365 POP3 (OAUTH2)

Use this setting to retrieve mails from Microsoft 365 mailboxes with POP3.

APOP

APOP is similar to POP3, except for a different way to authenticate.

IMAP

Some POP servers use a very short connection idle timeout. Switching to IMAP might be a solution in this case.

Microsoft 365 IMAP (OAUTH2)

Use this setting to retrieve mails from Microsoft 365 mailboxes with IMAP.

ETRN (ESMTP)

ETRN is a command of the ESMTP protocol. It might be used if SX-GATE is connected to the Internet with a dial-up line using a fixed IP address. The mail server of the provider tries to forward incoming emails directly to this fixed IP address. If SX-GATE is unavailable, as e.g. the dial-up line is offline, the mail server of the provider keeps the mail in a queue. Just after the dial-up line connects again, SX-GATE used the ETRN command to trigger a new delivery attempt of all waiting mails.

14.6.2-A OAuth2

In order to retrieve mails from a Microsoft 365 account, it is necessary to use the OAuth2 authentication scheme. SX-GATE uses the "client credentials flow", i.e. comparable to a user account, an application with an application password is created for the SX-GATE mail client in Entra ID (formerly Azure Active Directory). POP3 or IMAP4 access permissions are granted to the application. Finally, using the Exchange Management Shell, the application has to be granted access to the required mailboxes. With its application ID and password, SX-GATE will then be able to get a short-lived access token, which in turn grants access to all of the configured mailboxes.

The steps in detail:

Register application

Login to Microsoft Azure with an administrator account (<https://portal.azure.com>).

Select "Microsoft Entra ID", then "Manage > App registrations".

Click "New registration" and assign a name of your choice. Leave the other settings unchanged and click "Register".

In the menu on the left, click "Certificates & secrets" and then "Client secrets". Issue a new application password by clicking "New client secret" and "Add".

Copy the generated password in column "Value" immediately by clicking the copy icon behind the password. It will no longer be possible to copy the password at a later point in time. Paste the password into the SX-GATE mail client's oauth2 configuration or temporarily store it in a safe place to paste it later into SX-GATE.

Now click "Manage > API permissions" in the menu on the left, then "Add a permission". Select "APIs my organization uses" and type "Office" into the search field. Select "Office 365 Exchange Online" and click "Application permissions". Open the sections "IMAP" and/or "POP" and check the respective "AccessAsApp" permission. Close the window with "Add permissions". Finally click "Grant admin consent for DOMAINNAME".

Now click "Overview" in the menu on the left and copy the values "Application (client) ID" and "Directory (tenant) ID" into the oauth2 configuration of the SX-GATE mail client or store the values to configure SX-GATE later.

Leave the App registration by clicking "Home" in the upper left corner.

Select "Microsoft Entra ID" again, but this time choose "Manage > Enterprise Applications". Copy the "Object ID" of the application you just registered for later use. The "Application ID" is also displayed here again. You will need both values in a moment when configuring Exchange.

Grant access in Exchange

First you should check in the "Microsoft 365 admin center" (<https://admin.microsoft.com>), if POP3 or IMAP4 access has been granted for the required users. Click each user below "Users > Active Users", then "Mail" and check the permissions below "Email apps".

Now connect with the Exchange Management-Shell. Open the Powershell and if necessary, install the ExchangeOnlineManagement module. You might have to import the module with "Import-Module ExchangeOnlineManagement".

Open the connection with "Connect-ExchangeOnline -UserPrincipalName ADMINUSER". To connect via proxy, store the proxy settings in a variable beforehand, e.g. with "\$proxyoptions = New-PSSessionOption -ProxyAccessType ieconfig". Then append the option "-PSSessionOption \$proxyoptions" to the connect command.

Register the application once using the command "New-ServicePrincipal -AppId APPLICATION_ID -ServiceId OBJECT_ID". Replace APPLICATION_ID and OBJECT_ID with the values you copied earlier.

If the application has already been registered, the command "Get-ServicePrincipal" will show you its "Object ID" (here it is called "ServiceId").

Now grant access for this ID to each user mailbox SX-GATE has to connect with: "Add-MailboxPermission -Identity USER -User OBJECT_ID -AccessRights FullAccess". Replace USER with the user's email address.

Configure credentials in SX-GATE

If you haven't done so already, paste the values you copied earlier into the OAuth2 configuration of the SX-GATE mail client.

While adding the individual user mailboxes, SX-GATE will not ask for the users' passwords, as SX-GATE can login to all the users' mailboxes with its application password.

Tenant

Enter your Entra ID tenant name or ID.

OAuth2 client ID

Enter the client ID you have registered in Entra ID for the SX-GATE mail client.

Secret OAuth2 client key

Enter the application password you have generated in the Azure Active Directory for the SX-GATE mail client.



The Azure AD application password has a limited validity period. Please remember to issue a new application password in time and copy it to SX-GATE.

14.6.2-B Mailboxes

Mailboxes

Use this control to define which mailboxes to retrieve from the selected POP server and how to process the respective emails.

To define a new mailbox you first have to fill in the corresponding credentials. You should have received them from the provider. Then you have to specify the recipient's address. If you want to define a multi-drop mailbox, you have to leave the username of the recipient empty or specify the character "*". The recipients domain defaults to "localhost", so it might not be necessary to enter anything here. By default mails are forwarded to the mail server of SX-GATE for further processing. You can however determine a different server.



Directly forwarding emails to a different mail server will bypass the security features of the SX-GATE mail server. This includes virusscanning and attachment filtering. All other features like the SPAM filter are not available as well.

14.6.2-C Multi-drop Parameters

The settings on this screen are used by multi-drop accounts only.

Check for recipient in mail header

To deduce the original recipient of an email retrieved from a multi-drop mailbox, the email headers are scanned for email addresses with the correct domain. Here you can select which header will be scanned. The default "Received" is not very reliable, however it is almost always available. Please check your emails if one of the other headers give you better results.



With "Received:" also the following headers will be checked in the listed order: "Resent-To:", "Resent-Cc:", "Resent-Bcc:", "To:", "Cc:", "Bcc:" and "Apparently-To:". The first one of these headers with a matching email address will be used.

Number of headers to skip

Usually always the first occurrence of a header is checked. If every mail contains the requested header multiple times and the first occurrence does not provide the correct value, you can determine how many of these headers have to be ignored.

Prefix to remove from recipient name

Some POP servers supply the original recipient address in one of the headers, but prefix it with a certain string. Enter this string here to have SX-GATE remove it automatically. So the mail will be delivered to the correct recipient.

14.6.2-D Multi-drop Domains

The settings on this screen are used by multi-drop accounts only.

To deduce the original recipient of an email retrieved from a multi-drop mailbox, the email headers are scanned for email addresses with the correct domain. Here you have to specify the domains to look for and how the domain information has to be forwarded.



When scanning for the domains, also any subdomain of one of the listed domains will match.



If you do not specify any domain to look for, all multi-drop emails will be delivered to the administrator.

Domains to scan for and replace by domain specified at multi-drop mailbox

If an email address with one of the domains listed here is found, only the recipients name will be used when forwarding the mail. As the domain part SX-GATE will use the value which was specified as recipient domain when adding the multi-drop mailbox.

Let's illustrate this with an example: Imagine the domain "example.org" is listed here. In an email the address "test@www.example.org" has been found. As a listed domain always matches any subdomain as well, this is indeed a hit. So "test" is deduced as the original recipient's name. Now let's assume the specification of the multi-drop account contains "*@example.com" as recipient address. Therefore the email will now be forwarded to "test@example.com".

Domains to scan for and pass on

If an email address with one of the domains listed here is found, the complete and unmodified address will be used as recipient.

Let us assume the same settings as in the example above. Only this time the domain "example.org" has been added to this list. Again the email address "test@www.example.org" is a match despite of the subdomain. However in this example the mail will be delivered to "test@www.example.org".

14.6.2-E Server settings

Port

The port SX-GATE connects with depends on the selected protocol and the option "Use encrypted port (SSL)". For POP3 either port 110 or the encrypted port 995 will be used. For IMAP it's 143 or 993. You can configure a different port here.

Use encrypted connection, verify server certificate

This setting will enforce an encrypted connection. The connection will fail if the server doesn't support encryption or the server certificate verification fails.

Use encrypted port (SSL)

Here you can activate SSL encrypted access to the mail server on TCP port 995 (POP3) or 993 (IMAP4) if this is supported by the provider.



Even if this option is disabled, SX-GATE will upgrade the connection to an encrypted one if the server indicates that it supports encryption. Port 110 (POP3) or 143 (IMAP4) is used throughout the connection.

Authentication with Certificate

In addition to password authentication, SX-GATE can identify itself to the mail server with a client certificate if the connection is encrypted. Individual certificates per mailbox are not supported yet.

Select one of the keys managed in menu System > Certificate manager > Keyring".

Don't delete messages on server

If this option is enabled, mails won't be deleted after successfully retrieving them from the POP server.



This option is intended mostly for debugging. You must not enable this option for a longer period of time, unless you can make sure that the mailboxes will be cleaned up regularly.

Retrieve new messages only

If this option is enabled, retrieved mails won't be deleted from the POP server. Messages which have been marked as seen will be ignored and kept on the POP server.

Max. number of messages per connection

With this parameter you can limit the amount of mails retrieved in a single poll. If the mailbox on the POP server contains more messages, SX-GATE will download them in the next cycles.



The POP server will delete retrieved mails at the end of the connection, provided it was terminated in a clean way. In case of an abnormal termination the mails will be retrieved and delivered again in the next cycle. So you should change this parameter carefully and only if it is absolutely necessary (default: 50).



In the worst case you can overload the system if you set this parameter to a high value!

14.6.2-F ETRN***Call ETRN for domain***

An ETRN command will be send to the respective ETRN server for each of the domains listed here.

14.7 Web proxy

This proxy is to be used by web browsers. It supports HTTP, HTTPS and FTP (download only). It listens for requests on port 8080. Please configure your web browsers accordingly unless you enabled the transparent proxy mode.

14.7.1 Settings

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

14.7.1-A Client access.....	524
14.7.1-B SX-GATE authentication.....	525
14.7.1-C NTLM authentication.....	526
14.7.1-D Windows authentication.....	527
14.7.1-E LDAP authentication.....	527
14.7.1-F Authentication options.....	529
14.7.1-G PAC file.....	530
14.7.1-H Destination ports.....	531
14.7.1-I ICAP.....	532
14.7.1-J Bandwidth limits.....	533
14.7.1-K Provider proxy.....	534
14.7.1-L Proxy selection.....	535
14.7.1-M Cache parameters.....	535
14.7.1-N Advanced.....	537

Proxy authentication

Activate this feature if you want to give Internet access only to authenticated users. The proxy has to be configured in the browser.



With transparent proxying (redirection of connections by firewall instead of browser configuration) the proxy will not require authentication.

There are multiple authentication options available:

none

Internet access via the proxy is possible without authentication. In this case you do not need to create user accounts for accessing the proxy (group "system-proxy").

by SX-GATE

This option allows Internet access only after a successful authentication. You have to assign user accounts and passwords in the SX-GATE user administration (group "system-proxy").

by Windows domain (NTLM)

Here the user's current Windows domain authentication is used to automatically authorize proxy access. Usually the user will not be prompted for a login and a password.

by LDAP server

If you select this option, Internet access is granted to those users, who can log on to an LDAP server. You don't have to add users on SX-GATE to use this authentication method.

by Windows (obsolete)

If you select this option, a user has to be able to access a certain file with his Windows username and Windows password if he want's to access the Internet. This file resided on the Primary Domain Controller (PDC) of your Windows domain. Access to this file is granted using the file access control of the PDC. You don't have to add users on SX-GATE to use this authentication method.

14.7.1-A Client access

Proxy access for source IP addresses

Use this option to grant proxy access to specific client IP addresses only.

Accept transparent proxy access

It is possible to access the SX-GATE web proxy in transparent mode. This allows the redirection of HTTP requests to port 80 of an internet web server to the web proxy. So clients can use the proxy without modification of the browser configuration. Besides enabling this option, you will have to enter an appropriate firewall rule. Please change to "Modules > Firewall > Policies" and select the interface the client is connected to. Usually this is SX-GATE's LAN interface "eth0". Enable the redirection of connections to port 80 on tab "Transp. proxy".



Transparent access is always granted without user authentication.

Select key/certificate for TLS port

To enable encrypted connections between client and proxy, please select one of the keys managed in menu "System > Certificate manager > Keyring".



The browsers have to trust the selected certificate.

The encrypted proxy port is 8443. Usually there's no option in the proxy settings of the browsers to enable encrypted connections. Instead you have to use automatic proxy configuration (PAC file, WPAD) to configure the browsers.



The PAC file served by SX-GATE is modified accordingly when the TLS port is enabled.

TLS protocol

Select the encryption strength for encrypted communication with the proxy.



The actual encryption parameters associated with each option are updated from time to time.

outdated

For compatibility with older devices, AES ciphers using the discouraged Cipher Block Chaining (CBC) and the obsolete hash SHA1 will be enabled when selecting this option. The minimum TLS version is 1.0.

compatibel

Select this option for wide compatibility with older client systems. This will enable the obsolete hash SHA1. The minimum TLS version is 1.2.

contemporary

Only halfway recent client systems will be supported when selecting this option. At least TLS 1.2 is required. It is a good choice for security. On Windows clients Internet Explorer 11, Edge or an alternative browser like Chrome or Firefox are required.

maximum

Requires TLS 1.3.

14.7.1-B SX-GATE authentication

The settings on this screen will only be effective if proxy authentication has been activated in mode "by SX-GATE".

Authentication methods

Select the accepted authentication methods.

Basic

This is the most simple authentication scheme.



In this mode the password is not protected when it is sent from the browser to the proxy. With network analysis software it is easy to decode.

Digest

Select this option to make sure that the password is always protected while in transit.

Digest + Basic

Use this setting for compatibility with clients not supporting the Digest authentication scheme. Clients which can handle both schemes will automatically prefer Digest.

14.7.1-C NTLM authentication

This screen is available only if you selected the authentication option "by Windows domain (NTLM)".

Creating user accounts in the SX-GATE group administration is not required for logging in. However, if you wish to use the URL filter, you may need to add some or all users on SX-GATE. Otherwise it would not be possible to grant individual rights to certain user groups.

Authorized users

Select which users are authorized to use the proxy.

Join Windows domain

SX-GATE needs a machine trust account in the Windows domain to be able to perform NTLM authentication. Use this wizard to set the actual domain and to create the account.

Windows domain

Creating a machine trust account requires administrator privileges. Please enter the credentials of a Windows administrator.



Once the account is created, login and password are no longer required. They will not be stored on SX-GATE.

ActiveDirectory server IP

Please enter the IP address of the ActiveDirectory server. If you want to use the NT4 compatibility mode, enter the NetBIOS name of your local Windows domain instead.



The NetBIOS domain name is for instance displayed below "Network Places" where it might be labeled "Workgroup". A NetBIOS domain name usually contains no dots (e.g. "EXAMPLE"). In contrast an active directory domain name is actually an Internet domain name. As such it contains at least one dot (e.g. "example.com").

Administrator login

Please enter the login name of a Windows administrator.

14.7.1-D Windows authentication

This screen is available only if you selected the authentication option "by Windows (obsolete)".

Creating user accounts in the SX-GATE group administration is not required for logging in. However, if you wish to use the URL filter, you may need to add some or all users on SX-GATE. Otherwise it would not be possible to grant individual rights to certain user groups.

Windows domain

Please enter your windows domain here. Furthermore you have to create a file with the name "proxyauth" on the NETLOGON share of your primary domain controller (PDC). This file must exclusively contain the word "allow". Now grant read access to all those users who should be authorised to access the Internet.

14.7.1-E LDAP authentication

This screen is only available if the authentication mode "by LDAP server" has been selected.

Creating user accounts in the SX-GATE group administration is not required for logging in. However, if you wish to use the URL filter, you may need to add some or all users

on SX-GATE. Otherwise it would not be possible to grant individual rights to certain user groups.

LDAP server

Enter the IP address or the DNS name of your LDAP server into this field.

Encrypted LDAP connection

Activate secure LDAP for encrypted communication between the proxy and the LDAP server.



Communication between browser and proxy is not encrypted. The browser transmits the user's credentials more or less in plaintext.

Type of server

Select the LDAP server type. Your choice will determine the attribute used to find a user in the LDAP directory.

other (UID)

Select this option if the login can be found as attribute "UID" in LDAP user objects. This convention is used by most LDAP servers.

MS ActiveDirectory (SAM)

If you select this option, SX-GATE will search for objects which have the login specified as "SAMAccountName" attribute. In the Microsoft ActiveDirectory, this attribute refers to the user login name for compatibility with "Windows NT 3.5x/4.0". Please be aware that the ActiveDirectory search requires read permissions. If there's no read access to a user object, it will not be possible to log on as this user.

MS ActiveDirectory (CN)

If the user object is to be identified with the "CN" attribute, select this option. In the Microsoft Active Directory, the "CN" attribute corresponds to the user object name, which immutable. Using this attribute as the user name can cause problems, since special characters and spaces are often part of the name.

Searchbase

If you want to use LDAP authentication you have to specify the searchbase required for your LDAP server. This container must contain the user objects. Two examples:

- CN=users,DC=ad,DC=example,DC=com
- OU=SBSUsers,OU=Users,OU=MyBusiness,DC=example,DC=com

Search hierarchically

Activate the hierarchical search if user objects can not only be found directly in the searchbase container, but also in containers below. Searching in the LDAP server might require specific access permissions.

Authorized users

The attribute "memberOf" in LDAP user objects can be used to restrict access to certain users. In Microsoft Active Directory, "memberOf" refers to a user's group membership. Simply enter the complete DN of the group (e.g. "CN=internet-users,CN=users,DC=ad,DC=example,DC=com"). If you leave this field empty, all users found in the LDAP searchbase will be able to authenticate themselves.

Login for LDAP search

A hierarchical search or searching for a user object with a specific "SAMAccountName" attribute requires permission to perform an anonymous LDAP search within the search path (in ActiveDirectory this involves read permission for "everyone"). If this is not possible or desired, SX-GATE must log on to the LDAP server. To do this, please enter the login for the LDAP account here.



You must state the complete distinguished name (DN) of the LDAP account (e.g. "CN=proxyuser,CN=users,DC=ad,DC=example,DC=com").

14.7.1-F Authentication options

This tab is not available if proxy authentication is off.

No authentication required for access to

Specify domain names or IP addresses, if you want to grant unauthenticated access to these destinations. The specification of a domain includes all subdomains. So if e.g. the domain "example.com" is found in the list, unauthenticated access is also possible to "www.example.com" and "ftp.example.com".



Unauthenticated proxy access to the hostname of SX-GATE and SX-GATE's eth0-IP is always granted.

Many web pages include elements from other internet domains. To completely disable authentication for a certain web page all domains used by this page have to be included in this list.

No authentication required for client

Connections from IPs from this list may use the proxy without authentication.

Deny multiple logins of the same user

This option will link a user login for 10 minutes to the source IP address of the user's last successful access. If during this period of time, the same login is used by another IP address, it may be possible that the user has forwarded his credentials. Therefore access will be blocked.

14.7.1-G PAC file

In both, the browser's proxy settings and the Active Directory group policies, you can enter the address of a proxy autoconf file (PAC file). SX-GATE's administration webserver provides a suitable file. Fill in the following URL if you want to use it: "http://<SX-GATE's LAN IP>:8000/proxy.pac".

The PAC file provided by SX-GATE makes the browser use SX-GATE's web proxy for all connections except for connections to the local host running the browser (IP 127.0.0.1 or primary IP of that host), connections to SX-GATE (LAN IP or fully qualified hostname according to "System > Setup") and connections to unqualified hostnames (i.e. plain hostnames without a domain). Use the following settings to add further exceptions.

Connection to destination domain

Use this list to configure by domain whether the browser should use the proxy or connect directly. The order of the entries is important. Note that you can as well enter individual IP addresses. However there's no DNS resolution, so this will only affect connections where an explicit IP from the list has been entered as destination in the browser.

Direct connections for networks

The browser will open direct connections to hosts with an IP address from the networks in this list. The proxy will not be used for these connections. Most of the time not an IP address but a hostname is given as a connection's target. So the browser has to lookup the IP address corresponding to each hostname using DNS queries.



If only a few individual servers are addressed by IP, you should consider entering these addresses in the list "Connection to destination domain" instead. As long as there's no entry in the list here, the browser doesn't need to query DNS servers.

Proxy address in cluster mode

Please select the proxy address advertised by master and backup in cluster mode.

Each node's individual IP

The client connects to the proxy of the cluster node that delivered the PAC file.

Common cluster IP

The client connects to the proxy of the active cluster node. In case of a failover, the IP moves to the other cluster node. This will break the connection from the client to the proxy and the client will have to establish a new one.

Master IP with fallback to Backup IP

The client prefers connections to the proxy of the master node. In case of a cluster failover the connection keeps running via master if possible. If the master proxy is not available, the client connects to the backup node.

Backup IP with fallback to Master IP

As before but preferring the backup node, so that it is used more actively.

User-defined entry

Enter a DNS name that points to the individual IPs of both cluster nodes to get loadbalancing via DNS round-robin. The proxy connection is not affected by a cluster failover. If the proxy becomes unavailable on the currently selected IP, the client will switch to the proxy on the other IP.

14.7.1-H Destination ports

Accepted destination ports for unencrypted connections

This control allows you to restrict the server ports which may be accessed via the proxy. Especially the ports 80 (HTTP) and 21 (FTP) are important here. This setting does not apply to encrypted access.

Accepted CONNECT destinations

The method CONNECT offers clients the possibility to establish connections of any type via the proxy. CONNECT is also used to tunnel encrypted connections (HTTPS) through the proxy.



Commonly it is sufficient to grant access to port 443 (HTTPS) only. Do not add unnecessary ports here, as this could be abused.



The contents of connections which have been established with the CONNECT method will not be examined by the content filter unless its option to break encrypted connections has been enabled.

Deny CONNECT to IP addresses

There is software (e.g. many peer-to-peer clients) which abuses the CONNECT method to bypass firewall restrictions. However often these clients won't request a connection to a hostname, but rather to an IP address. Enable this option to deny these connections.



You can still grant access to specific IP addresses by entering them as "Accepted CONNECT destinations".



If you access SX-GATE's configuration server by IP address via web proxy, it will probably deny further connections after enabling this feature.

14.7.1-I ICAP

SX-GATE's web proxy can query external filters with an ICAP interface.

ICAP server for request filter (REQMOD)

If the browser requests received by the web proxy have to be passed to an ICAP server, you have to fill in its name here.

Service path of request filter

Particularly if the ICAP server offers multiple services, you might have to specify the path of the requested service. You can also pass parameters to the ICAP service here.

ICAP server for response filter (RESPMOD)

If the data received from internet servers has to be processed by an ICAP server, you have to specify its name or IP address here.

Service path of response filter

Particularly if the ICAP server offers multiple services, you might have to specify the path of the requested service. You can also pass parameters to the ICAP service here.

14.7.1-J Bandwidth limits

Bandwidth limits

The bandwidth for certain requests may be limited to avoid congestion of the Internet link. Each new request is compared with the rules configured here. The bandwidth quota of the first matching rule applies.



If there's no hit at all, no limitation will occur.

Each rule consists of the following parameters:

Source IP/network

Select an IP object or enter an IP or network with corresponding netmask to limit the rule to specific source addresses. Leave empty if the rule should apply regardless of the client IP. A "*" is displayed in the table in this case.

Group

A rule can be limited to certain users by selecting a group, provided that proxy authentication is enabled. Users and groups are configured in menu "System > User administration". Select "*" and the rule will apply to any user and also to unauthenticated requests.



Active Directory groups are not yet available here.

Destination

Enter a target domain to limit the rule to requests for a specific domain or its subdomains. Select "*" if the rule should apply independent of its destination.

Bandwidth limit

Enter the bandwidth quota in kbit/s which will apply to all requests matching this rule. Simultaneous connections must share this quota.



Leave empty or use the special value "0" for unlimited bandwidth.

Maximum size of uploads

This setting limits the size of POST and PUT requests. These request types are used to transmit files or form parameters.



The limit applies to unencrypted connections only.

Maximum size of downloads

This setting limits the size of objects that can be downloaded via the proxy. In general, the addressed server informs the client in advance of the size of the download. Therefore an error message can be returned immediately. However, if the size of the requested file is not known in advance, downloading will be cancelled with no comments when the limit is reached.



The limit applies to unencrypted connections only.

14.7.1-K Provider proxy

If your provider offers a proxy server, you can configure the SX-GATE web proxy to forward requests via this proxy. If your provider operates a caching proxy server, its use can speed up Internet access. In some cases it may be mandatory to use the proxy due to the security policy of your provider.

Use proxy server of ISP

Supply the name or the IP address of the proxy in this input field. Leave the field empty if you don't want to use a provider proxy.

Port

To be able to connect to the proxy server of your ISP the corresponding port number must be specified here. Common values are 80, 3128 or 8080.

Force use of ISP proxy

If your provider operates a firewall which does not allow direct communication with the Internet, it may be necessary to handle all requests using their proxy server. Please activate the option in this case. Otherwise SX-GATE assumes a caching proxy used to speed up the Internet connection.

In this mode the SX-GATE web proxy optimises the forwarding of requests. SX-GATE will forward only those requests which might be cached to the provider's proxy. For requests that may not be cached anyway, a direct connection to the target web server will be established instead. As an example files may not be cached if user authentication is necessary to download them. Also encrypted (https) connections may not be cached.

ISP proxy login

If necessary, the SX-GATE web proxy can log on to the provider proxy. Provide the required credentials in the corresponding fields. If authentication is not required these fields should remain blank.

14.7.1-L Proxy selection

Target specific upstream proxies

If requests to particular domains or IP addresses need to be forwarded to a specific proxy, you can specify the request target and the corresponding proxy here. If a domain is given as target, its subdomains are included.

Bypass ISP proxy for access to

This area can be used to always directly access certain addresses (e.g. from the intranet). An upstream proxy or firewall that is configured at "Use proxy server of ISP" will not be used for requests to addresses stated here. The specification of a domain includes all subdomains. So if e.g. the domain "example.com" is found in the list, direct access is also used for "www.example.com" and "ftp.example.com".



Requests for the hostname of SX-GATE will always be sent direct.

14.7.1-M Cache parameters

Some notes on the caching process of the SX-GATE proxy.

Among others, objects will not be cached if

- the connection is encrypted (HTTPS)
- the web server requests authentication
- caching is forbidden by the web server
- the object's size exceeds a certain configurable threshold
- the proxy has been configured not to cache objects from the corresponding source

An already cached object will be refreshed if e.g.

- the browser reloads the page
- the object expired according to the expiration date determined by the web server

If no expiration date was specified for an object, at some point in time the proxy of SX-GATE will start to ask the web server if the object was modified since it has been cached. If yes, it will be refreshed. When SX-GATE begins to send this type of requests depends linearly on the last time the file was modified on the web server. However as an upper limit, SX-GATE will check for modifications after 7 days on FTP servers and 3 days on HTTP servers.

If the cache runs out of disk space, expired objects and the least recently used objects will be deleted.

If the browser presents outdated pages, please use the "reload" feature of your browser.



To completely reload the contents displayed by the browser you usually have to press a combination of keys (Internet Explorer: Ctrl-F5). If you still see outdated contents, please clear the cache of the browser.

RAM cache

This setting specified how much main memory (RAM) the proxy may use for caching objects. Delivery of objects stored in the RAM cache is extremely fast.

Harddisk cache

Here you can set up how much storage the proxy cache may use on the harddisk drive. The special value "0" disables the disk cache. The cache directory resides in "/var/spool/squid/".



Before you raise this value, please check the available amount of disk space on the corresponding harddisk partition.

Do not cache objects larger than

To prevent the cache from quickly filling up, files will not be cached if they exceeded a certain size. Here you can specify this size.



To be able to store a large object in the cache it is often necessary to remove lots of small objects beforehand. Therefore, if the value of this parameter is set too high, you might encounter temporary severe performance loss.

No caching for objects from

To keep SX-GATE from caching objects from certain sites you can enter the respective addresses here. The specification of a domain includes all subdomains. So if e.g. the domain "example.com" is found in the list, caching of objects from "www.example.com" and "ftp.example.com" is also disabled.



By adding a new address, objects from this site which have already been cached will not be removed.



Most browsers also use a cache to speed up Internet access. This control will not influence if or how long a browser stores objects in its cache.

Delete cache

This function will delete both, the memory and the disk cache of SX-GATE's web proxy. The proxy will be stopped for a short time and restarted with an empty cache. After this the former contents of the disk cache will be deleted in the background.



Depending on the cache size it may take several minutes to delete the old cache. You should not update or reboot SX-GATE until it is done.

14.7.1-N Advanced***Email address of administrator***

The web proxy will display the email address you configure here along with error messages presented to users.

Name of the web proxy

The web proxy will display the hostname you configure here along with error messages presented to users.

Email address for anonymous FTP login

When accessing anonymous FTP servers, the server requests an arbitrary email address as password. The address sent by the SX-GATE web proxy when accessing such a server can be determined here.

14.7.2 URL filter

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

14.7.2-A Policy.....	538
14.7.2-B Options.....	540
14.7.2-C Database.....	541

The URL filter checks the URL of every browser request. The reply of the webserver will not be checked. This is the task of the web proxy component Content filter.

URL filter enabled

This switch is used to enable the URL filter. It is used to restrict access to certain Internet addresses.

14.7.2-A Policy

User groups

Please select the source of the user groups used in the policy below.



If proxy authentication is disabled or if the ruleset doesn't refer to user groups, this setting has no relevance.

from SX-GATE user administration

User groups are configured in the SX-GATE menu "System > User administration".

from Windows domain

For this setting SX-GATE requires a computer account in the Windows domain. You can create a computer account when "Proxy authentication" is set to "by Windows domain (NTLM)" in menu "Modules > Web proxy > Settings".



In the windows domain the groups must be created as security groups. Only direct user members of these groups will be considered. So nested groups are not supported.



If users are added or removed from a group in the windows domain it will take up to 15 minutes until SX-GATE reflects those changes.

URL filter policy

The URL filter tests each client request, whether it is acceptable or must be denied, by successively evaluating the rules configured on this screen. If a requests fulfills all preconditions of a rule (time, source IP, user) the requested URL is looked up in the URL filter list the rule references. In case of a hit, access is either granted or denied with a message as specified by the rule. No further rules will be evaluated. If however there's no match, evaluation continues with the next rule.



If there's no hit at all, access will be granted.

Each rule consists of the following parameters:

Active

You can switch a rule on and off.

Period

A rule may be enabled only for certain periods of time. Configure periods in menu "Definitions > Periods". A rule can be valid either within or outside the selected period.

Source IP/network

Select an IP object or enter an IP or network with corresponding netmask to limit the rule to specific source addresses. Leave empty if the rule should apply regardless of the client IP. A "*" is displayed in the table in this case.

Group

A rule can be limited to certain users by selecting a group, provided that proxy authentication is enabled. Users and groups are configured in menu "System > User administration". Select "*" and the rule will apply to any user and also to unauthenticated requests.

Policy

This setting determines whether a request is accepted or denied if the rule matches.

Filter list

The requested URL is looked up in the selected URL filter list. Configure the lists in menu "Definitions > URL filter lists". The ruleset is easier to understand if you use descriptive names for the filter lists. Select "*" if the rule should apply to any URL.



At least two rules are necessary to grant access to approved URLs only. The first rule references an URL filter list with the allowed target. The second rule denies access to any URL (Filter list "*").

14.7.2-B Options

Proxy tunnel detection

This option activates checks for tunneled connections (https) that try to bypass local security guidelines.



This option is only active for requests that have the category "Proxy server" blocked.

Reverse lookup IP addresses

If this option is on a reverse lookup will be done for IP addresses to find the matching DNS name. This will prevent that blocked URLs are accessible by using IP addresses in a browser's address bar.

Message "Access denied"

Except for requests denied by database category "Advertising", an error is reported to the browser if the URL filter denies access. For an encrypted connection this is just an error code and a browser depending message will be displayed to the user. For unencrypted connections or if the proxy option to break and inspect encrypted connections is enabled, the proxy can deliver an error message to the user. There are several different options for this message.

Simple

If this option is selected, only a brief message indicating that access is denied will be shown.

Detailed

To get more detailed information you can select this option. This includes e.g. the information if access has been denied due to a blocked filename extension or it will give you the database category associated with a forbidden domain.

Detailed with logging

Extends the previous option with logging of blocked requests.

Custom URL:

It is even possible to use a custom forbidden message. Enter a complete web server URL (e.g. <http://www.example.com/forbidden.html>) which is to be displayed whenever a request is denied.



In the web browser the URL specified here will be shown in the context of the denied address. So you will have to use absolute URLs (including <http://> and the server name or IP) if the custom message refers to other objects like e.g. images or contains links.

14.7.2-C Database

Use database:

You can choose from two databases:

free available

This database is a compilation from several lists, freely available on the Internet. It covers only a fraction of all existing sites and may include wrong entries as well.



The free database probably fails to meet higher demands as e.g. required by educational organizations.

commercial

You need to purchase a license to use this commercial database. Please contact your SX-GATE dealer.

Update daily at

This database can be updated daily. Please enter the time when you want to update. Leave this field empty to disable automatic updates.



To use the commercial database you need a valid login and password!

Upload uncategorized URLs

By activating this feature all accessed web sites that are not included the URL filter database are sent to the software producer to improve the quality of the database.

Privacy is guaranteed since no identification of client, source or user is included, just the domain name is registered for categorization.

Additionally some data is submitted for statistical evaluation:

- Information on used hardware and operating system (e.g.. i686, number of processors, Linux 2.6.32.28)
- Hostname (e.g. router)
- Number of unique IPs querying the URL filter module.
- Number of queries.
- Number of HTTPS queries.
- Number of found tunnels.
- Number of blocked queries.
- A counter telling the number of adult content blocked in web search engine results.



This feature can only be used if you don't use a parent proxy!

Update database now

Press this button to immediately update the database.

14.7.3 Content filter

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

14.7.3-A General.....	543
14.7.3-B Virusscan.....	544
14.7.3-C Tag filter.....	546
14.7.3-D Tag filter whitelist.....	547
14.7.3-E Content type filter.....	548
14.7.3-F SSL filter.....	548

Content filter

Here you can activate the content filter which provides virusscan, tag filtering and SSL filtering.



The virusscanning option relies on an actual virusscanner. The virusscanner licenses are not included with SX-GATE and must be purchased separately. Further information about supported or already installed scanners can be found in the menu "Modules > Virusscanner". This is also where you would install a virusscanner engine or its license key.

14.7.3-A General

Verify content type

Web server responses usually declare the file type in the HTTP header. Misconfigured or malicious web servers provide generic or false content types.

By using this setting SX-GATE tries to find the real file type by looking at the first bytes of each transferred file.



Activating this option may increase the number of files to scan for viruses dramatically and thus the system's load!

Bypass on port 8081/8444

With content filtering enabled, actually two chained proxies run on SX-GATE. The content filter proxy accepts connections on TCP ports 8080 and 8443 and forwards them to the proxy cache on port 8081. By default direct connections to port 8081 will not be accepted. Enable this option and configure a client to use proxy port 8081 or 8444 to always bypass the content filter (virusscanning, tagfiltering, ...). To be able to bypass the content filter also for transparently proxied connections, this option also enables the ports 8083 (HTTP) and 8446 (HTTPS).



This option should only be enabled for compatibility with older SX-GATE releases. If some applications do not cooperate with the virusscan proxy, you should add appropriate entries at "Trusted servers (incl. subdomains)".

Trusted servers (incl. subdomains)

Content filtering can affect the functionality of certain web sites. In this table you can disable the content filter for individual domains completely or, by setting individual checkboxes, enable only some subcomponents of the filter. Entries always include all subdomains. More specific entries like e.g. "www.example.com" have precedence over more general entries like e.g. "example.com".



If virusscan or the option "Verify content type" is enabled, the content filter will modify requests to download only parts of a file, so that always complete files are downloaded. In particular some software updaters always expect partial content, even though the reply indicates that the complete file is served. If you encounter problems, please disable the named components for the affected server.



If the component "Tag filter" or "Verify content type" is enabled, requests will be modified to prevent automatic compression of contents.

Virusscan

The status screens of the virusscanning module can cause problems with some client software. Especially programs which automatically download files (e.g. to update software components) can be affected. You can either disable the status messages or the virusscan as a whole.

Tag filter

If the tag filter is active, some web sites can become unusable. Disable tag filtering for problematic sites by adding them to the list without checking the tag filter checkbox.

Content-Type

If this switch is not checked, both, "Verify content type" and "Content type filter", are disabled for the given server.

Break SSL

For privacy reasons you might want to exclude some servers when breaking SSL connections.

SSL checks

Define an exception if one of the SSL checks fails for a certain server.

14.7.3-B Virusscan

Do not scan documents of content type

In this control you can specify a list of content types. Corresponding documents will not be scanned for viruses. To add an entry use the format "maintype/subtype", where an asterisk (*) can be stated as the maintype or the subtype to match any value (e.g. "image/*" for any image format). If the content type of a requested document is not in this list, the file will be passed to the virusscanner before it is delivered to the client.



If you want to use the tag filter only and thus want to completely deactivate the virus scanner, please add the content type `"*/*"`.



Scanning all content types is possible, however it can result in severe system overload. It is vital to limit the parameter "Number of concurrent virus scanner processes" in this case. Furthermore it is not advisable to scan endless data streams. These may occur especially with audio and video data types (`"audio/*"` and `"video/*"`).

This component will scan only those files which have been downloaded via the virusscanning proxy of SX-GATE. The virusscanning proxy has to be enabled. It is not possible to scan the contents of encrypted connections, unless the option to break SSL connections has been enabled.



Microsoft Internet explorer users from version 5 and above can use the function "copy to folder" when clicking the right mouse button while pointing to an FTP link. This will initiate a direct FTP download, bypassing the web proxy. If direct FTP access has been allowed in the firewall, the corresponding downloads will not be scanned for viruses! However, if direct FTP access is not permitted in the firewall, downloads using this feature will fail.

Forward password protected files unscanned

This configures how password protected files are handled. By default they will be blocked and temporarily stored in a quarantine folder. If this option is enabled these files will be delivered to the client without scanning for viruses.

Special handling if file size exceeds

Files that exceed 2GB in size can't be handled by the virus scanners. You are able to lower this limit here. There is a special treatment for files which exceed this limit. Take a look at the following parameter.

Larger downloads will be

Choose how to proceed with larger files.



Downloads from servers in the "Trusted servers (incl. subdomains)" list will be accepted anyway.

Number of concurrent virus scanner processes

You can limit the number of concurrently running virus scanners using this control. This will protect the system from overload caused by lots of scanners running in parallel.



A typical example of use is scanning all images for viruses (data types "image/*"). Opening a typical web page usually involves opening and scanning several images at the same time. A missing limit can cause system overload.

14.7.3-C Tag filter

Check documents of content type

To remove potentially dangerous tags from HTML documents you can specify in the following list which file types should be scanned. Specify entries using the format "maintype/subtype", where an asterisk (*) can be stated as the maintype or the subtype to match any value (e.g. "*/html"). If a document corresponds to one of the content types listed here, it will be edited by the tag filter.

This component will scan only those files which have been downloaded via the virusscanning proxy of SX-GATE. The virusscanning proxy has to be enabled. It is not possible to scan the contents of encrypted connections, unless the option to break SSL connections has been enabled.

Hide SCRIPT tag and script handlers

Activate this switch to defang the tag "<script>" as well as script handlers like "onLoad" or "onClick". This will partly prevent the execution of script languages like JavaScript and VBScript.



This feature will turn many web sites unusable.

Hide APPLET tag

Activate this switch to defang the tag "<applet>". This tag is used to call Java Applets.

Hide EMBED tag

Activate this switch to defang the tag "<embed>". This tag is used to e.g. include plugins.

Hide OBJECT tag

Activate this switch to defang the tag "<object>". This tag is used to e.g. execute Java Applets, ActiveX controls and plugins.

14.7.3-D Tag filter whitelist**Permitted applications**

With "Trusted servers (incl. subdomains)" on tab "General" you can disable filtering for specific servers. The list "Permitted applications" in contrast allows you to permit specific applications. How an application is identified depends on the HTML tag used to include it. You will have to examine the HTML source of the web page to find the required values for whitelisting an application.



Keep in mind that the tag filter replaces the first letter of a filtered tag by an exclamation mark. To find filtered object, embed or applet tags, you will have to look for "!bject", "!mbed" or "!pplet", respectively.

You can append the following values to the list:

Class IDs

Class IDs can be found in object tags' "classid" attributes. It consists of the string "clsid:" followed by a structured combination of digits and letters. The following example is used to include Adobe Flash:

```
<object classid="clsid:d27cdb6e-ae6d-11cf-96b8-444553540000">
```

To accept this application, add "clsid:d27cdb6e-ae6d-11cf-96b8-444553540000" to the list.



If the object tag also contains a "type" attribute, its value has to be added, too (see content type below).

Content type

Content types are given in the "type" attribute of object and embed tags. Examples are

```
<object type="application/x-shockwave-flash">
```

and

```
<embed type="application/x-shockwave-flash">
```

To accept both cases, "application/x-shockwave-flash" must be included in the list.



If the object tag also contains a "classid" attribute, the class ID has to be accepted, too (see above). If there's no "type" attribute in an embed tag, there's unfortunately no way to whitelist it here.

Java classes

Applies to object and applet tags. If an object tag is used to include Java, you need to check the "classid" attribute. It should look like this:

```
<object classid="java:test.class">
```

. To accept this applet, add "java:test.class". For whitelisting an applet tag, please append the contents of the "code" attribute to the string "java:". If for example the tag reads

```
<applet code="test.class">
```

, you would have to enter "java:test.class".

14.7.3-E Content type filter

Block documents with content type

In this control you can specify a list of content types. Corresponding documents will be filtered by the proxy. To add an entry use the format "maintype/subtype", where an asterisk (*) can be stated as the maintype or the subtype to match any value (e.g. "video/*" for any video format).

This component will scan only those files which have been downloaded via the virusscanning proxy of SX-GATE. The virusscanning proxy has to be enabled. It is not possible to scan the contents of encrypted connections, unless the option to break SSL connections has been enabled.

14.7.3-F SSL filter

SSL check for CONNECT method

For encrypted communication, browsers use the CONNECT method to request a connection to the target server. The payload of such connections won't be filtered, as it is expected to be encrypted. Some applications use this loophole to bypass the firewall. The SSL check, when enabled, makes sure that at least only encrypted connections are accepted.



With "Break SSL" enabled, this option only applies if SSL breaking has been disabled for a certain domain but SSL checks are still enabled. On the other hand, for breaking an SSL connection, it must always be encrypted. Furthermore HTTP must be spoken inside.

Break SSL

Normally it is not possible to examine the contents of encrypted connections. This does not necessarily apply to SX-GATE's virusscan proxy. It is able to split connections into one encrypted connection between browser and proxy and an other encrypted connection between proxy and web server on the Internet. In this case the proxy will present a self-created certificate to the client, which resembles the original. It is signed by the Certificate Authority from menu "System > Certificate manager > CA certificates", below "SX-GATE CA" on tab "SSL proxy CA". There, you can also download the public key which should be installed on all client browsers. Otherwise users will be prompted to accept the certificate once for each server they want to access.



Connections to server listed on tab "General" in "Trusted servers (incl. subdomains)" will not be broken open.

TLS protocol (internal)

Select the encryption strength for encrypted communication of browsers with the proxy. If the encrypted web proxy port is enabled, you can configure this setting in menu "Modules > Web proxy > Settings".



The actual encryption parameters associated with each option are updated from time to time.

outdated

For compatibility with outdated devices, AES ciphers using the discouraged Cipher Block Chaining (CBC) and the obsolete hash SHA1 will be enabled when selecting this option. The minimum TLS version is 1.0.

compatibel

Select this option for wide compatibility with older client systems. This will enable the obsolete hash SHA1. The minimum TLS version is 1.2.

contemporary

Only halfway recent client systems will be supported when selecting this option. At least TLS 1.2 is required. It is a good choice for security. On Windows clients

Internet Explorer 11, Edge or an alternative browser like Chrome or Firefox are required.

maximum

Requires TLS 1.3.

TLS protocol (external)

Select the encryption strength for encrypted communication of the proxy with web servers.



The actual encryption parameters associated with each option are updated from time to time.

outdated

For compatibility with outdated servers, AES ciphers using the discouraged Cipher Block Chaining (CBC) and the obsolete hash SHA1 will be enabled when selecting this option. The minimum TLS version is 1.0.

compatibel

Select this option for wide compatibility with older servers. This will enable the obsolete hash SHA1. The minimum TLS version is 1.2.

contemporary

Only halfway recent client systems will be supported when selecting this option. At least TLS 1.2 is required. It is a good choice for security. On Windows clients Internet Explorer 11, Edge or an alternative browser like Chrome or Firefox are required.

Trusted CAs

Web server certificates must have been issued by one of the CAs listed here in order to be verified successfully.

Block unknown CA

What should the proxy do when it encounters a server certificate which is either self-signed or has been issued by a CA which is unknown to SX-GATE? When disabled, the proxy will issue a self-signed certificate for the server, so the browser will show a warning and the user has to decide if he wants to trust the connection or not. When enabled, SX-GATE will deny the connection without prompting the user.

Block expired certificates

When enabled, server certificates beyond its validity period will be blocked by the proxy. Otherwise the user's web client will show a warning and the user is prompted to choose whether to accept or refuse the connection.

Block unmatched servernames

When enabled, access to servers is only allowed if the server's name is listed in the certificate. Otherwise the user's web client will show a warning and the user is prompted to choose whether to accept or refuse the connection.

Verify revocation status of certificates by using OCSP

no

OCSP will not be used to check revocation status of certificates.

yes, accept OSCP errors

Revocation status of certificates will be checked using OCSP. Only revoked certificates will block connections.

yes, block on errors

Revocation status of certificates will be checked using OCSP. In addition to revoked certificates connections will also be blocked if query errors (like connecting failure to the OCSP responder) occur.

Show detailed error message when blocked by URL filter

With this option you can control how the proxy handles SSL connections to domains the URL filter blocks completely.



A detailed error message is always displayed if the URL filter doesn't block the whole domain but just individual files or subdirectories.

If the option is disabled, the proxy will reject the SSL connection as a whole. The proxy won't open a connection to the Internet in this case. On the other hand it is not possible to display a proper error message in the browser. The browser will show a generic error message, indicating that the proxy refused the connection.

If you enable the option, an SSL connection to the destination host will be opened. Each request however will be rejected by the proxy with the message configured in the URL filter options. So the destination host will see an SSL connection but won't receive any requests via the connection.

14.8 Reverse proxy

The reverse proxy provides internet access to local web servers. Security is the primary concern for access to web servers in the LAN. For DMZ web servers the reverse proxy can act as a load balancer. The reverse proxy accepts HTTP and HTTPS connections. The backends can also be contacted using either HTTP or HTTPS.

14.8.1 Settings

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

14.8.1-A Filter.....	552
14.8.1-B WAF.....	553
14.8.1-C WAF rules.....	554

14.8.1-A Filter

If a web application turns out to be vulnerable but no update is available yet, it might be handy to block certain requests. The rules on this page affect all requests processed by the reverse proxy.

Blocked URLs

The patterns configured here are applied to the URL path including URL parameters (i.e. everything after the server name) and are case insensitive. If the pattern starts/ends with a letter or digit, the pattern matches only if the pattern is found at the beginning/end of a word or URL component (path, filename, parameter name, ...). So e.g. the pattern "pace" won't match "/spaces/" but will match "/pace/" or "/list?q=pace". The special character "*" serves as a wildcard for an arbitrary amount of arbitrary characters. So "*pace*" will match "/spaces/". A "+" is either a plus or a space character.



%-encoded characters in the URL will be converted beforehand.

Blocked headers

The reverse proxy will catch requests that include one of the headers blocked here. If a header name is specified, the pattern is looked up in the value of this header.



If no header is specified ("*") the pattern is applied to all headers including the header names.

The search is case insensitive. If the pattern starts/ends with a letter or digit, the pattern matches only if the pattern is found at the beginning/end of a word. The special character "*" serves as a wildcard for an arbitrary amount of arbitrary characters. A "+" is either a plus or a space character.

14.8.1-B WAF

The web application firewall (WAF) checks client requests for compliance with the standards, unusual properties and known attacks. Potentially unwanted requests are rejected.



Signatures are updated as part of the SX-GATE updates.

Web application firewall

Enable the WAF here. Expect false alerts, so please keep an eye on the corresponding log "Reverse proxy WAF "and configure exceptions for problematic rules. Expect more false alerts when using the extended ruleset.

Exceptions for rules

Enter the IDs of rules you want to disable. Check the Log "Reverse proxy WAF" for alerts and the corresponding rule IDs.

If you select "*" (completely)" as "Target", the rule will be disabled completely. For some alerts it is possible to disable the rule just partially. Select the corresponding entry from the list to disable the rule just when checking parameters (ARGS), cookies or headers. Even more specific, by entering a "Name" the rule is disabled just when checking the parameter, cookie or header with that name.



If "Target" is set to "*" (completely)", "Name" has no meaning.

14.8.1-C WAF rules

Depending on the technologies used on your webserver, you can enable additional rules here.

For a few application you can also enable exception rules, disabling problematic rules for specific URLs.

14.8.2 Ports

A table gives you an overview of the available objects. If multiple columns are displayed you can change the sort order by clicking the column title. If there are more than 20 entries, a navigation bar will appear below the bottom right hand corner of the table. You can switch between a grouped view or a pager. The full screen mode allows you to see all entries at the same time. Pick an entry by clicking its title in the left column. A pencil icon or a trashcan in the right column allow you to rename or delete an entry. Add new objects by clicking "New Entry" below the table on the left.

Reverse proxy port

The proxy will listen for requests on the port specified here.



Access to the selected port still has to be granted in SX-GATE's firewall configuration.



For unencrypted access you might want to configure the HTTP standard port 80. Possibly this port is already in use. Please check in menu "System > Services" on tab "Server" if the service "HTTP server" is enabled. If this is the case, port 80 can not be used by the reverse proxy. Use a different, unused port like e.g. 8888. If nevertheless requests should be sent to port 80 you can configure DNAT rules in the firewall configuration which redirect requests for port 80 to the reverse proxy port.

Connection

Select the kind of connections expected on this port.

encrypted (https://)

Clients connecting to the SX-GATE are required to use a SSL/TLS encrypted communication.

authenticated (https://)

With this setting the clients are required to authenticate themselves with a certificate issued by SX-GATE's CA.

plaintext (http://)

Communication between clients and SX-GATE is unencrypted.

14.8.2.1

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

14.8.2.1-A General.....	555
14.8.2.1-B Certificate.....	558
14.8.2.1-C Trusted CA.....	558

Connection

Select the kind of connections expected on this port.

authenticated (https://)

With this setting the clients are required to authenticate themselves with a certificate issued by SX-GATE's CA.

14.8.2.1-A General

The reverse proxy can be used in two different ways. As a mediator which forwards requests to internal web servers and as a load balancer distributing requests in front of a server farm.

The settings on this screen control how the reverse proxy can be reached from the Internet and the restrictions to impose on requests. To configure the backend servers which deliver the actual contents, please open the menu tree by clicking on the plus sign. There you can define a set of backend servers per hostname (virtual hosting). Requests to hostnames without dedicated entry will be rejected or distributed according to the rules of the special entry "*".

Message for authentication popup

Upon request the reverse proxy will ask for a login before it forwards requests to certain backends. Only members of SX-GATE group "system-proxy" will be accepted. Web browsers usually open a small popup windows, asking for login and password. Among other things, the popup will display the message you enter here. It should indicate the authentication's purpose to the user.



You should however avoid to draw the attention of criminals on the system by being too specific.

Check syntax of requests

Enabling this option enhances the security. Every requested URL will be validated if it complies with the standard. Access will be denied if the URL contains invalid characters or the order of its components is not correct.

permissive

A lot of non standard-compliant characters will be accepted as part of an URL when selecting this option. Choose it as a last resort if the more restrictive options do not work for you. If access to the backend is still denied you will have to disable the syntax check.

Microsoft optimized

Some violations of the standard have to be accepted to provide access to Microsoft's Outlook Web App (OWA). Problems in very specific cases might occur nevertheless.

strict

With this option, the verification conforms broadly to RFC2396.

Accept extended HTTP commands

By default only the HTTP methods "GET", "POST" and "HEAD" will be accepted by the reverse proxy. Enable this option if "PUT" and all the WebDAV methods have to be supported, too.



This option is required for access to Microsofts Outlook Web App (OWA), Outlook Anywhere or a remotedesktop gateway.

Maximum size of uploads

This parameter defines an upper limit for the request size. The total size of form parameters or files transmitted with e.g. the "POST" and "PUT" methods must not exceed this limit. Leave blank to impose no limit.

TLS protocol

Select the encryption strength. For serving uncritical contents to the public you should pick a lower value for maximum browser compatibility. Select a high value when providing services to a closed user group.



The actual encryption parameters associated with each option are updated from time to time.

outdated

Use this setting to enable the obsolete hash SHA1. The minimum TLS version is 1.0.

compatibel

Select this option for wide compatibility with older client systems. This will enable the obsolete hash SHA1. The minimum TLS version is 1.2.

contemporary

Only halfway recent client systems will be supported when selecting this option. At least TLS 1.2 is required. It is a good choice for security. On Windows clients Internet Explorer 11, Edge or an alternative browser like Chrome or Firefox are required.

maximum

Requires TLS 1.3. Currently this option only makes sense for closed user groups. Make sure that all clients support TLS 1.3 before selecting this option.

Instruct browser to always use a secure connection for all domains

With this setting you can enable HTTP Strict Transport Security. The browser is told to always use encryption when connecting with the respective host name. In addition the user will no longer be able to override invalid certificate warnings. These restrictions apply after the first visit of the browser and are meant to counteract man-in-the-middle attacks. However this feature is not supported by all browsers.



The browser restrictions will affect any virtual hostname the browser used to address this reverse proxy port. You must not enable this feature if you need to access a web services running on the same hostname which is not using encryption.

The browser will enforce the secure connection for the number of days configured. The special value "0" can be used to clear this setting ahead of time, but this of course requires the browser to visit the site again without facing any certificate related problems. Leave empty if the reverse proxy shall not insert a Strict Transport Security option.



In production use you should configure a value in the range of several months. High values improve the clients security but on the other hand require a foresighted administrator.

14.8.2.1-B Certificate

This certificate is needed for encrypted access to the reverse proxy of SX-GATE.

Select key/certificate

Please select one of the keys managed in menu "System > Certificate manager > Keyring".

14.8.2.1-C Trusted CA

Configure the certificate authority (CA) used to authenticate the clients.

Trusted CA

Please select the CA.

Import trusted CA

Select CA certificate file

Now the certificate chain must be added to the certificate. This may include one or more intermediate CAs. The chain ends with the root CA. All certificates must be in PEM format. Please ask your CA for the required certificates.

Appended CA certificate

The uploaded certificate is appended to the certificate chain.

Please read on at [Select CA certificate file](#)

Please read on at [Install CA certificate](#)

Install CA certificate

The import procedure is complete. The new certificate is now ready to be installed.

Import certificate revocation list

Here you can install the recent certificate revocation list (CRL) of the trusted CA. A CRL offer the possibility to invalidate a certificate already before it expires. This is useful if for example an employee leaves the company and access has to be denied. Please import the CRL file in PEM format.



The CRL must have been issued by the trusted CA. Otherwise it is not considered.

Delete certificate revocation list

Here you can delete the certificate revocation list. Formerly invalidated certificates will then be accepted again.

14.8.2.2 - Virtual hosts

A table gives you an overview of the available objects. If multiple columns are displayed you can change the sort order by clicking the column title. If there are more than 20 entries, a navigation bar will appear below the bottom right hand corner of the table. You can switch between a grouped view or a pager. The full screen mode allows you to see all entries at the same time. Pick an entry by clicking its title in the left column. A pencil icon or a trashcan in the right column allow you to rename or delete an entry. Add new objects by clicking "New Entry" below the table on the left.

Server name (virtual host)

The requests sent by a web browser usually contain the name of the addressed server in the host header. You can restrict access to certain backends to requests which contain a specific host header value. Enter a DNS name or an IP of SX-GATE which is valid in the Internet and the reverse proxy will forward only those requests with the correct host header to corresponding backends.



It is easy to forge the host header. So you must never use virtual hosts to forward requests from different security zones (e.g. LAN and Internet) to different backend servers. Configure one reverse proxy port per security zone instead and use firewall DNAT rules to redirect requests from the various security zones to the corresponding reverse proxy port.

Leave blank to define a virtual host for requests without or with a different host header. This will create an entry labeled "*".



If there is no virtual host "*" or no suitable backend is enabled in virtual host "*", requests with no proper host header will be rejected. This makes unauthorized access more difficult.

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

14.8.2.2-A Microsoft IIS services.....	560
14.8.2.2-B SX-GATE services.....	562
14.8.2.2-C Backend servers.....	564
14.8.2.2-D Connection parameters.....	567
14.8.2.2-E Load balancing.....	568

14.8.2.2-A Microsoft IIS services

The reverse proxy includes optimized settings for access to selected services offered by a Microsoft IIS server. The proxy makes sure that only the required paths on IIS are accessible from the Internet.

Remotedesktop gateway

Enter the IP address of the Microsoft Internet Information Server (IIS), acting as a remotedesktop gateway. The reverse proxy will use HTTPS to connect with IIS. In IIS the RPC proxy service must be configured in path "/rpc". Leave empty if you don't want to publish a remotedesktop gateway service.



To our knowledge, reverse proxy authentication using client certificates is not supported by Microsoft's terminalserver client.

Access to RD Web Access

Enable this option to grant access to Remotedesktop Web Access (RDWEB). This includes the following path: "/rdweb", "/remoteDesktopGateway" und "/KdcProxy".



To access RDWEB with a browser you have to append the corresponding base path to the URL (e.g. <https://www.example.com/rdweb>).



This option won't take effect unless a Remotedesktop gateway is configured.

Exchange services: internal protocol

To enable access to Exchange services, please select the protocol for the connection between SX-GATE and Exchange/IIS first. If you opt for unencrypted HTTP, remember to enable SSL offloading in the Exchange server configuration.



Please take account of Microsoft's technical specifications. As a backend server, IIS must internally be running on port 443 (encrypted) or 80 (no encryption). External clients must contact SX-GATE's reverse proxy on port 443 (encrypted).

IIS running Exchange services

Enter the IP address of the Microsoft Internet Information Server (ISS) offering Exchange services.

Access to OWA

Enable this option to grant access to Outlook Web App (OWA). This includes the following paths: "/owa", "/exchange", "/exchweb", "/public" and "/oab".



To access OWA with a browser you have to append the corresponding base path to the URL (e.g. <https://www.example.com/owa>).

Access to Exchange Admin Center / Control Panel

Enable this option to grant access to Exchange Admin Center (EAC), formerly known as Exchange Control Panel (ECP). This grants access to the path "/ecp".



To access EAC / ECP with a browser you have to append the corresponding base path to the URL (e.g. <https://www.example.com/ecp>).

Access with Exchange Active Sync (EAS)

Particularly mobile devices use the ActiveSync protocol to connect with Exchange. This option enables access to IIS path "/Microsoft-Server-ActiveSync".

Access with RPC/Outlook Anywhere

This option enables Outlook to establish an HTTPS tunnel to Exchange. In IIS the RPC proxy service must be configured in path "/rpc". In newer Exchange and Outlook releases the MAPI-over-HTTP will be used instead.



Before you try with Outlook, make sure the HTTPS connection can be established without any warnings. Point the web browser of the Outlook PC to the Reverse Proxy. The certificate must not be expired, it has to present the correct server name and it must have been issued by a certificate authority the Outlook PC trusts.



To our knowledge, reverse proxy authentication using client certificates is not supported by Outlook.

Access with MAPI-over-HTTP

Outlook clients starting with 2010 SP2, 2013 SP1 and 2016 can connect with Exchange servers running at least version 2013 SP1 or 2016 using MAPI-over-HTTP. The corresponding virtual directory on IIS is "/mapi".

Access to Exchange Web Services

This is the modern interface to access Exchange. It's used for example by Outlook 2011 for Mac. The reverse proxy will forward to various files below "/ews/".

Client setup using autodiscover

This option grants access to Exchange's autodiscover feature (various files in directory "/autodiscover/"). It makes configuring external Outlook and ActiveSync clients easy.

For the domain "example.com" the client would first try to find the autodiscover server at "example.com", then "autodiscover.example.com". Finally the client would lookup a DNS entry of type "SRV" for the domain "_autodiscover._tcp.example.com". The entry must refer to port 443 and the DNS name of SX-GATE (e.g. "owa.example.com"). The advantage of the SRV entry is that no additional hostname is required in the certificate. So a cheap certificate is usually sufficient.

14.8.2.2-B SX-GATE services

The reverse proxy is required to access SX-GATE extensions (apps). It's also possible to access the SX-GATE administration interface via reverse proxy. This allows you to restrict access to certain parts. Typically you might want to grant access for mail quarantine handling but not to the SX-GATE administration.

SX-GATE groupware

If this option is enabled, every request with an URL starting with either "/groupware", "/SOGGo" or "/SOGGo.woa" will be forwarded to SX-GATE's groupware server. For backward compatibility the paths "/webmail" and "/cgi-bin/openwebmail" are also redirected. The groupware extension (app) has to be installed.



To access the groupware with a browser, you have to append "/groupware" to the URL (e.g. <https://www.example.com/groupware>).

SX-GATE Active Sync

Mobile devices and Outlook can access the SX-GATE groupware server with Exchange Active Sync (EAS). This option affects path "/Microsoft-Server-ActiveSync". If EAS is also enabled on tab "Microsoft IIS services", requests will be forwarded to Exchange.

SX-GATE CalDAV

This option enables access to the CalDAV server of SX-GATE's groupware, so any software which includes a CalDAV client can access scheduling information from the groupware calendars. The corresponding URL paths are "/SOGGo/dav/*/Calendar", "/SOGGo/dav/public/*/Calendar" and "/.well-known/caldav".

SX-GATE CardDAV

This option enables access to the CardDAV server of SX-GATE's groupware, so any software which includes a CardDAV client can access contacts from the groupware address books. The corresponding URL paths are "/SOGGo/dav/*/Contacts", "/SOGGo/dav/public/*/Contacts" and "/.well-known/carddav".

SX-GATE RDP/VNC/SSH web client

For clientless access to RDP, VNC and SSH servers via web client can be enabled with this option, if this SX-GATE extension (App) has been installed. The option forwards path "/webclient".



To access the web client with the browser, you have to append "/webclient" to the URL (e.g. <https://www.example.com/webclient>).

SX-GATE email quarantine area

Use this option to grant user access to the email quarantine area. If enabled, request for "/cgi-bin/unquarantine.cgi" will be forwarded to SX-GATE's administration server.



There's no need to enable this option if "User access to quarantine area" is disabled in menu "Modules > Mail Server > SPAM/Virus/Malware" on tab "MIME filter".

Access to SX-GATE admin GUI

This switch enables access to the SX-GATE administration GUI via reverse proxy.



To direct a web browser to the administration GUI `/riabconf/en` has to be appended to the URL (e.g. `https://www.example.com/riabconf/en`).

URLs which start with `/riabconf`, `/js`, `/styles` or `/flags`. In addition requests for certain files in directories with a one-letter or one-digit name will also be passed to the administration server.

ACME HTTP-Authorization

This option is required when SX-GATE obtains certificates from a CA via ACME (Automatic Certificate Management Environment), like e.g. from Let's Encrypt. The corresponding path is `/.well-known/acme-challenge/`.

14.8.2.2-C Backend servers

Userdefined backend servers

The reverse proxy forwards requests to the servers on this list. You can apply different settings by URL path. Case is ignored. Rules are evaluated top down. If there are multiple entries for the same path, the reverse proxy will act as a load balancer.

It is not possible to modify the URL path of requests to e.g. forward `/pathA` to backend A without path and `/pathB` to backend B without path. The URL path is always forwarded to the backend as-is. To address different backend servers using identical paths you must either configure different virtual hosts in the reverse proxy or use different external IPs associated with different reverse proxy ports.

Act.

Allows you to switch a rule off.

Auth.

Access to the backends requires authentication if this option is enabled. The reverse proxy will solely accept the credentials of members of SX-GATE group `"system-proxy"`. Enable this feature if access to the backends is limited to specific users. Information about the server software running on the backends or the kind of application provided will so remain invisible to unauthorized people.

SX-GATE's reverse proxy requests so called `"Basic Authentication"`. Usually the web browser opens a popup window to prompt for the required credentials.



With Basic Authentication the browser will send login and password more or less in plaintext. Therefore only encrypted connections (HTTPS) to the reverse proxy should be used if you enable this feature.

Check if authentication is required by the backend servers. If the backend credentials are prompted on a form which is embedded in the web pages there's no conflict. Users will then have to authenticate themselves at the reverse proxy first, then at the backend.



If the backend server requests Basic Authentication, authentication must not be enabled in SX-GATE's reverse proxy.

URL-Path

Only requests with a matching path will be forwarded to the corresponding backend server. The path you enter here is actually a path prefix, i.e. it may be followed by arbitrary characters. Use "*" as a wildcard within the path prefix. Note that "*" includes the path separator, so path "/images/a.gif?id=1" matches pattern "/*.gif". The special entry "/" matches any path, so it should go last in the list.



If there's no "/" entry, an error will be returned to browsers which try to access the reverse proxy without one of the listed paths.

Protocol

Make your choice. The connection between SX-GATE and the backend server may be encrypted or not.

Server

Please enter the IP or DNS name of the backend.

Port

If you don't enter a specific port, the backend will be contacted on the standard ports (80 for HTTP, 443 for HTTPS).

Factor

When load balancing (multiple entries with the same URL path), this value allows you to even out performance differences of the backends.

Comment

For your documentation.

Redirect home page to

The reverse proxy can reply to requests for the home page ("/") with an HTTP redirect. So users will be able to access a path based backend server without heaving to type

or even know the actual path. Enter e.g. "https://owa.example.com/owa" to redirect requests for "https://owa.example.com" to the Outlook Web App backend. It's also possible to redirect to the SX-GATE administration interface. In this specific case all paths starting with "/riabconf" are also redirected.



This setting does not have any effect if a userdefined backend server for path "/" is configured.

All other paths

Configure how to proceed with URL paths for which no backend has been configured.



This setting does not have any effect if a userdefined backend server for path "/" is configured.

redirect from http:// to https:// (incl. path)

Use this setting to redirect unencrypted to encrypted connections. Any path or parameter information is preserved. So e.g. a request for http://www.example.com/path/file.html is redirected to https://www.example.com/path/file.html.

redirect to URL

Forward the request to a URL of your choice. The URL must start with http:// or https://. By specifying a URL path, you can control whether the path and parameters should be taken from the browser request or not.



If the configured URL contains no path at all, path and parameters will be taken from the browser request. If the configured URL includes a path (a single "/" is already sufficient), browsers are always redirected to the configured URL.

Let's assume the browser requests the URL "https://example.com/test.html?lang=en".

Configured URL: "https://www.example.com" (without path)

Browser is redirected to "https://www.example.com/test.html?lang=en"

Configured URL: "https://www.example.com/" (path is "/")

Browser is redirected to "https://www.example.com/"

Configured URL: "https://www.example.com/welcome/" (path is "/welcome/")

Browser is redirected to "https://www.example.com/welcome/"

14.8.2.2-D Connection parameters

The reverse proxy is required to access SX-GATE extensions (apps). It's also possible to access the SX-GATE administration interface via reverse proxy. This allows you to restrict access to certain parts. Typically you might want to grant access for mail quarantine handling but not to the SX-GATE administration.

TLS protocol for HTTPS connections

Select the encryption strength for HTTPS connections from SX-GATE to the backend servers.



The actual encryption parameters associated with each option are updated from time to time.

outdated

Use this setting to enable the obsolete hash SHA1. The minimum TLS version is 1.0.

compatibel

Select this option for wide compatibility with older server systems. This will enable the obsolete hash SHA1. The minimum TLS version is 1.2.

contemporary

Only halfway recent server systems will be supported when selecting this option. At least TLS 1.2 is required. It is a good choice for security.

maximum

Requires TLS 1.3.

HTTP(S) properties

This setting controls the HTTP version used when talking to backend servers and if multiplpe requests will be sent via a single connection or not.



Only connections configured on tab "Backend servers" are affected.

HTTP/1.0, single request per connection

This is the recommended mode of operation. By closing the connection after each request the effect of memory leaks and software bugs is minimized.

HTTP/1.1, multiple requests per connection

The reverse proxy keeps connections to the backend server open and sends multiple requests via the same connection. This increases the overall performance and reduces the load on busy systems. If multiple clients access the same backend server at the same time, the reverse proxy might send requests of different clients via the same connection.

Integrated Windows authentication

This mode corresponds to the mode above, however an individual connection from the reverse proxy to the backend is exclusively associated with each connection from the client to the reverse proxy. This is necessary whenever the backend server requests NTLM or Kerberos authentication from the client, as these authentication schemes actually authenticate connections as a whole and not, as usual, individual requests.



Connections configured on tab "Microsoft IIS services" always use this mode, no matter if it is selected here or not.

14.8.2.2-E Load balancing

Configure multiple backend server for the same URL path on tab "Backend servers" and SX-GATE will act as a load balancer for the corresponding requests.

Basically a load balancer distributes requests to several backends, serving the same contents and applications. SX-GATE's reverse proxy chooses a random backend, taking into account the weighting factor you can assign to each backend. An optional session detection will make sure that subsequent requests of the same client stick to the same backend. A backend which does not respond will no longer receive requests. The reverse proxy will check every 10 seconds if it is alive again.

Session tracking

Some applications require that subsequent requests of the same client are processed by the same backend server. Usually the backend itself uses some sort of session tracking to accomplish this. In the best case the reverse proxy and the backend use the same method to identify a session.

<none>

If this option has been selected, the reverse proxy will choose a random backend for every request. This setting is the best choice for serving simple static contents.

IP address

This is the simplest way to identify a session. Subsequent requests from the same source IP will be served by the same backend. This method may be unreliable

with clients situated behind a proxy. Select this option if session detection is not vital or if none of the following options are possible.

Basic auth

If a client has to authenticate itself using the so called "Basic Authentication", this option is a good choice. With Basic Authentication the browser usually opens a small popup window to prompt for the user's credentials. Subsequent requests using the same credentials will always be sent to the same backend server. It does not matter whether the backend or SX-GATE's reverse proxy requested the authentication.

URL parameter

Select this option if a session id is passed along with every request as value of a specific URL parameter. Enter the name of the respective parameter. The parameter part of an URL starts with a question mark. Parameters are separated by "&" characters and have the form "name=value". Subsequent requests with the same parameter value will be served by the same backend.

Cookie

If the backend servers use cookies to identify a session you should select this option. Fill in the name of the cookie. Requests with the same value for this cookie will be forwarded to the same backend.

14.9 More Proxies

This menu lets you configure the following proxy services:

FTP proxy

FTP clients may use this proxy for their connections. Uploads and downloads are supported. Connect to port 2121 or configure transparent proxying.

SIP proxy

The SIP proxy is used by SIP clients (e.g. VoIP telephones) to connect to the internet. The proxy can be used in two different scenarios, either as a simple proxy or as a basix VoIP registrar. The service enables clients to cope with the NAT barrier of the gateway. Thus the clients can be connected from the local and the internet side.

POP3/SMTP proxy

This proxy allows mail clients to contact any POP3 and SMTP server on the Internet. It operates as a transparent proxy only.

SOCKS proxy

SOCKS is a generic proxy, running on port 1080. With SOCKS client software you can usually add SOCKS proxy capabilities to applications without native SOCKS support.

14.9.1 FTP proxy

The FTP proxy allows FTP clients to access FTP servers in a secured way. In comparison to a firewall policy which allows straight through FTP connections, proxied connections have several advantages. There's no direct IP connection between the FTP client and the FTP server. Restricting the accepted FTP sites prevents abuse. Security is enhanced by validity checks of the transmitted commands and the optional virusscan of downloads.



By default the FTP proxy will deny access to any server. A list of accepted target servers has to be defined first. Wildcard entries which allow access to any server are possible.

SX-GATE's FTP proxy can even operate transparent if you configure the firewall accordingly. Transparent means that the client will not notice that the requests are proxied. Furthermore there's no need to change the clients configuration. Change to "Modules > Firewall > Policies" and select the interface the client is connected to. Usually this is SX-GATE's LAN interface "eth0". Enable the redirection of connections to port 21 on tab "Transp. proxy".

In non-transparent mode any FTP client can use the proxy, too. If the FTP client allows you to configure an FTP proxy, you will have to enter SX-GATE as the proxy server on port 2121. The notations for the proxy type vary. Select something like "USER

with no login" or "USER user@host:port". Even if the FTP client does not offer proxy configuration, SX-GATE's FTP proxy can be used easily. In this case you may no longer contact the FTP site directly. No matter which FTP site you want to contact, connect to SX-GATE instead. Do not forget to specify the non-standard port 2121. FTP clients invoked from the command line usually take the port as an additional parameter (e.g. "ftp 192.168.0.254 2121"). Instead of entering the remote login only, you will now have to append an "@" character and the address of the FTP site (e.g. "login@ftp.example.com"). A non-standard port can be specified separated by a colon (e.g. "login@ftp.example.com:21000"). Login with your password as usual. SX-GATE's FTP proxy will not prompt for a password of its own.



Only "real" FTP clients are able to use the FTP proxy with non-transparent access. For FTP downloads with a web browser SX-GATE's web proxy on port 8080 has to be used instead.

Allowed FTP servers

Use this control to specify the accepted target FTP servers and its corresponding accounts. If the list is empty, the proxy will deny access to any server.

Account

Enter the login for the target FTP server here. Use "ftp" to grant access for anonymous FTP. If you leave the input field empty, the FTP proxy will accept logins to any account on the FTP server.

Destination server

Fill in the name or the IP address of the target FTP server here. Do not enter anything in order to accept access to any FTP server.

Port

Optionally you can specify a non-standard port for the FTP server. If you do not specify anything in here, SX-GATE assumes 21.

Some typical example rules which may be combined to satisfy your requirements. The specification of the server port can be omitted as it is usually not required.

Access to any FTP server

Simply leave all fields blank and click "Add". The rule "**@*:21" will appear.



Combining this rule with others will only make sense if the other rules refer to a different port.

Anonymous access to any FTP server

Enter "ftp" as "Account" and leave all other fields blank. "Add" will add the rule "ftp@*:21" to the list.



This rule will grant access to publicly available contents but will deny access to protected areas (e.g. maintenance of private homepages).

Access to any account on a specific FTP server

Enter the server name (e.g. ftp.example.com) as "Destination server" but don't fill in anything at ""Account". Clicking on "Add", the new entry "**@ftp.example.com:21" will appear.

Access to a single account on a specific FTP server

Specify the account and the server in the respective input fields and click "Add". The created rule will look like e.g. "webmaster@www.example.com:21".

Download virusscan

If this feature is enabled, all files downloaded using the FTP proxy will be scanned for viruses.



Uploads will not be scanned.



A functional virusscanner must be installed on SX-GATE if you want to use this feature. The virus scanner licenses are not included with SX-GATE and must be purchased separately. Further information about supported or already installed scanners can be found in the menu "Modules > Virusscanner". The installation of a virusscanner also has to be made there.

Accept special characters

The proxy replaces non-printable and non-ASCII characters in commands. Enable this option if you need access to files or directories with such characters.

14.9.2 SIP proxy

Client connections running through a NAT device (Network Address Translation) are a problem for Voice over IP. Therefore SX-GATE provides a SIP proxy with integrated RTP proxy for IP phones supporting the SIP protocol. So both, signaling and the actual voice data can be proxied.



Only IP phones connected to the SX-GATE interface eth0 can use the SIP proxy. The proxy supports UDP only.

There are two ways to use the SIP proxy:

Outbound proxy with external registrar

In this case the IP phones register with a registrar in the Internet. Supplemental services like a voice box or a gateway into the public telephone system. Here the primary task of SX-GATE's proxy is to forward incoming calls to the correct IP phone.



Calls to internal IP phones will not be routed through the external registrar.



If the Internet IP of SX-GATE is dynamic, a short registration interval has to be configured in the IP phone. A re-registration is the only means to inform the registrar of an IP change. Thus the registration interval determines the maximum period of time a local IP phone will be unreachable after an IP change.

To configure this scenario you have to configure the internal IP address of SX-GATE as the outbound proxy in the SIP phones. Ask your VoIP provider about the username, password and the name of the registrar server.

Local registrar

SX-GATE's SIP proxy can also act as a simple registrar. An appropriate DNS entry must point to the external IP of SX-GATE to allow incoming calls.



If the external SX-GATE IP is dynamic you will have to use dynamic DNS. After an IP change the time required to update the DNS entry determines how long the local IP phones will be unreachable. The registration interval of the IP phones has no influence.

Configure the IP phones as follows: Enter the DNS name as registrar server. The username is arbitrary but must of course be unique. The username is used to determine the local destination of the call. Finally the internal IP of SX-GATE has to be configured as outbound proxy.



There's no user authentication, but access to the SIP proxy can be restricted by client IP.

The firewall configuration of SX-GATE's Internet interface has to accept incoming UDP packets to port 5060.



If you are using an external registrar it might be sufficient to accept packets with specific source IPs of your VoIP provider.

Accept registrations of the following IP addresses

The SX-GATE SIP proxy will refuse registration if the client IP is not listed here. This applies to both modes of operation (external registrar or SX-GATE as registrar).



All the addresses specified here must be connected to the SX-GATE interface eth0.

SIP headers to delete

Sometimes problems occur when SIP messages grow so large that the corresponding network packets have to be fragmented. If you're lucky, you can avoid fragmentation by removing unnecessary headers.

14.9.3 POP3/SMTP proxy

The POP3/SMTP proxy allows users to retrieve mails from any POP3 server and to send mails via any SMTP server on the Internet and still benefit from SX-GATE's anti-virus and anti-SPAM capabilities.



Purpose of the proxy is to provide access to individual (private) mail accounts. The regular (business) mail should be processed by SX-GATE's mail client and server components, offering a variety of additional features.

The POP3/SMTP proxy always operates in transparent mode. Enable the corresponding switches in the firewall setup or enter custom DNAT rules, redirecting POP3 or SMTP connections to port 8110.

In the rare case when the pop server is not accepting connections on port 110 but on port 995 (POP3S) only, please follow the instructions below :

- Set up your mail client to establish an unencrypted connection to port 995.
- Enter a custom DNAT rule in the firewall configuration of SX-GATE's LAN interface, that redirects protocol POP3S to port 8110 on SX-GATE.

Number of concurrent connections

This parameter limits the number of concurrent connections handled by the proxy.



If the virusscan option is enabled, this parameter also controls the maximum of concurrent scanner processes spawned by the proxy. Depending on the actual scanner, there's a risk of system overload. So please enter a moderate value.

Verify certificates

While the connection between client and proxy is always unencrypted, the connection on the Internet side between proxy and POP or SMTP server is encrypted if the server supports this. Enable this option to also verify that the server certificate is valid and has been issued by a trusted CA.



It is not possible to verify that the server certificate has been issued to the same servername as configured in the client, as the proxy doesn't know the value configured on the client.

Virusscan

When enabled, SX-GATE will perform a virus check on emails downloaded with POP3 or sent by SMTP via the proxy.



A functional virusscanner must be installed on SX-GATE if you want to use this feature. The virus scanner licenses are not included with SX-GATE and must be purchased separately. Further information about supported or already installed scanners can be found in the menu "Modules > Virusscanner". The installation of a virusscanner also has to be made there.



If no scanner is installed, the installed scanner's license has expired or an unexpected error occurs while scanning, the proxy will be stopped.

Notify admin of discovered virus

Each discovered virus will be logged. For POP3 connections, the administrator can opt-in to an additional email notification on each incident.

Tag an email as SPAM when it is scored more than

This setting applies to POP3 connections only. If the SPAM score exceeds the threshold for tagging an email as SPAM, the subject of the mail is prefixed by the text "***** SPAM *****".



The overall behaviour of the SPAM filter is configured at "Modules > Mail Server > SPAM/Virus/Malware".

14.9.4 SOCKS proxy

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

14.9.4-A Connections.....	576
14.9.4-B Client access.....	577

14.9.4-A Connections

To provide internet access to applications, that are not able to use other proxies or firewall NAT rules, you can use the generic SOCKS-proxy. Supported protocols are SOCKS4 and SOCKS5. With the help of a SOCKS wrapper application nearly every networking application should be able to use the SOCKS proxy. Some programs even provide builtin SOCKS support.



For protocols like e.g. HTTP, HTTPS and FTP SX-GATE offers dedicated proxy services. SOCKS should not be used for these protocols. Specialized proxies provide more features and better protocol support than a generic proxy.



Data transmitted via the SOCKS proxy is not checked by any virus scanner. Also the integrity of the transported protocol is not verified.

By default the SOCKS proxy denies any connection request. Rules have to be added to grant access. The rules configured on this screen will apply to any SOCKS enabled application. However you also specify per-user SOCKS rules in the user administration. The respective user has to authenticate himself before he is allowed to connect.

Userindependant rules

The rules configured here indicate which connections the SOCKS proxy will accept.

First select the desired protocol. Specify a single IP address or a network address with its corresponding netmask if you want to restrict the acceptable source or destination IPs.



Protocols are defined in menu "Definitions > Protocols".



Non UDP and TCP protocol signatures will be ignored.

14.9.4-B Client access

Proxy access for source IP addresses

SX-GATE's SOCKS proxy will refuse connections if the client's IP is not listed here.

14.10 HTTP server

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

14.10-A Intranet.....	578
14.10-B WWW.....	579
14.10-C Content maintenance.....	580
14.10-D Advanced.....	581

14.10-A Intranet

SX-GATE offers you the possibility to publish documents for the intranet on a web server. Access to the intranet server is limited to the "INTRANET" networks as specified at "Definitions > IP objects". It also possible to connect to this area via the web proxy of SX-GATE. The upload of files is possible by FTP and windows network shares. Use the predefined user "intranet" as login.



By default this service is not enabled. Start the web server at "System > Services".

Servername of the Intranet server

Here you determine the server name of the intranet web server. You might have to add this name to the DNS. The intranet server is addressed by the name you configure here or by the LAN IP address.

Web-Proxy Auto-Discovery domain

Most browsers are able to automatically detect the web proxy configuration using Web-Proxy Auto-Discovery (WPAD). The browser needs to download a config file from a web server. One of the methods WPAD specifies to determine the URL of this config file uses DHCP. You can configure it in menu "Modules > DHCP" on tab "Windows parameters". Here you can enable a DNS based method. The browser tries to download the file "wpad.dat" from a server named "wpad.<LOCAL DOMAIN>".

Specify the network domain configured on your workstations here. SX-GATE will then set up appropriate DNS entries in its name server and instruct the intranet web server to redirect requests for "wpad.dat" to

"http://<SX-GATE's LAN-IP>:8000/proxy.pac"

. This is a predefined config file which instructs the browsers to use SX-GATE as web proxy.



If the workstations are in different subdomains (e.g. "sales.example.com" and "management.example.com"), enter the domain part they have in common ("example.com").

Change password of user "intranet"

Here you can either specify the password for the predefined user "intranet" or disable the corresponding account. The user "intranet" has to be used to maintain the intranet web server directory.



This user is not listed in the user administration menu of SX-GATE.

14.10-B WWW

SX-GATE offers you the possibility to operate a simple Internet web server. The upload of files is possible by FTP and windows network shares. Use the predefined user "www" as login.

Enable WWW server

With this switch you can activate the Internet web server. If it is not checked only the intranet service for the local networks is available.



Most likely the firewall policy has to be modified to grant access to the web server for clients in the Internet. Open the HTTP port 80. In addition, the web server is not enabled by default. Start it at "System > Services".

Servername of the WWW server

Here you determine the server name of the web server (e.g. www.example.com). A corresponding DNS record might have to be added for the server. This is usually done by your provider.

Change password of user "www"

Here you can either specify the password for the predefined user "www" or disable the corresponding account. The user "www" has to be used to maintain the www server directory.



This user is not listed in the user administration menu of SX-GATE.

14.10-C Content maintenance

The SX-GATE windows shares can be used to comfortably manage the SX-GATE web servers using windows.



By default, the corresponding service is not active. Enable it in "System > Services".

Access using Windows network share

Access to the network shares is limited to the "INTRANET" networks as specified at "Definitions > IP objects".

Windows workgroup or domain

Please enter the name of your Windows workgroup or domain here.



Do not confuse the windows domain with your Internet domain.

Intranet share enabled

Use this switch to enable the network share "intranet". This share can be used to update the contents of SX-GATE's intranet server.



You have to connect to this share as user "intranet". The corresponding password is specified in the menu "Modules > HTTP server".

Intranet CGI share enabled

Use this switch to enable the network share "intracgi". This share can be used to update the CGI scripts of SX-GATE's intranet server.



You have to connect to this share as user "intranet". The corresponding password is specified in the menu "Modules > HTTP server".

WWW share enabled

Use this switch to enable the network share "www". This share can be used to update the contents of SX-GATE's web server.



You have to connect to this share as user "www". The corresponding password is specified in the menu "Modules > HTTP server".

WWW CGI share enabled

Use this switch to enable the network share "wwwcgi". This share can be used to update the CGI scripts of SX-GATE's web server.



You have to connect to this share as user "www". The corresponding password is specified in the menu "Modules > HTTP server".

14.10-D Advanced

Email address of administrator

Anytime the web server sends an error message to the browser, this email address will be included as administrative contact address.

14.11 FTP server

Here you can specify which class of users has access to the FTP server of SX-GATE. Restricting access using the option "allowed from local networks" refers to source IP addresses which belong to the "INTRANET" networks as defined in "Definitions > IP objects".

Access for admin

With this switch you configure FTP access for user "admin".

Access for ftpadmin/intranet/www

Here you can configure access for the predefined users "ftpadmin", "www" and "intranet". The user "ftpadmin" is used to maintain the FTP directories for anonymous FTP access and to maintain the TFTP server directory. With the users "www" and "intranet" have access to the respective areas of SX-GATE's built-in web server. The directories for these users are secured in a special way. An FTP client which is connected as one of these users will not be able to leave the respective base directory.

Anonymous access

SX-GATE allows you to share files using the integrated anonymous FTP server. You can maintain the corresponding directory via FTP using the login name "ftpadmin". FTP clients which are connected to the FTP server as anonymous user will not be able to leave the base directory of this service.

Anonymous file upload to directory "incoming"

If you want to allow file uploads for user "anonymous", please activate this option. Uploads have to be stored in the directory "incoming". The user "ftpadmin" can create subdirectories in this directory. For anonymous users it will not be possible to download files which have been uploaded to the "incoming" directory.

Change password of user "ftpadmin"

Here you can either specify the password for the predefined user "ftpadmin" or disable the corresponding account. The user "ftpadmin" has to be used to maintain the FTP server directory for anonymous FTP and to maintain the TFTP server directory.



This user is not listed in the user administration menu of SX-GATE.

14.12 SNMP server

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

14.12-A General.....	583
14.12-B SX-GATE-OIDs.....	584

14.12-A General

SNMP can be used to poll status information from SX-GATE. Please enable the service in menu "System > Services"



Only SNMPv3 is supported. Authentication and encryption are mandatory.

Allowed IP addresses

Only the IP addresses specified here are allowed to retrieve information from the SNMP server.

Username

Clients must use this login and password to access SX-GATE's SNMP server. The minimum password length is 8 characters.

Authorization protocol

Select the method used to protect the password.



The MD5 and SHA1 protocols should no longer be used. SHA-224 is not recommended by the German Federal Office for Information Security (BSI). They are offered for reasons of compatibility. Please use SHA-256, SHA-384 or SHA-512.

Privacy passphrase

The SNMP communication is encrypted, using this passphrase. Please use a rather long string, consisting of upper and lower case characters, digits and special characters. At least 8 characters are required.

Privacy protocol

Please select the cipher.



The DES protocol should no longer be used. It is offered for compatibility reasons. Please use AES-256, AES-192 or AES-128 instead.

Contact

This value serves for informational purposes only.

Location

This value serves for informational purposes only.

14.12-B SX-GATE-OIDs

SX-GATE features product-specific OIDs. You can activate them here.

The values of the individual OIDs are updated regularly regardless of their retrieval. The interval is linked to the basic OID and is between one minute (e.g. status of a service) and 12 hours (e.g. SX-GATE version). Further information can be found in the description of the SX-GATE-MIB.



It may take up to 15 seconds for the full values to be available after an OID is first retrieved after the service is restarted.

Enable SX-GATE-oids

Enable SX-GATE-oids

14.13 Logging

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

14.13-A Archiving.....	585
14.13-B Remote syslog server.....	587
14.13-C SX-GATE syslog server.....	588
14.13-D Netflow/IPFIX.....	588
14.13-E Anomaly detection.....	589

14.13-A Archiving

Besides archiving log files on SX-GATE itself, these can also be copied to an SMB, FTP, SFTP or secure shell server. The files will be gzip compressed before transferring them. Sending the logs via e-mail is also possible although this is not recommended as the log files might become very large. Just like the internal archiving, the log files will be copied just after midnight.



Please be sure to observe all statutory requirements. Archiving log files may not be allowed, in particular for privacy reasons and data protection.

In the following input fields you can determine if and how a log has to be archived. Leave the field blank if you don't want to archive the file externally. Otherwise enter the target in URL format.

Archive via SMB (Windows share):

Uploading the log to an SMB server requires a URL which uses the format "smb://LOGIN:PASSWORD@ADDRESS/SHARE/PATH/FILENAME".

If you enter e.g. "smb://admin:secret@127.0.0.1/logs/path/messages.log", SX-GATE will connect to the share "logs" located on the SMB server 127.0.0.1 and login as user "admin" with password "secret". It will store the log as file "messages.log" in the directory "path". Specifying a share name is required, a path is optional. However any subdirectory given in the URL must already exist on the server.

Archive via FTP:

Uploading the log to an FTP server requires a URL which uses the format "ftp://LOGIN:PASSWORD@ADDRESS/PATH/FILENAME".

If you enter e.g. "ftp://admin:secret@127.0.0.1/logs/messages.log", SX-GATE will connect to the FTP server 127.0.0.1 and login as user "admin" with password "secret". It will store the log as file "messages.log" in the directory "logs".

Specifying a path is optional. However any subdirectory given in the URL must already exist on the server.

If you have to use an upstream FTP proxy to upload the file, please append a space character and the proxy specification to the URL. A proxy specification uses the format

"ftpproxy://ADDRESS:PORT".

If authentication is required, use

"ftpproxy://LOGIN:PASSWORD@ADDRESS:PORT"

instead.

Archive via SFTP

To transfer the archive encrypted, you can use secure file transfer protocol (sftp). Specify the destination URL in the format

"sftp://LOGIN@ADDRESS/PATH/FILENAME"

(e.g. sftp://admin@127.0.0.1/logs/messages.log). SX-GATE will not authenticate itself with a password, but with an ED25519 or RSA key. The SFTP server has to be configured accordingly. Destination directory must exist on the server.

Archive via secure copy (secure shell)

Just like SFTP you can also use secure copy (scp) to transfer the archive encrypted. Specify the destination URL in the format

"scp://LOGIN@ADDRESS/PATH/FILENAME"

(e.g. scp://admin@127.0.0.1/logs/messages.log). SX-GATE will not authenticate itself with a password, but with an ED25519 or RSA key. The secure shell server has to be configured accordingly. Also with secure shell the specification of a path is optional. If subdirectories are given they must exist on the server.

Archive via email:

Due to the size of log files it is not advisable to archive the logs via email. If you want to mail the logs anyway, please specify the destination using the format "mailto:ADDRESS".

You can include variables in the filename of FTP, SMB and secure copy URLs. The previously archived log file will not be overwritten in this case.

The following variables are available:

- %Y: 4 figure year (e.g. 2001)
- %y: 2 figure year (e.g. 01)
- %m: Month (from 01 to 12)
- %d: Day (from 01 to 31)
- %H: Hour (from 00 to 23)
- %M: Minute (from 00 to 59)
- %S: Second (from 00 to 59)
- %U: Week of the year (Value from 00 to 53)
- %w: Day of the week (0 for Sunday to 6 for Saturday)
- %j: Day of the year (from 001 to 366)

If for instance you specify the destination

```
"scp://admin@127.0.0.1/logs/messages-%m-%d.rbu",
```

the filename will include the current month and day as a number. Thus the log file will not be overwritten until next year.

Delete all old log files

This command will delete all old logs on the system. This comes in handy if the system is running out of disk space due to exceptionally large log files. Depending on the rotation cycle of the respective log the entries up to the previous day, week (up to and including Saturday) or month will be deleted. The current log files are not affected.



Use this feature only in case of necessity. Rapidly growing logs are often caused by some misconfiguration. Try to find out what's going wrong and remedy the deficiencies.



There's no way to restore a deleted log.

Test archiving

With this command an attempt is made to copy the current logs to the specified URLs

14.13-B Remote syslog server

If you have a remote syslog server you can enable remote logging to that server here.



Only log messages will be included which are generated by using the syslog API. This excludes the following log files:

- IDS/IPS
- Web proxy access
- Web proxy messages
- Reverse proxy access
- Reverse proxy messages
- WWW server access
- WWW server messages
- Intranet server messages
- Administration

14.13-C SX-GATE syslog server

You can use SX-GATE as a syslog server for other devices.



Access to the syslog server is neither authenticated nor encrypted. Use firewall rules to restrict access to this port to an absolute minimum.

Port

The syslog server will listen to the port configured here. The default port is 514.

14.13-D Netflow/IPFIX

You can pass information about network connections to a Netflow v5, v9 or IPFIX server for further analysis.

Mode

Select which connections to export.

selected interfaces

Enable the export in the interface settings below menu "Modules > Firewall > Policies".

all interfaces

The connections of all interfaces will be exported, except for device internal communication.



This may produce a large amount of data.

Collector

SX-GATE will send the data to the system you configure here. The collector should be part of the local network.



Data is sent neither authenticated nor encrypted.

14.13-E Anomaly detection

Anomaly detection looks for exceptionally high values for the number of lines in certain log files or the throughput of the Internet interface. If an hourly statistical evaluation indicates that there is an anomaly, the "admin" is notified by email. Further information on diagnosis of the respective anomaly can be found in the documentation of the corresponding switch on this tab.



An email notification does not necessarily indicate an actual problem. Still you should take the email as an occasion to check the system.

Usually you will analyze logs in menu "Monitoring > Log files" to find out more about the anomaly. Select the correct log, increase the number of displayed lines significantly and narrow down the time period to e.g. one hour before to one hour after the occurrence of the anomaly. If necessary you can pre-filter the log with certain keywords. Then submit the query. In the results screen, please notice the histogram on the top left. By dragging the side edges, you can restrict the display to the time range with the most frequent entries.

Log "IDS/IPS"

This sensor counts the "Priority 1" alarms of the IDS/IPS system. Lines that contain either "Attempt" or "ET_SCAN" are ignored.

Analyse the log "IDS/IPS". An overview of the longer-term development can be found at "Statistics > Firewall > IDS/IPS".



The statistics are updated daily after midnight.

Log "firewall"

This sensor counts the number of lines with "drop" or "rej" in the firewall log, i.e. intercepted packages.

Analyse the log "firewall". An overview of the longer-term development can be found at "Statistics > Firewall > Packet filter".



The statistics are updated daily after midnight.

Log "Web proxy access" (only 4xx error codes)

This sensor counts web proxy access lines with 4xx status codes. These status codes are returned when a client sends an invalid request, e.g. if the requested file does not exist or to request client credentials if user authentication is required.

Analyse the log "Web proxy access". Filter the search results for 4xx status codes. An overview of the longer-term development can be found at "Statistics > Proxies > Web proxy".



The statistics are updated daily after midnight.

Log "Web proxy access"

This sensor counts the total number of web proxy accesses.

Analyse the log "Web proxy access". An overview of the longer-term development can be found at "Statistics > Proxies > Web proxy".



The statistics are updated daily after midnight.

Log "Reverse proxy access" (only 5xx error codes)

This sensor counts reverse proxy access lines with 5xx status codes. These status codes are returned upon a server-side error, e.g. if no suitable backend server has been configured or if the backend is unreachable.

Analyse the log "Reverse proxy access". Filter the search results for 5xx status codes. An overview of the longer-term development can be found at "Statistics > Proxies > Reverse proxy".



The statistics are updated daily after midnight.

Log "Reverse proxy access"

This sensor counts the total number of reverse proxy accesses.

Analyse the log "Reverse proxy access". An overview of the longer-term development can be found at "Statistics > Proxies > Reverse proxy".



The statistics are updated daily after midnight.

Internet usage (inbound)

This sensor monitors the amount of data transferred inbound via the Internet interface. An alert can be caused by a local system that downloaded large amounts of data from the Internet or by an external system that uploaded large amounts of data.

If the inbound bandwidth usage of Internet interface is still high, you can analyse the currently active connections in menu "Monitoring > Firewall". Click the column headers of the table to sort by the amount of transmitted data. To check if an internal system causes the high bandwidth consumption, sort by amount of data transmitted from destination to source. To check if an external system is responsible, sort by amount of data from source to destination.

Unfortunately it is difficult to find the cause of the problem in retrospect. An graphical overview of bandwidth consumption and number of connections can be found at "Statistics > Network". The menus "Statistics > Proxies" und "Statistics > Web server" are updated daily after midnight and might provide further points of reference. If a permanent analysis option is required, you can enable a continuous export of the extensive firewall connection data to a system specialised for this on tab "Netflow/IPFIX".

Internet usage (outbound)

This sensor monitors the amount of data transferred outbound via the Internet interface. An alert can be caused by a local system that uploads large amounts of data into the Internet or by an external system that downloads large amounts of data.

If the outbound bandwidth usage of Internet interface is still high, you can analyse the currently active connections in menu "Monitoring > Firewall". Click the column headers of the table to sort by the amount of transmitted data. To check if an internal system causes the high bandwidth consumption, sort by amount of data transmitted from source to destination. To check if an external system is responsible, sort by amount of data from destination to source.

Unfortunately it is difficult to find the cause of the problem in retrospect. An graphical overview of bandwidth consumption and number of connections can be found at "Statistics > Network". The menus "Statistics > Proxies" und "Statistics > Web server" are updated daily after midnight and might provide further points of reference. If a permanent analysis option is required, you can enable a continuous export of the extensive firewall connection data to a system specialised for this on tab "Netflow/IPFIX".

14.14 Virusscanner

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

14.14-A Signature update.....	592
14.14-B Avira.....	592
14.14-C WithSecure (F-Secure).....	593
14.14-D Kaspersky.....	594
14.14-E Install / update / uninstall.....	594

14.14-A Signature update

Update anti-virus signatures automatically

Enable this option if installed virus scanners should update their anti-virus signatures regularly.

Signature update notification

If requested, the administrator will be notified by email after every update attempt. Disable this option if only persisting error conditions should be reported, i.e. a single failure is not reported.



It is highly recommended to activate notification even on apparently successful updates. The system cannot detect every error condition automatically.

14.14-B Avira

The Avira virus scanner for SX-GATE can be purchased exclusively from SX-GATE dealers. The available license depends on the number of users and will only cover the installation of the scanner on SX-GATE. The license is valid for a certain period of time and therefore has to be renewed regularly. When buying or renewing the license you will receive a license key file. You must install this file on the tab "Install / update / uninstall". SX-GATE will in time notify the administrator by mail before the license expires.



Software updates of the Avira virus scanners will be installed along with the regular SX-GATE updates.

Online support for scanner?

If this option is enabled the virus scanner will contact an online service provided by the scanner maker to increase detection rate.

Currently installed version

You can find detailed information about the currently installed Avira scanner here. Furthermore a selftest of the scanner will be performed every time you enter this screen. The status "OK" indicates that the scanner is working as expected.

Update signatures now

Press this button to immediately update the Avira signatures.

14.14-C WithSecure (F-Secure)

The WithSecure virus scanner for SX-GATE can be purchased exclusively from SX-GATE dealers. The available license depends on the number of users and will only cover the installation of the scanner on SX-GATE. The license is valid for a certain period of time and therefore has to be renewed regularly. When buying or renewing the license you will receive a license key file. You must install this file on the tab "Install / update / uninstall". SX-GATE will in time notify the administrator by mail before the license expires.



To install or update the WithSecure Antivirus app please go to "System > Apps" vor.

Online support for scanner?

If this option is enabled the virus scanner will contact an online service provided by the scanner maker to increase detection rate.

Currently installed version

You can find detailed information about the currently installed WithSecure scanner here. Furthermore a selftest of the scanner will be performed every time you enter this screen. The status "OK" indicates that the scanner is working as expected.

Update signatures now

Press this button to immediately update the WithSecure signatures.

14.14-D Kaspersky

The Kaspersky virus scanner for SX-GATE can be purchased exclusively from SX-GATE dealers. The available license depends on the number of users and will only cover the installation of the scanner on SX-GATE. The license is valid for a certain period of time and therefore has to be renewed regularly. When buying or renewing the license you will receive a license key file. You must install this file on the tab "Install / update / uninstall". SX-GATE will in time notify the administrator by mail before the license expires.



Software updates of the Kaspersky virus scanners will be installed along with the regular SX-GATE updates.

Online support for scanner?

If this option is enabled the virus scanner will contact an online service provided by the scanner maker to increase detection rate.

Currently installed version

You can find detailed information about the currently installed Kaspersky scanner here. Furthermore a selftest of the scanner will be performed every time you enter this screen. The status "OK" indicates that the scanner is working as expected.

Update signatures now

Press this button to immediately update the Kaspersky signatures.

14.14-E Install / update / uninstall

Virus scanner licenses are not part of SX-GATE and must therefore be purchased separately. You will find further information in the documentation of the scanner specific screen.

Upload virusscanning engine, signatures or license keys

This area allows you to install or update virus scan engines. You can also upload signature archives here.

Avira

Installing the Avira scanner requires a special archive which has been adapted to SX-GATE. This archive has the filename extension "*.rin". In addition you also have to install the Avira license key file here. This file has the filename extension "*.key". To renew an expired Avira license you only have to upload the new key file here. Although the scan engine will be updated along with the regular SX-

GATE updates, you can also update the engine by simply uploading the archive with the new release here.

F-Secure

You can install the F-Secure license key file here. This file has the filename extension "*.key". To renew an expired F-Secure license you only have to upload the new key file here.

Kaspersky

Also the installation of the Kaspersky scanner requires a special archive (*.rin). In addition you also have to install the Kaspersky license key file here. This file has the filename extension "*.key". To renew an expired Kaspersky license you only have to upload the new key file here. The scan engine will be updated along with the regular SX-GATE updates. You can also update the engine by uploading an archive with the new release here, however you might run into problems with the license key.

Uninstall virus scanner

This control allows you to uninstall a virus scanner which has been installed on SX-GATE.

14.15 Time server

The configuration options in this menu are structured by topic. You can change between the different screens by clicking on the tabs at the top.

14.15-A Synchronisation.....	596
14.15-B SX-GATE time.....	597

14.15-A Synchronisation

SX-GATE can be configured to synchronise its system time with public time servers in the Internet. You can then synchronise other systems in your local LAN with the time of SX-GATE. To get the current time, connect to TCP port 13 (daytime) or 37 (time), UDP port 123 (NTP) or use the windows shares for time synchronisation.



You need to activate the SX-GATE service "NTP time server" if you want to use the NTP protocol.



To synchronise the system time of older Windows systems (before Windows 2000), you have to activate the SX-GATE service "Windows shares". Then issue the command

`"NET TIME /SET \\SX-GATE-IP /YES"`

on the DOS prompt of a windows machine to synchronise its time. You can add this command to the login script of your domain controller or to the autoexec batch file of the workstations to synchronise automatically. It is not necessary to activate the NTP service in this case.

Synchronisation schedule

Please select the frequency of time synchronisation. SX-GATE will synchronise either daily or every Sunday between 4.00 a.m. and 4.59 a.m.. If enabled, the SX-GATE service "NTP time server" will perform an additional continuous synchronization.

Public time servers

SX-GATE will synchronise its system time with the servers specified here. Using the ntp.org server pool is recommended (e.g. europe.pool.ntp.org). Any hostname from this domain represents a number of public NTP servers. When resolving the DNS hostname, a random server is selected. If at least one hostname from the pool.ntp.org domain has been specified, SX-GATE will contact at least three pool servers.

Verify time servers

Use this function to verify that all configured time servers are available.



The current system time of SX-GATE will not be modified.
Change to tab "SX-GATE time" to adjust the time.

14.15-B SX-GATE time***Synchronise now***

If you want to contact the listed time servers immediately in order to synchronise the system time of SX-GATE, please clicking this button. Note that you will need to be connected to the Internet.

SX-GATE timezone

The timezone currently used by SX-GATE is shown here.

Change timezone

To change the timezone setting of SX-GATE click this button.

15 Configuration of an L2TP IPsec VPN client

15.1 Microsoft Windows

This howto describes the configuration of an L2TP IPsec VPN to SX-GATE, using the builtin IPsec implementation of Microsoft Windows. Screenshots have been taken from Windows XP Professional, however the configuration in other windows releases supporting L2TP IPsec is quite similar.



Depending on the Windows release you are using, the screenshots in this howto may differ from the screens you will encounter.

Prerequisites for the windows client:

- Manual configuration: Windows 2000 or newer
- Automatic configuration: Windows XP SP2 or newer and authentication using certificates.
- If NAT traversal is required: On the systems running Windows XP (up to SP1) or Windows 2000 the Microsoft patch Q818043 has to be applied
- Preshared Key authentication is not supported with Windows 2000

The SX-GATE VPN server should be already configured. It is highly recommended to use SX-GATE's wizard "IPsec VPN" from the "Wizards" menu. If you are using X.509 certificates for authentication, please make sure to have the required key and certificate files at hands.



On the last screen of the "IPsec VPN" wizard you will find a note which tells you how to issue certificates. Please rerun the wizard if you missed that hint.

Basically the L2TP-IPsec connectivity is provided by two different SX-GATE services:

IPsec VPN

The IPsec connection provides a secure tunnel for the L2TP protocol it encapsulates.

Only L2TP packets (UDP port 1701) will be accepted within the IPsec tunnel.

The IPsec tunnel must be authenticated with either a preshared key or by X.509 certificates.

L2TP server

Similar to a dial-up connection, L2TP is based on the PPP protocol.

PPP provides e.g. authentication, IP negotiation and the actual connectivity between client and destination network.

PAP is used for user authentication.



Using PAP to authenticate is safe, although it transmits the password unencrypted. Remember that L2TP is protected by the encapsulating IPSec tunnel.

There are two different options a L2TP-IPSec-VPN connection can be configured

Automatic configuration

You use the setup package which is offered to you by SX-GATE as download after creating a new certificate. This package contains all the files which are necessary for doing an automatic import of the certificates and also configures the connection for you.

Manual configuration

You have to configure all the necessary parameters yourself. If you are using certificates for authentication, you will have to import them.

15.1.1 Automatic configuration

As described in chapter "System > Certificate manager > CA certificates > Certificates", section "Create setup package", you can download a special setup-package after creating a new certificate. This file needs to be copied to the windows client on which you want to setup the L2TP connection to SX-GATE.

When you start this executable file a window will open up, prompting for the import password.

The password is used to decode and import the certificates.



If the certificate import fails, as e.g. the Windows version is too old, all the necessary files for a manual configuration will be copied into the user's home directory.

Then the "Connection Manager Administration Kit" is used to configure the VPN connection. All there is to do is selecting if the connection should be available to all users or only for the current user.

Now the Connection Manager is opened. Simply enter username and password and connect to SX-GATE.

15.1.2 Manual configuration

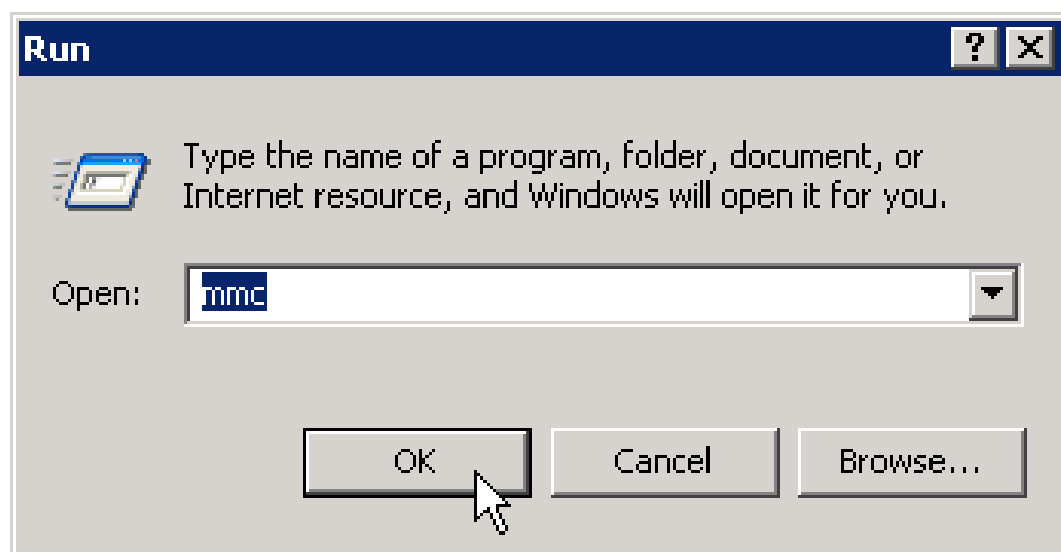
Select IPSec authentication type

If the IPSec connection will not be authenticated by certificates, you can skip the description of the certificate import.

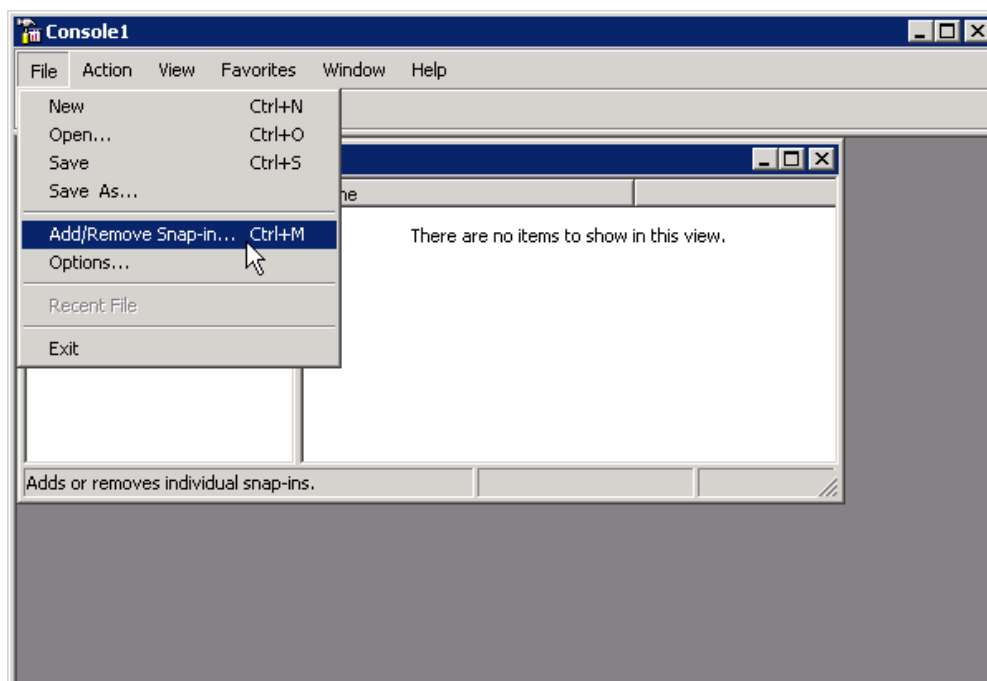
- X.509 certificate
Please read on at [Setup management console](#) (p. 602)
- passphrase (preshared key)
Please read on at [Connection setup](#) (p. 609)

Setup management console

Select "Run" from the Windows "Start" menu

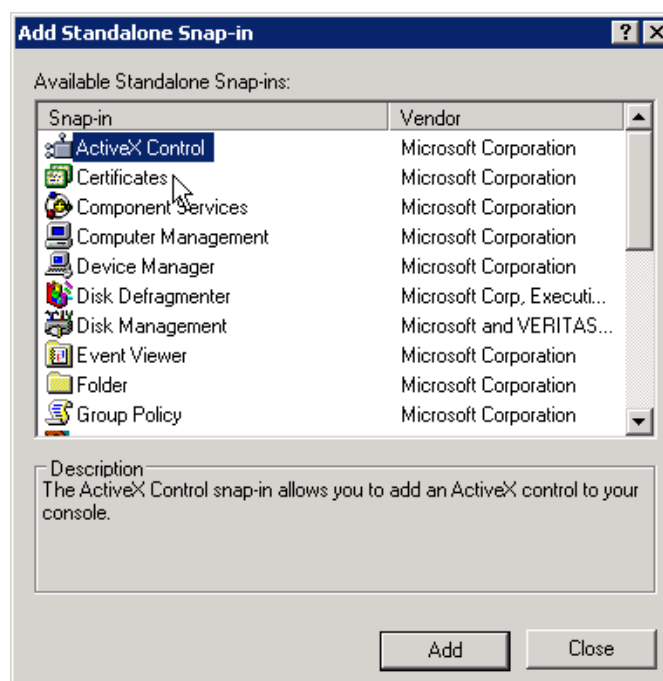


Open the Management Console by typing "mmc" and pressing "OK"

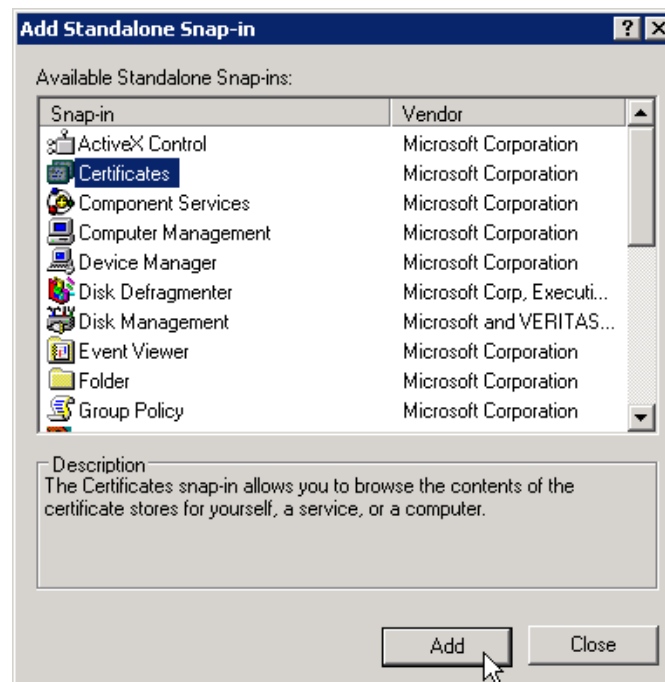


Select "Add/Remove Snap-in" from the "File" menu

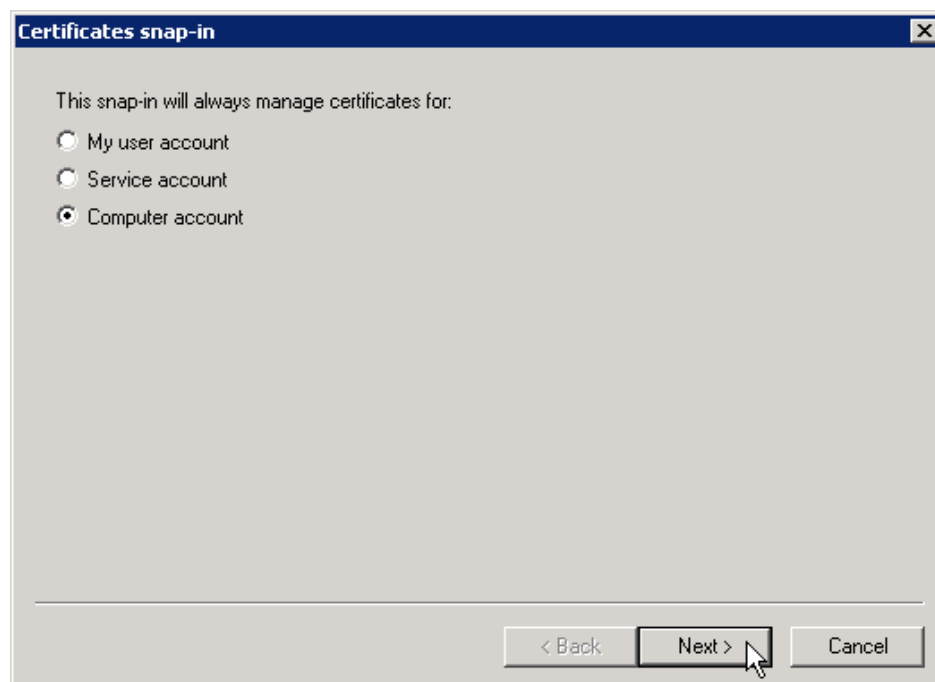
Click "Add" for a list of available snap-ins.



Select the snap-in "Certificates" and insert it with "Add".



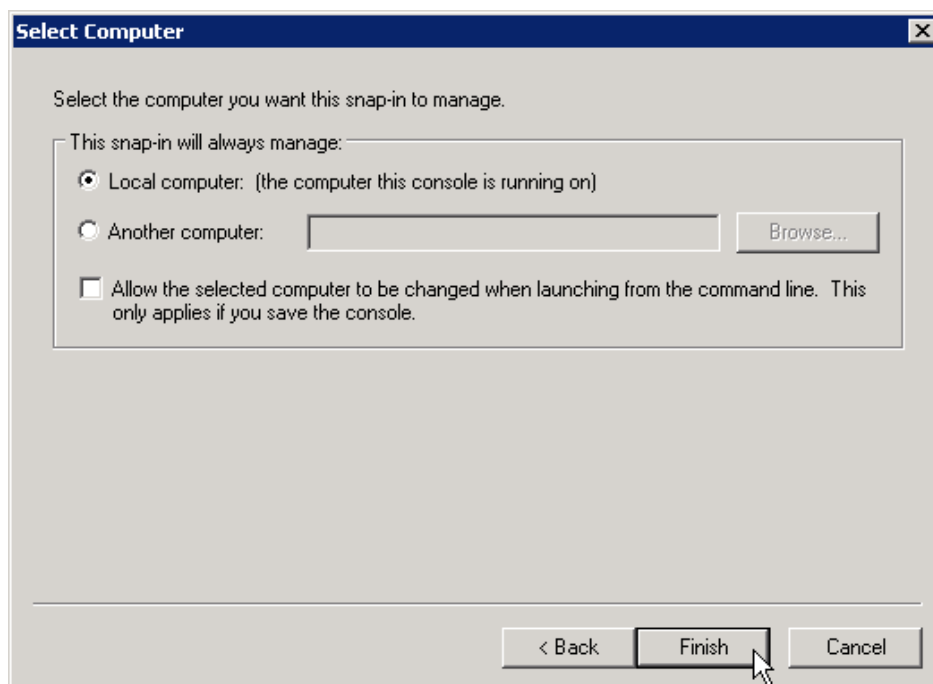
It is crucial to select "Computer account" as managed account type.



Proceed with "Next".

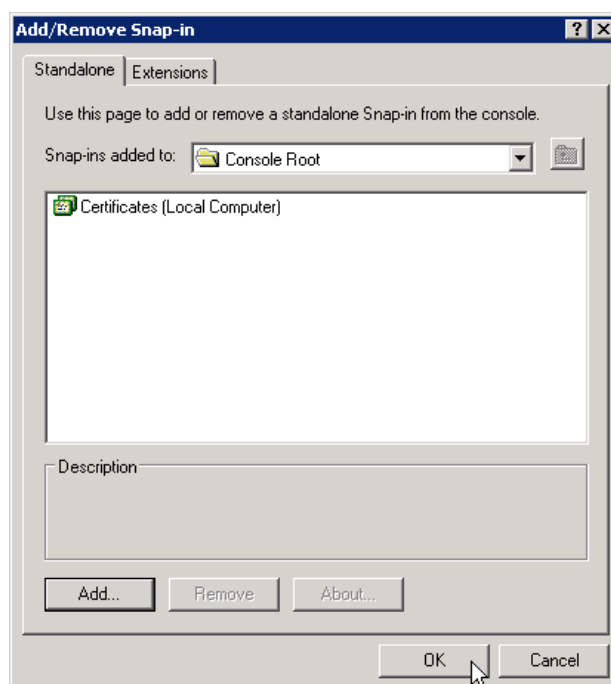
The snap-in has to manage certificates on the "local Computer".

Press "Finish" to add the new snap-in.



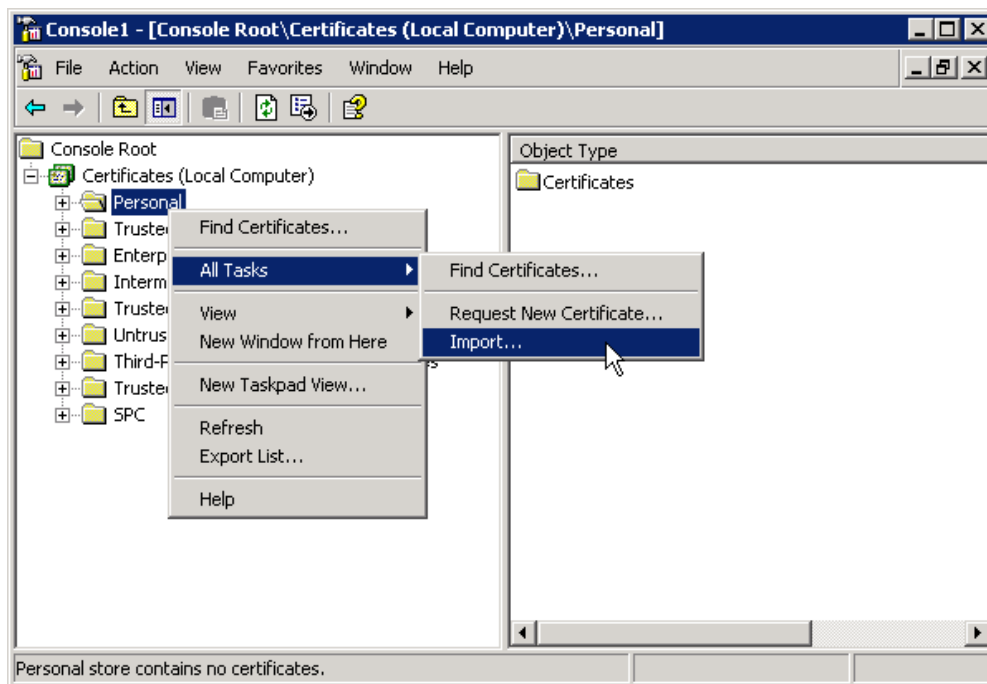
"Close" the list of available snap-ins.

With "OK" the computer is prepared to import the VPN key.



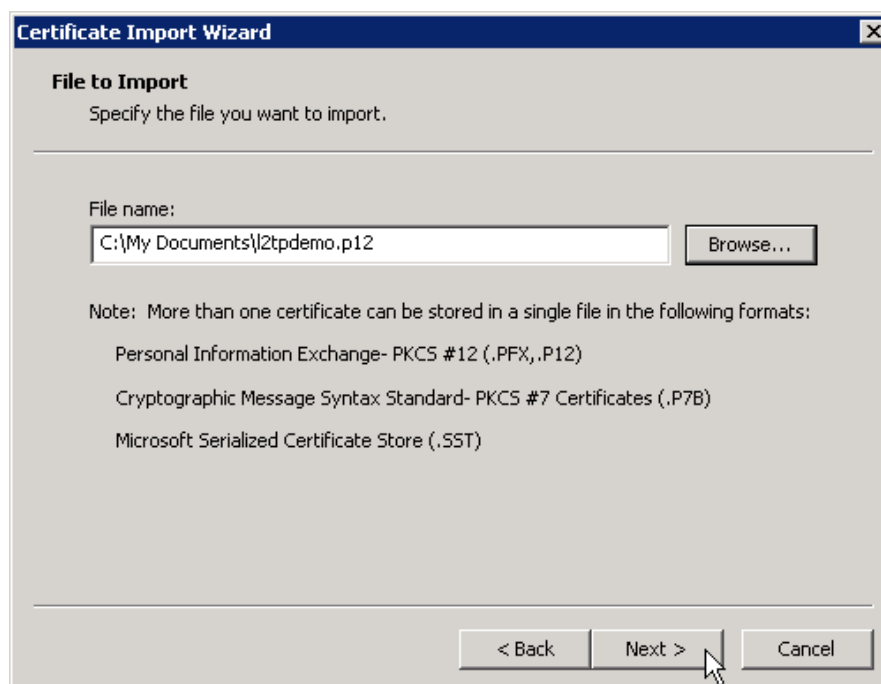
Import certificate

Open the folders "Console Root" and "Certificates (Local Computer)" from the tree view. Right-click the "Personal" item and select "All Tasks > Import" from the context menu.



Leave the welcome screen by clicking "Next".

Select the PKCS#12 file (*.p12) which contains the required certificates and the private key.



Proceed with "Next".

You will now be prompted for the password protecting the PKCS#12 file.



This password was assigned while issuing the certificate to protect the PKCS#12 file's private key. Do not confuse this password with the CA password, which has to be provided everytime a new certificate is signed.

The screenshot shows the 'Certificate Import Wizard' window, specifically the 'Password' step. The title bar reads 'Certificate Import Wizard'. Below the title, the section is 'Password'. The text says: 'To maintain security, the private key was protected with a password.' Below this, it says: 'Type the password for the private key.' There is a text box labeled 'Password:' containing '*****'. Below the text box are two checkboxes. The first checkbox is unchecked and labeled 'Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.' The second checkbox is also unchecked and labeled 'Mark this key as exportable. This will allow you to back up or transport your keys at a later time.' At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

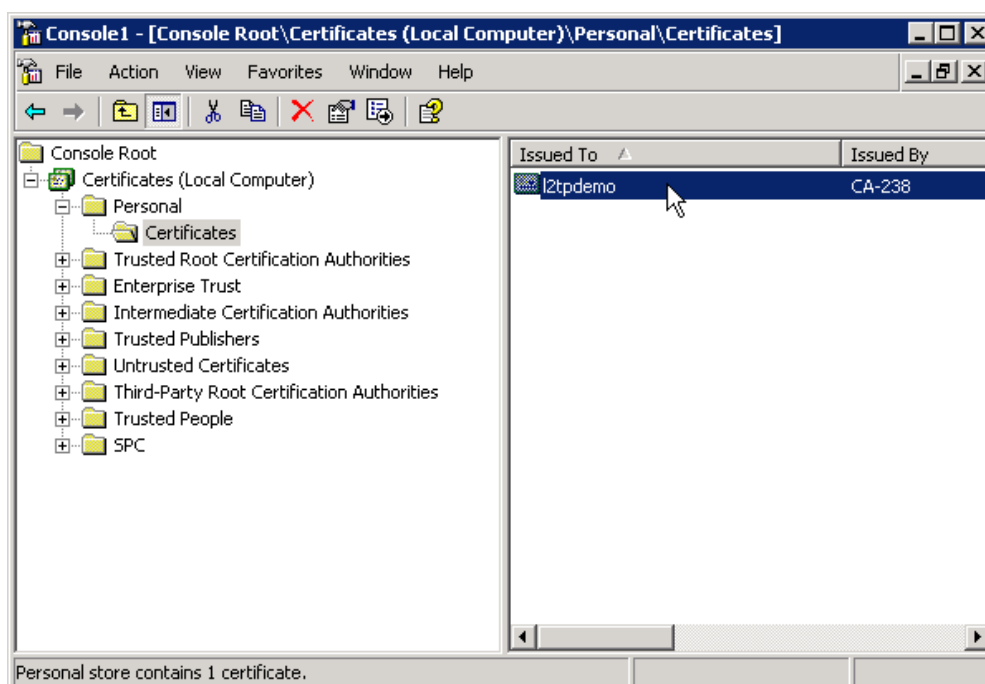
Press "Next".

On the next screen, it is very important to pick "Automatically select the certificates store based on the type of certificate".

The screenshot shows the 'Certificate Import Wizard' window, specifically the 'Certificate Store' step. The title bar reads 'Certificate Import Wizard'. Below the title, the section is 'Certificate Store'. The text says: 'Certificate stores are system areas where certificates are kept.' Below this, it says: 'Windows can automatically select a certificate store, or you can specify a location for'. There are two radio buttons. The first radio button is selected and labeled 'Automatically select the certificate store based on the type of certificate'. The second radio button is unselected and labeled 'Place all certificates in the following store'. Below the second radio button, there is a text box labeled 'Certificate store:' containing 'Personal'. To the right of the text box is a 'Browse...' button. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'. A mouse cursor is pointing at the 'Next >' button.

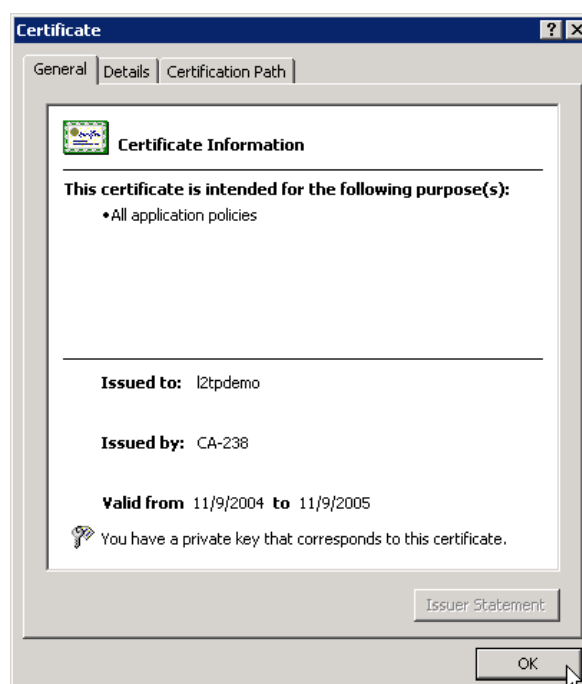
Complete the import procedure with "Next" and "Finish".

From the "Action" menu select "Reload" and the certificate you just imported should appear in folder "Certificates" below "Personal".



Double-click the certificate and inspect it.

The certificate icon on top of the dialog box must not be crossed out. If it is crossed out, it is invalid and you will not be able to establish the VPN connection. You will find some reasons on the next page.



The certificate import is complete.

Some common reasons for an invalid certificate are:

Certificate is expired or not valid yet

Please compare the certificate's period of validity with the current system time

Certificate of the Certification Authority (CA) is missing

Verify if the folder "Trusted Root Certification Authorities > Certificates" contains the certificate of the CA which issued the client's certificate. If not it has to be imported. Ask your CA for their certificate



If you are using SX-GATE's builtin CA to issue certificates, the CA certificate will be imported automatically as it is part of the PKCS#12 file

CA certificate is expired or not valid yet

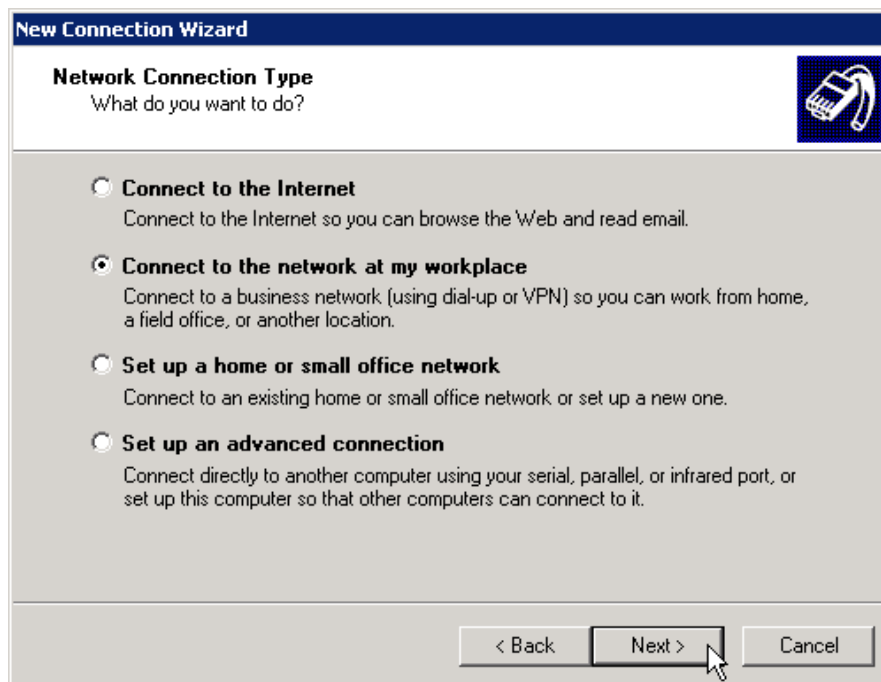
Open the CA certificate with a double-click and verify its period of validity

Connection setup

From the Windows "Start" menu select "Programs > Accessories > Communication > New Connection Wizard".

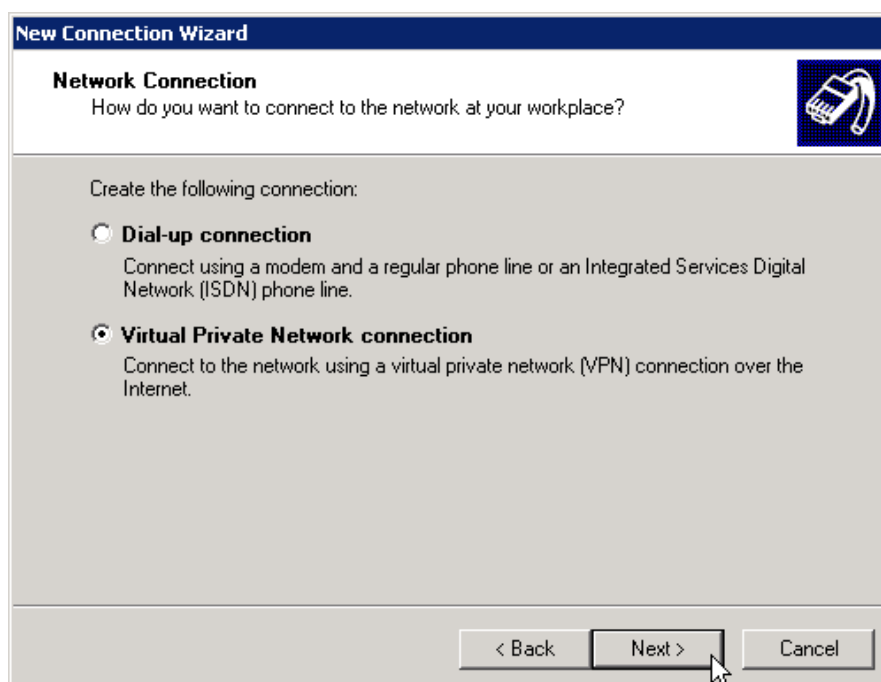


Click "Next" on the welcome screen.
Select "Connect to the network at my workplace".

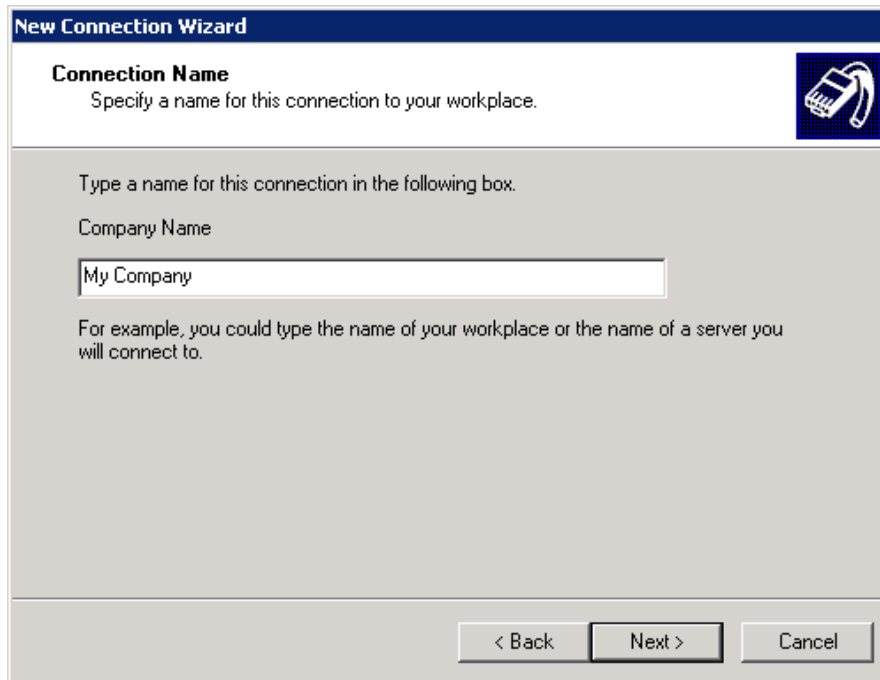


"Next" will let you choose the type of connection.

Pick "Virtual Private Network connection" and continue with "Next".

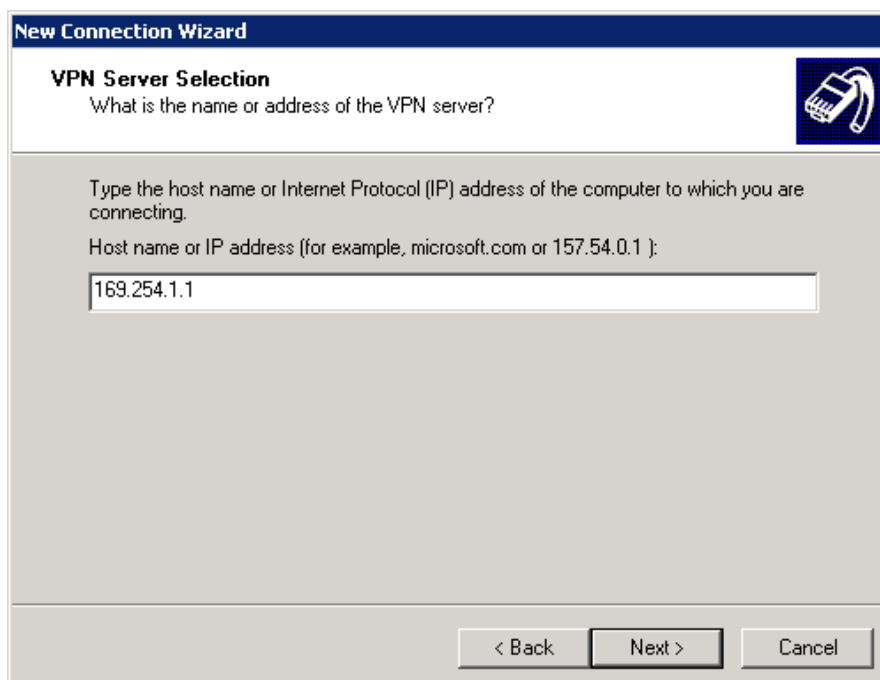


Supply a descriptive name for the connection (e.g. your company's name) and click "Next".



The screenshot shows the 'New Connection Wizard' window. The title bar is blue with the text 'New Connection Wizard'. Below the title bar, the section is titled 'Connection Name' with a sub-instruction: 'Specify a name for this connection to your workplace.' To the right of this text is a small icon of a hand holding a plug. Below this, there is a text box labeled 'Company Name' containing the text 'My Company'. Further down, there is a larger text area with the instruction: 'Type a name for this connection in the following box.' and 'For example, you could type the name of your workplace or the name of a server you will connect to.' At the bottom of the window are three buttons: '< Back', 'Next >', and 'Cancel'.

Specify SX-GATE's external (internet) IP address as VPN server.



The screenshot shows the 'New Connection Wizard' window at the 'VPN Server Selection' step. The title bar is blue with the text 'New Connection Wizard'. Below the title bar, the section is titled 'VPN Server Selection' with a sub-instruction: 'What is the name or address of the VPN server?' To the right of this text is a small icon of a hand holding a plug. Below this, there is a text box labeled 'Host name or IP address (for example, microsoft.com or 157.54.0.1):' containing the text '169.254.1.1'. Further down, there is a larger text area with the instruction: 'Type the host name or Internet Protocol (IP) address of the computer to which you are connecting.' At the bottom of the window are three buttons: '< Back', 'Next >', and 'Cancel'.

"Next" will finish the basic connection setup. It's recommended to let the wizard create a shortcut to this connection on your desktop.

Connection settings

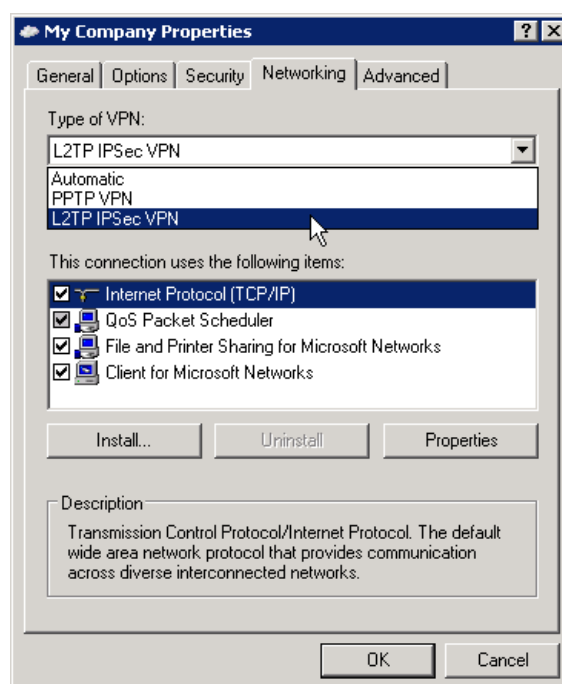
Now start the lately added connection.



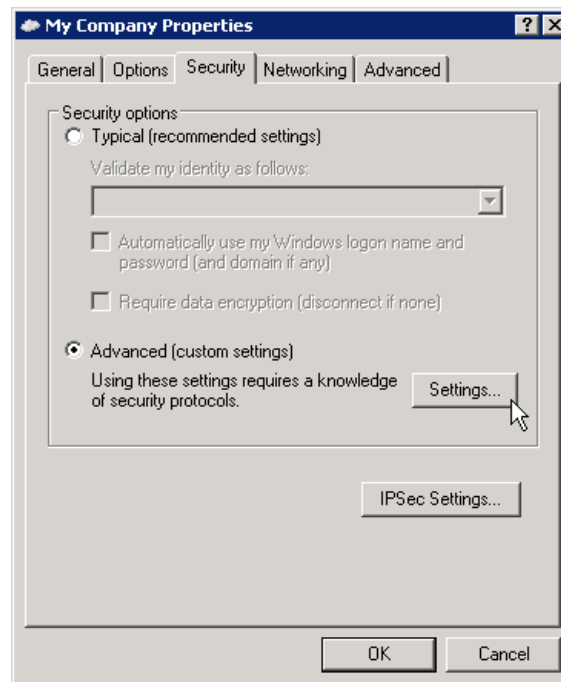
Before connecting, you still have to adjust some settings by clicking "Properties".

Change to tab "Networking".

The type of VPN must be set to "L2TP IPsec VPN".



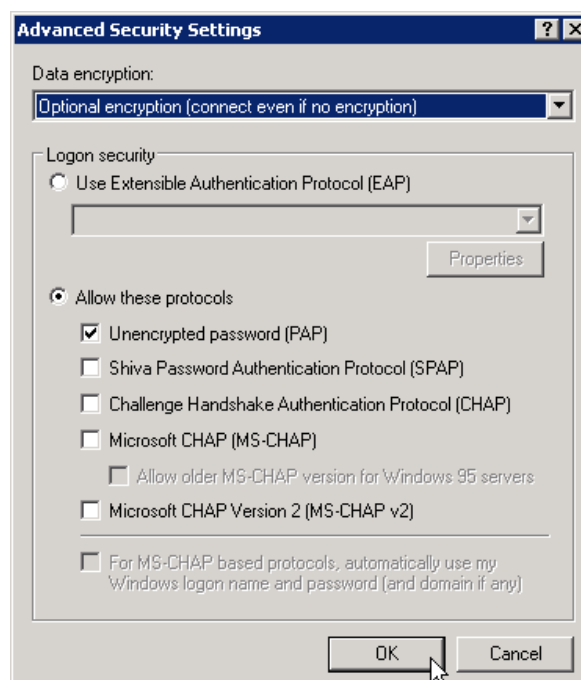
On tab "Security" select the option "Advanced (custom settings)" and click the "Settings" button next to it.



Select "Optional encryption" and allow the use of "Unencrypted Password (PAP)".



Although a security warning will pop up when pressing "OK", these settings are safe. PAP authentication is performed after the IPSec tunnel has been established. Its encryption will protect the transmission of the PAP password.



How do you authenticate?

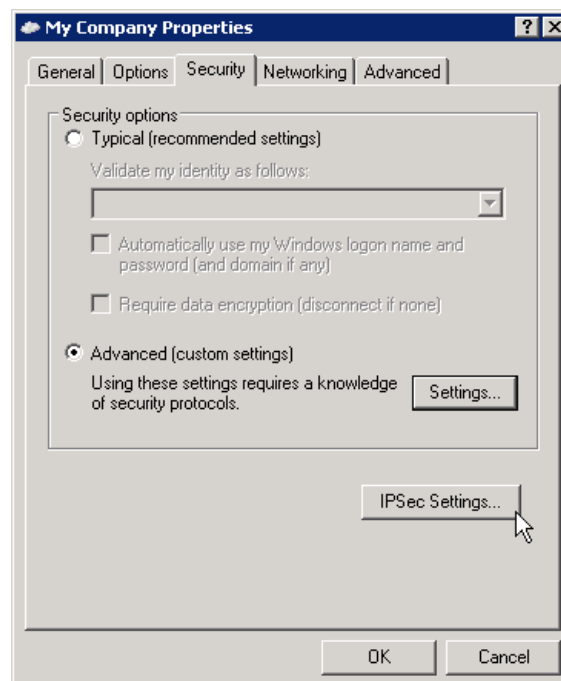
Some Windows releases support authentication using a preshared key. In case this is configured on your SX-GATE you also have to set it up on your Windows system.

How do you authenticate?

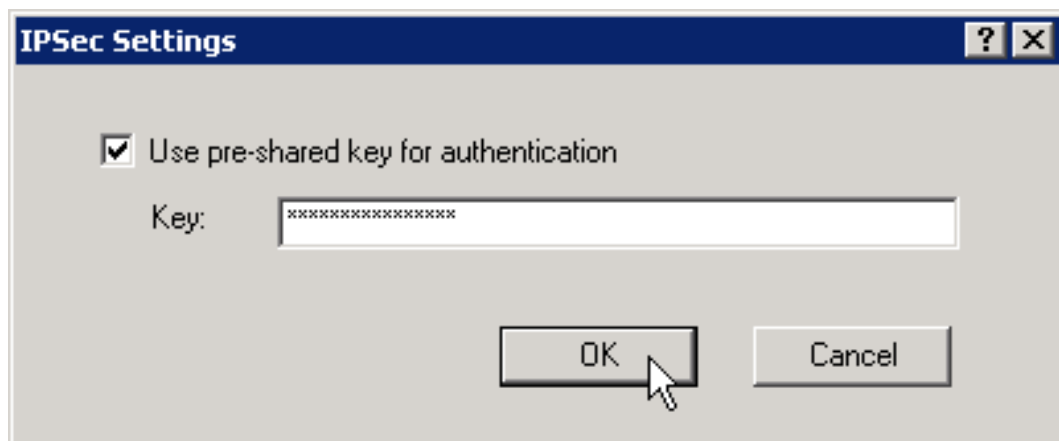
- X.509 certificate
Please read on at [Connect](#) (p. 615)
- preshared key
Please read on at [Preshared Key](#) (p. 614)

Preshared Key

If the IPSec connection is authenticated using a preshared key, you have to click "IPSec Settings" now.



Check "Use pre-shared key for authentication" and specify the same key you configured on SX-GATE.



Connect

Turn back to the connect screen by clicking "OK".

Specify the login and password of a member of the SX-GATE group "system-ras".

Press "Connect" to establish the L2TP connection with SX-GATE. Use e.g. ping to test if the remote network is reachable.



If a dial-up connection is used for internet access, make sure it has been started beforehand.



Troubleshooting

As an L2TP IPsec connection is established in two steps, problems could occur at both stages: IPsec or L2TP. Please inspect the corresponding logfiles, as they might contain error messages which help you to solve the problem.

When problems occur while establishing the IPsec tunnel, SX-GATE's log "IPsec" from menu "Monitoring" -> Log files" might indicate the reason.

Since Windows Vista it became rather complicated to get a diagnostic log of the IPSec connection. However getting an IPSec log in Windows XP is quite easy. It has to be enabled in the registry first:

- Select "Run" from the Windows Start-Menü
- Open the program "regedit"
- Select folder "\\HKEY_LOCAL_MACHINE\\SYSTEM\\CurrentControlSet\\Services\\PolicyAgent"
- Create a new subfolder named "Oakley" by selecting the menu item "Edit > New > Key"
- Change into the "Oakley" folder you just created
- Insert a new entry by clicking "Edit > New > DWORD Value" and name it "EnableLogging"
- Double-click this new entry and assign the value "1"
- You can now close the regedit window
- Now you have to restart the Windows IPSec service (using the command line: "net stop policyagent" and "net start policyagent"; using the services view: restart "IPSEC Services")

Now windows will provide further information on every ipsec connection in the file "%SystemRoot%\\debug\\oakley.log". %SystemRoot% is the Windows base directory.

In case you encounter problems in the L2TP stage, you will find further information in SX-GATE's log "PPP".

If you are not able to find the cause of the problem by inspecting the three logs stated above, please send a cut-out of one connection attempt to technical support.

15.2 Mac OS X

- Please read on at (p. 618)
- Please read on at (p. 618)

- Please read on at (p. 618)
- Please read on at (p. 618)

15.3 Apple iPhone

XAUTH as an alternative

For connecting an iOS device we recommend an IPsec VPN with XAUTH. For XAUTH, iOS fully supports certificates and the iOS device is very easy to configure by profile (.mobileconfig file).

To configure the XAUTH connection on SX-GATE, its VPN server should already be configured. It is highly recommended to use SX-GATE's wizard "IPsec VPN" from the "Wizards" menu. Then add a new connection of type "XAuth Client" to the ipsec interface in menu "Modules > Network". Define an address pool (setting "Virtual IP (Mode Config)") and change the authentication method to "any certificate signed by trusted CA".

As described in chapter "System > Certificate manager > CA certificates > Certificates", section "Create setup package", you can download an iOS profile after creating a new certificate. This file needs to be copied to the client on which you want to setup the XAUTH connection to SX-GATE.

Prerequisites

If you have decided not to configure an IPsec XAUTH connection, we will now show you how to configure an IPsec L2TP connection for an iOS device.

The SX-GATE VPN server should already be configured. It is highly recommended to use SX-GATE's wizard "IPsec VPN" from the "Wizards" menu.



The Wizard automatically sets up the vpn-server for certificate-based authentication. Unfortunately the iPhone supports only certificates purchased from certain CAs. So preshared keys are often used instead to authenticate an iPhone.

If there aren't any existing connections using certificates for authentication, just switch SX-GATE to authentication using "Preshared key". Otherwise, configure a second connection which is basically a copy of the connection for certificate based authentication, just using "Preshared key" for authentication. You will find the connections in menu "Modules > Network" below the ipsec interface (usually ipsec0).

To enter the actual Passphrase (PSK), open menu "Modules > Network" and click on the respective ipsec interface.

Configuration

On your iPhone, run the application "Settings" and select "General ==> Network ==> VPN". To configure a new connection choose "Add VPN Configuration".



Configure VPN account

Before we start with the configuration, make sure that the VPN type is set to "L2TP". Enter a "Description" for the connection and specify the server you want to connect with. This can either be an IP-Address or a DNS-Name of SX-GATE.

At "Account" you set the username used to login to SX-GATE. Please make sure that the user already exists on SX-GATE and is a member of SX-GATE's "system-ras" group. If you like you can enter the user's password, otherwise you will be asked for it everytime you start the connection.

Enter your Pre-Shared-Key in the "Secret" field and activate/de-activate the "Send all Traffic"-Switch depending on your needs.

Save your settings and click on the connection's name to start the connection. Once the tunnel is up you will see a small "VPN"-Symbol appearing in the upper menubar.



16 Contact

You can contact us in a number of ways.

Support hotline: +49-(0)7032-95596-21 (Mon-Thu 9-12 o'clock, 13-17 o'clock, Fri 9-12 o'clock, 13-16 o'clock)

Support email: support@xnetsolutions.de

Postal address:

XnetSolutions KG
Benzstraße 32
D-71083 Herrenberg
Germany

Internet: <http://www.xnetsolutions.de>

17 SX-GATE Support

Your SX-GATE online support (remote maintenance) can take place, if agreed by you, via Internet.

This service is available Monday to Thursday from 9 to 12 o'clock and from 13 to 17 o'clock and Fridays from 9 to 12 o'clock and from 13 to 16 o'clock.

Support hotline SX-GATE: +49-(0)7032-95596-21

E-Mail Support SX-GATE: support@xnetsolutions.de

Further support such as an extensive knowledge base and FAQs can be found at <http://www.xnetsolutions.de> .

Updates can be achieved at <http://update.sx-gate.de> .

Please have the following information at hand with any requests (see My Account -> Contact-> ID card):

Remote maintenance IP address

Version and update level