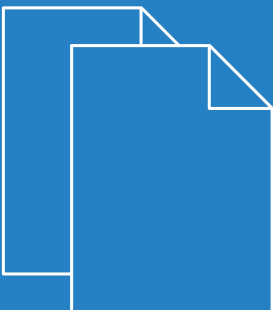


LCOS FX 10.4.0

Addendum



Contents

- 1 Addendum to LCOS FX version 10.4.0.....4**
- 2 Getting started.....5**
 - 2.1 Initial setup.....5
- 3 Factory settings.....11**
- 4 General settings.....12**
- 5 Download license.....13**
- 6 E-mail notifications.....14**
 - 6.1 E-mail settings.....14
 - 6.2 Notification settings.....15
- 7 LANCOM Management Cloud (LMC).....17**
 - 7.1 LANCOM Management Cloud settings.....17
- 8 VPN.....18**
 - 8.1 VPN.....18
 - 8.1.1 IPSec.....19
 - 8.1.2 VPN-SSL.....36

Copyright

© 2019 LANCOM Systems GmbH, Würselen (Germany). All rights reserved.

While the information in this manual has been compiled with great care, it may not be deemed an assurance of product characteristics. LANCOM Systems shall be liable only to the degree specified in the terms of sale and delivery.

The reproduction and distribution of the documentation and software supplied with this product and the use of its contents is subject to written authorization from LANCOM Systems. We reserve the right to make any alterations that arise as the result of technical development.

Windows® and Microsoft® are registered trademarks of Microsoft, Corp.

LANCOM, LANCOM Systems, LCOS, LANcommunity and Hyper Integration are registered trademarks. All other names or descriptions used may be trademarks or registered trademarks of their owners. This document contains statements relating to future products and their attributes. LANCOM Systems reserves the right to change these without notice. No liability for technical errors and/or omissions.

This product contains separate open-source software components which are subject to their own licenses, in particular the General Public License (GPL). If the respective license demands, the source files for the corresponding software components will be provided on request. Please send an e-mail to gpl@lancom.de.

Products from LANCOM Systems include software developed by the "OpenSSL Project" for use in the "OpenSSL Toolkit" (www.openssl.org).

Products from LANCOM Systems include cryptographic software written by Eric Young (ey@cryptsoft.com).

Products from LANCOM Systems include software developed by the NetBSD Foundation, Inc. and its contributors.

Products from LANCOM Systems contain the LZMA SDK developed by Igor Pavlov.

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Wuerselen

Germany

www.lancom-systems.com

1 Addendum to LCOS FX version 10.4.0

This document describes the changes and enhancements in LCOS FX version 10.4.0 since the previous version.

2 Getting started

As of LCOS FX version 10.4.0, putting your LANCOM R&S® Unified Firewall into operation is now supported by a wizard, which greatly simplifies the process.

2.1 Initial setup

1. Remove the preinstalled LANCOM R&S® Unified Firewall device from the packaging.
2. Connect a patch cable to the port labeled **eth1** on the front of your LANCOM R&S® Unified Firewall device and the Ethernet port of your computer.
3. Connect a patch cable to the port labeled **eth0** on the front of your LANCOM R&S® Unified Firewall device and the LAN port of the device (e.g. your router, DSL or cable modem) that you received from your Internet access provider. Make sure this device is switched on.
4. Make sure the network adapter of your computer is set to "Automatically configure the IP address".
5. Switch on your LANCOM R&S® Unified Firewall device.
6. Start a web browser on your computer.
7. Enter the following into the address bar of the browser: <https://192.168.1.254:3438>.
8. Create an exception for the certificate warning.
The LANCOM R&S® Unified Firewall login page appears.
9. On the login page of the LANCOM R&S® Unified Firewall web client, enter `admin` as **User Name** and the default **Password** `admin`.

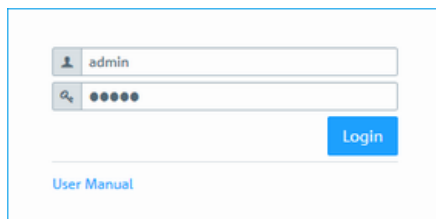


Figure 1: Login page of the LANCOM R&S® Unified Firewall web client

10. Click on **Login**.
11. After the first login with the default credentials, the system prompts you to accept the End User License Agreement (EULA) and then change the following two passwords:
 - The password for the user `admin` – you need this password to login to the LANCOM R&S® Unified Firewall web client.
 - The support password – the support password is the password used by the technical supporter to login to your LANCOM R&S® Unified Firewall. Keep it secure and protected from unauthorized access.

The new user password and support password must contain no less than eight and no more than 255 characters. You can use Latin letters, including German umlauts, as well as numbers and special characters. Do not use Cyrillic or other alphabets. You must use characters from at least three of the categories capital letters, lowercase letters, numbers, and special characters.



This step is mandatory.

12. Click on **Accept & Login** to accept the new passwords and the EULA.

The setup wizard appears.



With the exception of the language selection at the start of the setup wizard, you can cancel the wizard at any time with the **Cancel Wizard** button. After canceling the wizard, you can continue with a manual setup following the steps [Configuring the Internet Connection](#) and [Enabling Internet Access](#).

For most of the setup wizard, you can use the **Back** and **Next** buttons to navigate.

13. Select the language for the setup wizard and web client. You can switch the language of the web client later as required.

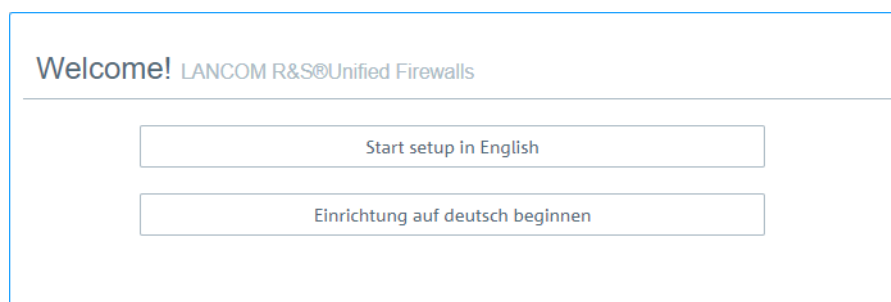


Figure 2: Welcome page of the setup wizard

14. To restore the configuration from a previous installation, click on **Select** to choose a backup file. Enter the associated backup password. Then click **Restore the backup and restart**.

The setup wizard is then closed, the configuration is restored from the backup, and the firewall restarts.

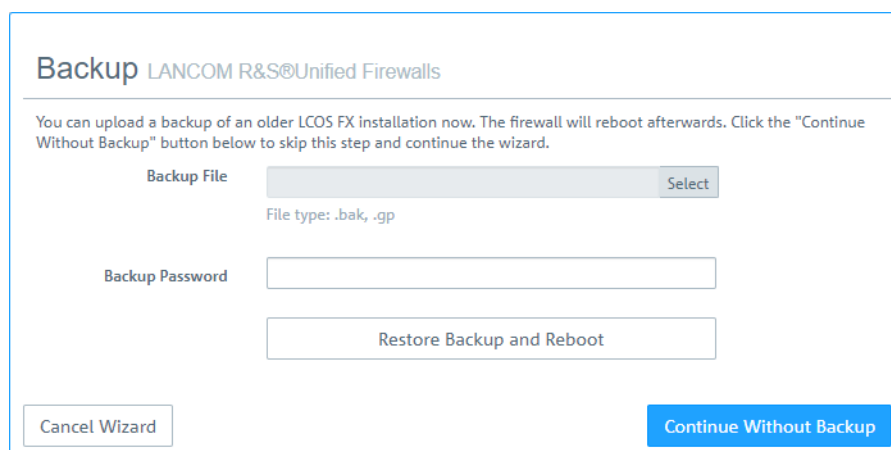


Figure 3: Optional: Restore a previous configuration from a backup

Alternatively, you can continue with a new installation with **Continue without backup**.

15. Configure the following general firewall settings:

Firewall hostname


Give your firewall a name to be used as the host name.

Time zone

The time zone is preset with the time zone currently set in the browser. Change this setting if necessary.

Send usage statistics

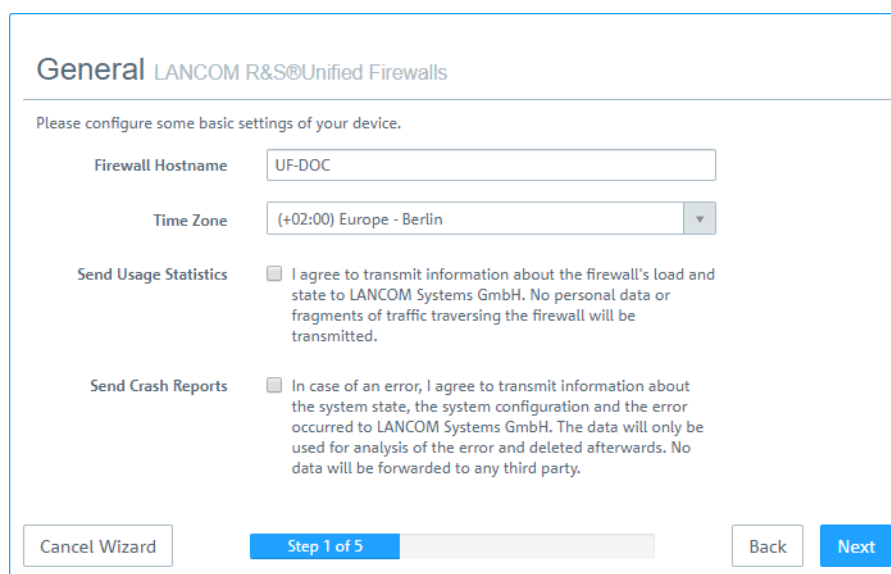
You can optionally allow information about the firewall's load and state to be recorded and sent to LANCOM Systems GmbH. No personal information or any of the firewall traffic will be transmitted.

 You can change this setting later. See also [General settings](#).

Send crash reports

In the event of a crash, you can optionally allow general information about the system status, current system configuration and the occurring error to be transmitted to LANCOM Systems GmbH. The data is used solely for error analysis and is then deleted. No data is disclosed to any third parties.

 You can change this setting later. See also [General settings](#).



General LANCOM R&S Unified Firewalls

Please configure some basic settings of your device.

Firewall Hostname:

Time Zone:


Send Usage Statistics: ☐ I agree to transmit information about the firewall's load and state to LANCOM Systems GmbH. No personal data or fragments of traffic traversing the firewall will be transmitted.

Send Crash Reports: ☐ In case of an error, I agree to transmit information about the system state, the system configuration and the error occurred to LANCOM Systems GmbH. The data will only be used for analysis of the error and deleted afterwards. No data will be forwarded to any third party.

Cancel Wizard Step 1 of 5 Back Next

Figure 4: General settings of the firewall

- Set the **Internet interface** as the firewall port (default: **eth0**) that is connected to the device supplied by your Internet service provider. You then enter your option for **Internet access**:

 Depending on your selection, you can configure the relevant data.

DHCP

The IP address for this interface is obtained via DHCP.

Static configuration

Enter the **IP address with prefix length** (CIDR notation), the **default gateway** and the **DNS server**.

ADSL / SDSL

Enter the **username** and the **password** that you have received from your Internet service provider.

VDSL

Enter the **VLAN ID**, the **username** and the **password** that you have received from your Internet service provider.

Internet Access LANCOM R&S Unified Firewalls

Please set up your firewall's internet access, so that LCOS FX system updates and UTM signature updates can be downloaded. In the next steps of the wizard, you can configure how the internet connection is shared with your local networks.

Internet Interface

Internet Access ☒ DHCP
☐ Static Configuration
☐ ADSL/SDSL
☐ VDSL

Cancel Wizard Step 2 of 5 Back Next

Figure 5: Internet access

17. Here you configure the local network to which the firewall is (to be) connected. Each line corresponds to a network interface of the firewall (**Interface** column).

You can enable/disable an interface, depending on whether you want to use it or not (**Active** column). The Internet interface cannot be deactivated.

In the field **IP and prefix length**, enter the IP that the firewall should use on this interface, together with the prefix length (CIDR notation). If you leave the field blank, the firewall will not have an IP connection on this interface. If this is the case, you will be unable to use this interface to access the firewall and you cannot provide a DHCP server, web or mail access for clients connected via this interface. Each interface should have its own subnet.

To enable a DHCP server on an interface, select the appropriate checkbox **Enable DHCP server**. The DHCP pool depends on the firewall IP associated with this port and is preset to the largest continuous range available on the subnet.

You can permit typical Internet applications (**Web** and **Mail**) for clients connected to an interface by selecting the corresponding checkbox. **Web** allows clients to connect to the Internet via HTTP. **Mail** enables SMTP, POP3 and IMAP traffic. This includes the SSL/TLS versions of these protocols.

LAN LANCOM R&S Unified Firewalls

Set up the firewall for your LAN.

Active	Interface	IP and Prefix Length	Enable DHCP Server	Allow Internet Access*
<input checked="" type="checkbox"/>	eth0	This interface is used to access the internet.		
<input checked="" type="checkbox"/>	eth1	<input type="text" value="192.168.56.101/24"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/> Web <input checked="" type="checkbox"/> Mail

* Allowing internet access of type "Mail" will allow SMTP, POP3 and IMAP connections. Type "Web" will allow HTTP connections. The SSL/TLS variants of these protocols will be allowed too.

Cancel Wizard Step 3 of 5 Back Next

Figure 6: Local networks

18. Select the security features **Anti-Malware**, **IDS/IPS** and/or **Content Filter**, which are to be activated. Depending on your device, not all features may be available.



After being started for the first time, or following a re-installation, the LANCOM R&S® Unified Firewall runs for 30 days as a demo version. You cannot perform a backup during the trial period. At the end of the trial period, the firewall will retain your configuration. The UTM features will be disabled and you can no longer save any changes.

For more information, please see [License](#).

Security LANCOM R&S® Unified Firewalls

Which security features should be enabled?

Anti-Malware

The anti-malware engine monitors mail and web traffic. It protects you against malicious software from the internet using state-of-the-art machine learning and sandboxing technology.

IDS/IPS

The IDS/IPS engine monitors the network traffic between your local networks and the internet. Malicious traffic will be dropped and attacks on your network blocked.

Content Filter

The content filter makes sure no unwanted web sites are accessible. The default setting will block pornographic, criminal and violent web sites.

i For the use of the security features outside of the trial period you require an appropriate license.

Cancel Wizard Step 4 of 5 Back Next

Figure 7: Security features

19. Here you see a summary of your settings and, if necessary, you can go back and adjust them. Click **Finish** if everything is to your satisfaction.

Summary LANCOM R&S® Unified Firewalls

Please review your input.

General Internet Access Security

Firewall Hostname	UF-DOC	Type	DHCP	Anti-Malware	✓
Time Zone	Europe - Berlin			IDS	✓
Send Usage Statistics	✓			Content Filter	✓
Send Crash Reports	✓				

LAN

IP and Prefix Length	DHCP	Web	Mail
eth0	This interface is used to access the internet.		
eth1	192.168.56.101/24	✗	✓

Cancel Wizard Step 5 of 5 Back Finish

Figure 8: Summary of settings

20. Wait for the setup wizard to finish. You will then see the links to use to access the web client after the setup wizard has completed. You can either click these links or click OK to go to the web client.

If you want to use the automatically generated certificate for the web proxy, download it and roll it out to your clients.

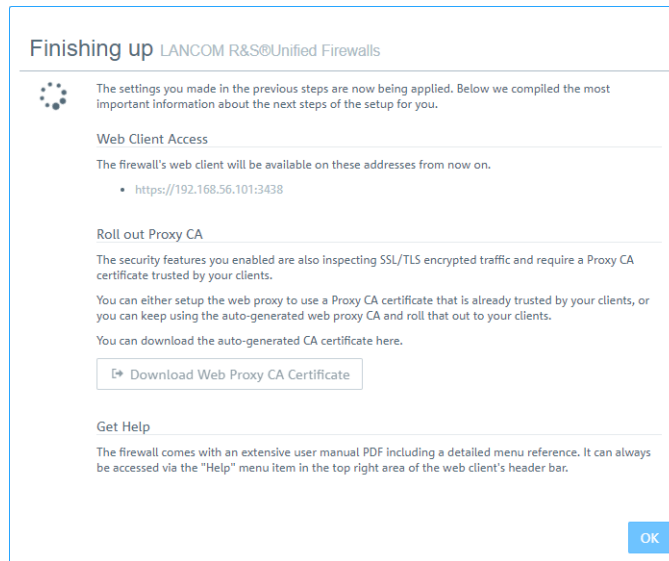


Figure 9: Finishing up



If you want to use the setup wizard again, you will need to reset your firewall to its factory defaults. See also [Header](#).

3 Factory settings



As of LCOS FX version 10.4.0 you can reset your LANCOM R&S® Unified Firewall to its factory settings. This new option can be found in the **System** menu in the header.

4 General settings

As of LCOS FX version 10.4.0 you can use this new dialog to make some central settings.

Navigate to **Firewall > General settings** to open an editing window where you can adjust some of the central settings for your LANCOM R&S® Unified Firewall.

In the **General settings** editing window you can modify the following parameters:

Input box	Description
Host name	Host name of the firewall.
Domain	Domain of the firewall. If the firewall is connected to an Active Directory, enter the corresponding Active Directory domain here.
Send usage statistics	<div>Collect information about the load and the state of the firewall and send this to LANCOM Systems GmbH.</div> <div> No personal information or any of the firewall traffic will be transmitted.</div>
Send crash reports	<div>In the event of an error, general information about the system status, the current system configuration and the error that occurred is transferred to LANCOM Systems GmbH.</div> <div> The data is used solely for error analysis and is then deleted. No data is disclosed to any third parties.</div>

If you have made changes, you can use the buttons at the bottom right of the edit window to save them (**Save**) or discard them (**Reset**). Otherwise you can close the window (**Close**).

5 Download license

As of LCOS FX version 10.4.0, you are able to download an uploaded license again. In the license manager, simply click on the license file which is displayed as a link on the tab **General** next to **Download** to start the file download.

6 E-mail notifications

As of LCOS FX version 10.4.0, you stay up to date when certain system events occur by having your LANCOM R&S® Unified Firewall notify you by e-mail. See the following sections for details.

6.1 E-mail settings

The e-mail settings are necessary for using the notification system. You can use this to receive e-mail messages about specific types of notification, either immediately or regularly in an aggregated form. Further details are available under [Notification settings](#) on page 15.

Navigate to **Firewall > E-mail settings** to open an editing window where you can configure the sender and message encryption. Optionally, settings are available for a relay server if e-mails cannot be sent directly.


In the **E-mail settings** editing window you can adjust the following parameters:

Input box	Description
I/O	A slider button indicates whether the E-mail settings are enabled (I) or disabled (O). Click on the slider button to change this.
Sender address	Sender e-mail address of the firewall system.
Connection security	Choose one of the possible options <i>None</i> , <i>TLS</i> or <i>StartTLS</i> .
Validate remote certificate	If enabled, the firewall verifies the certificate of the destination server or relay.
S/MIME certificate	If this is specified, then the firewall encrypts all outgoing e-mails with the public key of the selected certificate.

On the **Relay** tab you can configure preset values for the following items:

Input box	Description
Server	The address of the e-mail server.
Port	The port used by the e-mail server.
User name	Name used by the firewall to log in to the e-mail server.
Password	Password used by the firewall to log in to the e-mail server.

You can test your settings by using the button **Send test mail**. A dialog opens where you can enter a **recipient address**. You then click the **send** button.

 If you are using a relay server, please note that the subsequent status message only tells you if the relay server accepted the e-mail. If the relay server is unable to deliver the message, this can only be seen on the relay server itself.

If you have made changes, you can use the buttons at the bottom right of the edit window to save them (**Save**) or discard them (**Reset**). Otherwise you can close the window (**Close**).

6.2 Notification settings


The notification systems sends e-mail messages about specific types of notification, either immediately or regularly in an aggregated form. This requires an active e-mail function in which at least one sender is set. Security comes with the optional settings **Validate remote certificate** to verify the remote site before sending e-mail and **S/MIME certificate** to encrypt the outgoing mail. Further details are available under [E-mail settings](#) on page 14

Navigate to **Monitoring & statistics > Notification settings** to open an editing window where you can configure the following items:


Table 1: General

Input box	Description
I/O	A slider button indicates whether the notification settings are enabled (I) or disabled (O). Click on the slider button to change this.
Notification language	Set the language used in the notification e-mails. If the dialog is opened for the first time, the language is set to that used for the web client.
Subject template	Set the subject of the notification e-mails.
Recipients	List of recipient addresses where the notifications are sent. Click on ⊕ on the right-hand side to add your entry to the list.

In the **Aggregated notifications** editing window you can modify the following items:

Input box	Description
Aggregation interval	The events are collected and summarized in an e-mail at a specified interval. Enter the interval in minutes in which events are collected before they are sent as a message.
Max. number of notifications per mail	<p>Here you specify how many events are combined in an e-mail. This determines how many mails are sent at the end of each aggregation interval. At the same time, this limits the maximum size of the e-mail.</p> <p> If necessary, observe any spam guidelines of the recipient.</p>

In the **Instant notifications** editing window you can modify the following items:

Input box	Description
Max. number of mails per hour	<p>In the occurrence of an event of a type flagged for Instant notification, an e-mail is sent to the recipient immediately. Depending on the settings in the Notification Types section and the events that occur, large numbers of e-mails could be sent in a short time. This could lead to them being blocked if provider policies at the receiving end are infringed. To avoid this, you can use this item to limit the number of instant notifications sent per hour.</p> <p> All instant notifications are also sent in the next aggregated e-mail.</p>

In the **Notification types** editing window you can modify the following items:

Input box	Description
Filter	The displayed notification fields can be filtered by their name and set value.
Set for all selected notifications	All currently displayed notification fields are adjusted to the value set here. For example, to set all of the fields for IPSec to Instant , go to Filter and enter "ipsec", and you can change all of the IPSec-related notification fields to Instant .


6 E-mail notifications

Input box	Description
Expected system restart	Notification when the system is restarted as expected.
Unexpected system restart	Notification when the system is restarted unexpectedly.
HA role switch	Notification when a role switch is performed in high availability mode.
Internet connection offline	Notification when disconnected from the Internet.
Backup Internet connection activated	Notification when the default Internet connection is disconnected and the backup connection takes over.
Internet connection online	Notification when connecting to the Internet.
Default Internet connection restored	Notification when the default Internet connection is in use again.
IPSec site-to-site tunnel online	Notification when an IPSec site-to-site tunnel is established.
IPSec site-to-site tunnel offline	Notification when an IPSec site-to-site tunnel is disconnected.

If you have made changes, you can use the buttons at the bottom right of the edit window to save them (**Save**) or discard them (**Reset**). Otherwise you can close the window (**Close**).

7 LANCOM Management Cloud (LMC)

As of LCOS FX version 10.4.0 you can manage your LANCOM R&S® Unified Firewall via the LMC.

Icon / button	Description
	This marks all objects and settings that are managed by the LANCOM Management Cloud (LMC). These can be viewed with the web client, but cannot be edited. Objects managed by the LMC cannot be referenced. This means, for example, that an application filter profile created by the LMC cannot be used in a self-created desktop connection.

7.1 LANCOM Management Cloud settings

These are the settings for the configuration and monitoring of your device via the LANCOM Management Cloud (LMC).

Navigate to **Firewall > LMC Settings** to open an editing window where you can view and modify the settings for the LMC.


In the **LMC Settings** editing window you can adjust the following parameters:

Input box	Description
I/O	A slider button indicates whether firewall management via the LANCOM Management Cloud is enabled (I) or disabled (O). Click on the slider button to change the status of this option.
LMC domain	Enter the domain name for the LMC here. By default, the domain is set to the Public LMC for the first connection. If you wish to manage your device with your own Management Cloud ("Private Cloud" or "on-premises installation"), please enter your LMC domain.
Activation code	As an alternative to entering the serial number and the cloud PIN supplied with the device, it can also be assigned to a project in the LMC by means of an activation code. In the LMC go to Devices , click on Activation codes and then on Create activation code . This creates a temporary activation code. While it remains valid, this code can be used to activate any number of LANCOM devices, i.e. to transfer them to the LMC.

8 VPN

As of LCOS FX version 10.4.0, the menus for VPN and all of the IPSec-related dialogs have been restructured with a new implementation of this feature. See the following sections for details.

8.1 VPN

With the settings under  **VPN** you can configure your LANCOM R&S® Unified Firewall as a Virtual Private Network server to provide client-to-site (C2S) VPN connections. This allows computers in another location to use IPSec and VPN-SSL to securely access resources on the local network. A *site-to-site* (S2S) VPN gateway can use IPSec and VPN-SSL to establish a secure communication channel between two remote networks via the Internet.

Client-to-site VPN connections

A client-to-site VPN connection provides access to the corporate network from the outside. Authentication is performed either via IPSec with issued certificates, by means of a PSK (pre-shared key), or via VPN-SSL with certificates.

Client-to-site connections over IPSec and VPN-SSL operate in one of two modes, depending on the client settings:

- In the *split-tunnel mode*, the only communication to pass through the firewall is that between the client and the internal network (e.g. a company network). Clients can reach devices in the internal network through the tunnel. For other destinations (e.g. the Internet), the packets are not routed by the LANCOM R&S® Unified Firewall.

Example: A user dials in to a corporate network remotely from a hotel's wireless network using a VPN software client. Split tunneling allows the user to connect to file servers, database servers, mail servers, and other company network resources through the VPN connection. If the user connects to Internet resources (websites, FTP sites, etc.), the connection request is sent directly through the hotel network gateway.

- In the *full-tunnel mode* all traffic is routed back to your LANCOM R&S® Unified Firewall, including communication with the Internet.

Full tunneling does not allow the user to access the Internet directly through hotel networks. All of the traffic sent by the client will be sent to the firewall while the VPN connection is active.



C2S connections over IPSec are established using a normal VPN client, such as the LANCOM Advanced VPN Client. Please refer to [IPSec connection settings](#) on page 24 for further information.



VPN-SSL C2S connections are established using a normal VPN client. Please refer to [VPN SSL connection settings](#) on page 38 for further information.

Site-to-site VPN connections

In the case of a site-to-site connection, two locations are connected via an encrypted tunnel to form a virtual network and they exchange data through this tunnel. The two locations can have fixed IP addresses. Authentication is performed either via IPSec with issued certificates, by means of a PSK (pre-shared key), or via VPN-SSL with certificates.

IPSec

Internet protocol security (IPSec) is a set of protocols that operates at the network layer or the link layer and secures the exchange of packets over untrusted networks (such as the Internet) by authenticating and encrypting each IP packet in a communication session. IPSec meets the highest security requirements.

VPN-SSL

VPN over SSL provides a fast and secure way to get a roadwarrior connected. The biggest advantage of VPN-SSL is that all traffic passes through a TCP or UDP port and, unlike IPSec, no other special protocols are required.



Before setting up VPN connections, make sure that you have installed the necessary certificates as described in [Certificate Management](#).

8.1.1 IPSec

The IPSec (Internet Protocol Security) suite operates on the network layer and uses the authentication and encryption of IP packets to secure communication in untrusted networks.

For a site-to-site connection over IPSec, you need two VPN-IPSec-enabled servers. For a client-to-site connection, you need separate client software.

Your LANCOM R&S® Unified Firewall is able to use the IPSec protocol suite to establish and operate secure connections. This is made possible by ESP in tunnel mode. The key exchange can be performed using either version 1 of the IKE protocol or the newer IKEv2. You can choose between using pre-shared keys or X.509-standard certificates. IKEv1 also allows authentication via XAUTH. IKEv2 additionally supports authentication via EAP.

IPSec settings

You can enable IPSec and configure the settings under **VPN > IPSec > IPSec Settings**:

Table 2: General

Input box	Description
I/O	A slider button indicates whether IPSec is enabled (I) or disabled (O). Click on the slider button to change the status of this option.
Excluded interfaces	<p>This selection list is used to select interfaces that should not be used by the IPSec service. If nothing is entered here, then all interfaces are excluded on the system, including those that are newly created or generated automatically.</p> <p>Usually, exception interfaces and IP addresses are required when all traffic is sent to the central office through an IPSec tunnel. In a case like this, you have to be careful to ensure that the local networks remain accessible. By default, IPSec has a higher priority than normal routes. Consequently, even packets destined for local area networks could be sent to the VPN tunnel instead. Under normal circumstances, the default setting which excludes all local interfaces means that the local networks can always be reached.</p>
Excluded IP address	<p>Enter the IP addresses in CIDR format. Under no circumstances will packets for these networks be routed to a tunnel, even if a tunnel is configured for the destination address.</p> <p>Click on ⊕ on the right-hand side to add your entry to the list of IP addresses.</p>
Proxy ARP	If this option is enabled, the firewall will respond to ARP requests from local networks for virtual IP addresses for IPSec clients by sending its own MAC address.


Table 3: DHCP server

Input box	Description
Active	<p>IPSec can use a DHCP server to assign virtual IP addresses to the connected IPSec clients. You can enable this function here.</p> <p>To use this for an IPSec connection, go to Virtual IP pool and select the option DHCP virtual IP pool.</p>
IP address	Enter the IP address of the DHCP server. This can be either the address of a DHCP server or a broadcast address of a network.

Table 4: RADIUS server

Input box	Description
Active	In conjunction with EAP or XAUTH, IPsec can use the user management of a RADIUS server to authenticate the connection. Also, the RADIUS server can assign IP addresses to IPsec clients. To do this for an IPsec connection, go to Virtual IP pool and select the option RADIUS virtual IP pool . You can enable this function here.
IP address	IP address of the RADIUS server
Port	The port the RADIUS server.
Password	Password for accessing the RADIUS server.


If you have made changes, you can use the buttons at the bottom right of the edit window to save them (**Save**) or discard them (**Reset**). Otherwise you can close the window (**Close**).

Click  **Activate** in the toolbar at the top of the desktop to apply your configuration changes.

Security profiles

Under **VPN > IPsec > Security profiles** you will find a list of predefined profiles that you can extend with custom profiles.

 The predefined profiles cannot be edited or deleted.

 If used security profiles are changed, all related connections can be restarted in the extended list bar. Security profiles are selected in the templates and connections.



Click on  to add a new security profile.

Table 5: General settings

Input box	Description
Name	Give the security profile a descriptive name.
Used in	Indicates the IPsec connections currently using this profile.
Data compression	If you select data compression here, it will be activated for all connections using this profile. This saves bandwidth, but it also increases the CPU load.  If you enable data compression, it must also be activated at the remote site.


ISAKMP (IKE)

This tab is used to define security settings for the IKE phase. IKE defines how security parameters are negotiated and shared keys exchanged

Table 6: ISAKMP (IKE)

Input box	Description
IKE version	Select IKEv1 or IKEv2
Encryption algorithms	From the available encryption algorithms, select the ones you want to use from the list.
Authentication algorithms	From the available authentication algorithms, select the ones you want to use from the list.

Input box	Description
DH groups	From the available Diffie-Hellman groups, select the ones you want to use from the list.
SA lifetime	Enter the SA lifetime in seconds.
Mobile IKE (IKEv2 only)	This option is available for IKEv2 only and allows you to change IP addresses without disconnecting.

 The encryption algorithms, authentication algorithms, and DH groups defined here are used in establishing the IPSec connection to negotiate an encryption-authentication combination with the remote site. The more entries are defined here, the higher the number of possible combinations.

 With IKEv1, the number of possible combinations is limited to just over 200. There is no limit with IKEv2.

IPSec (ESP)

Encapsulating Security Payload (ESP) provides mechanisms to ensure the authenticity, integrity and confidentiality of the transmitted IP packets. These settings thus determine the encryption and authentication algorithms used for the actual IP packets.

Table 7: IPSec (ESP)


Input box	Description
Encryption algorithms	From the available encryption algorithms, select the ones you want to use from the list.
Authentication algorithms	From the available authentication algorithms, select the ones you want to use from the list.
DH-Groups	From the available Diffie-Hellman groups, select the ones you want to use from the list.
SA lifetime	Enter the SA lifetime in seconds.

Click on **Create**.

The **Security profile** dialog closes. The new security profile is added to the list of available security profiles in the object bar.

Virtual IP pools


Virtual IP pools can be used to send IP address configurations to connected clients. The virtual IP pools are available for selection on the **Tunnel** tab of the templates and connections.

Under **VPN > IPSec > Virtual IP pools** you will find, on the one hand, the predefined and non-modifiable virtual IP pools for the DHCP and RADIUS servers, and on the other hand the **Default virtual IP pool** that you can modify. Alternatively you can click on  to add a new virtual IP pool.

 The predefined profiles cannot be edited or deleted.


Table 8: Virtual IP pool

Input box	Description
Name	Give the virtual IP pool a descriptive name.
Used in	Indicates the IPSec connections currently using this virtual IP pool.
IP pool	Network address from which IP addresses are sent to the clients.
Preferred DNS server	IP address of the preferred DNS server

Input box	Description
Alternate DNS server	IP address of the alternative DNS server
Preferred WINS server	IP address of the preferred WINS server
Alternate WINS server	IP address of the alternative WINS server
DNS search domains	List of DNS search domains. Click on  on the right-hand side to add your entry to the list of DNS search domains.

Click on **Create**.

The **Virtual IP pool** dialog closes. The new pool is added to the list of available virtual IP pools in the object bar.

 If used virtual IP pools are changed, all related connections can be restarted in the extended list bar.

Templates

Connection templates are useful for pre-defining values for connections that are commonly used. Except for the template name, all values are optional and populate the various fields of a VPN connection created using this template.

Various templates have been predefined, such as the template "LANCOM Advanced VPN Client" to simplify IPSec connections with this client. The template "(empty)" is used if the values of an existing connection should be deleted.

 The predefined templates cannot be edited or deleted.

Under **VPN > IPSec > Templates** you can open the window **IPSec connection template**. Use the **IPSec connection template** windows to view and configure the following information:

Table 9: IPSec connection template

Input box	Description
Name	Give the template a descriptive name.
Security profile	Select one of the predefined security profiles.


On the **Connection** tab you can configure the presets for the following fields:

Table 10: Connection

Input box	Description
Connection	By optionally selecting a network or Internet connection, its IP addresses will be used for the IPSec connection.
Listening IP addresses	As an alternative to Connection , you can also enter user-specified IP addresses. If IP addresses are entered here, the Connection setting is ignored. If neither Connection nor Listening IP addresses are set, the IPSec service will automatically use one of the configured IP addresses of all connections.
Remote gateway	This address is necessary for the Initiate connection option in order to determine the address of the remote site.
Initiate connection	The firewall will connect to the address specified in the Remote gateway field.
Force NAT-T	NAT-T is usually set automatically if the connection requires it. If that mechanism fails, this option forces the use of NAT-T on a connection.

On the **Tunnels** tab you can configure the presets for the following fields:

Table 11: Tunnel

Input box	Description
Local networks	Local networks to be connected to the remote site.
Remote networks	Remote networks to connect to the local area networks.  All of the configured local networks are connected to all of the configured remote networks. For IKEv1 connections and IKEv2 connections with the option IKEv2 compatibility mode enabled, the maximum number of combinations is limited to 25. There is no limit for IKEv2 with the option IKEv2 compatibility mode disabled.
Virtual IP pool	The remote site is assigned an IP address from the configured IP pool.
IKEv2 compatibility mode	Instead of sending all configured local and remote networks through a single tunnel, a single tunnel is created for each connection between two networks (as with IKEv1). This option only applies to IKEv2 connections.

On the **Authentication** tab you can configure the presets for the following fields:

Table 12: Authentication

Input box	Description
Authentication type	Specify the authentication type. Possible values: <ul style="list-style-type: none"> > Certificate – authentication is based on a local and a remote certificate. > Certificate Authority – authentication is performed through a local and a remote certificate signed by the selected CA. > PSK (preshared key) – authentication is based on the entry of a password.
PSK (preshared key)	For authentication type PSK (preshared key) only – specify the required password here.
Local certificate	The certificate of the firewall for authentication. This must contain a private key.
Local identifier	If this field is empty, PSK authentication automatically uses the outgoing IP address of the firewall and, for certificate authentication, the distinguished name (DN) of the selected local certificate. <ul style="list-style-type: none"> > For PSK authentication, the following values are allowed: IP addresses, fully qualified domain names (FQDN), e-mail addresses (FQUN), and free text between quotation marks ("). > For certificate authentication, the following values are allowed: The distinguished name (DN) of the selected certificate, wildcard DN – all DN items must be present (in the correct order), but may be specified as a wildcard (e.g. CN=*) – any subject alternative names (SAN) of the selected certificate.
Remote certificate	Only with authentication type "Certificate": Certificate of the remote site.
Certificate authority	Only with authentication type "Certificate Authority": A CA whose signed certificates can be used for authentication.
Remote identifier	If this field is empty, PSK authentication automatically uses the IP address of the remote gateway (if set). For certificate authentication, the distinguished name (DN) of the selected remote certificate. <ul style="list-style-type: none"> > For PSK authentication, the following values are allowed: IP addresses, fully qualified domain names (FQDN), e-mail addresses (FQUN), and free text between quotation marks ("). > For certificate authentication, the following values are allowed: The distinguished name (DN) of the selected certificate, wildcard DN – all DN items must be present (in the correct order), but may be specified as a wildcard (e.g. CN=*) – any subject alternative names (SAN) of the selected certificate.

Input box	Description
EAP / XAUTH	Enables the use of additional user authentication. XAUTH for IKEv1 uses the local user database or a RADIUS server (depending on whether RADIUS is enabled in the IPSec settings or not). EAP for IKEv2 only works with an external RADIUS server, which must be activated in the IPSec settings. The RADIUS server is configured in the IPSec settings.

Click on **Create**.

The **IPSec connection template** dialog closes. The new template is added to the list of available templates in the object bar.

IPSec connections

Your LANCOM R&S[®] Unified Firewall is able to provide remote clients with VPN access via IPSec (IPSec client-to-site) and to create a secure tunnel between two remote networks (IPSec site-to-site).

Overview of IPSec connections

Navigate to **VPN > IPSec > Connections** to display the list of IPSec connections available on the system in the object bar.

In the expanded view, the table columns display the **Name** and the **Status** of the IPSec connection. Furthermore, the columns indicate the authentication method chosen for this connection. Use the buttons in the last column to view and modify the settings for a IPSec connection or to delete a connection from the system.

Please refer to [Icons and buttons](#) for further information.

IPSec connection settings

Under **VPN > IPSec > Connections** you can add an IPSec connection or edit an existing connection.

In the **Connection** editing window you can modify the following parameters:

Input box	Description
I/O	A slider button indicates whether the IPSec connection is enabled (I) or disabled (O). Click on the slider button to change the status of this connection. A new connection is enabled by default.
Name	Enter a unique name for this connection. This must consist of 1-63 alphanumeric characters and underscores.
Template	Optionally you can select one of the predefined templates. All settings are then taken from the template. Values that were not set in the template are reset. The template "(empty)" can be used to reset all values.
Security profile	Select one of the predefined security profiles.

On the **Connection** tab you can configure the presets for the following fields:



Table 13: Connection

Input box	Description
Connection	By optionally selecting a network or Internet connection, its IP addresses will be used for the IPSec connection.
Listening IP addresses	As an alternative to Connection , you can also enter user-specified IP addresses. Click on ⊕ on the right-hand side to add your entry to the list. If IP addresses are entered here, the Connection setting is ignored. If neither Connection nor Listening IP addresses are set, the IPSec service will automatically use one of the configured IP addresses of all connections.

Input box	Description
Remote gateway	This address is necessary for the Initiate connection option in order to determine the address of the remote site.
Initiate connection	The firewall will connect to the address specified in the Remote gateway field.
Force NAT-T	NAT-T is usually set automatically if the connection requires it. If that mechanism fails, this option forces the use of NAT-T on a connection.

On the **Tunnels** tab you can configure the presets for the following fields:

Table 14: Tunnels

Input box	Description
Local networks	Local networks to be connected to the remote site. Click on ⊕ on the right-hand side to add your entry to the list.
Remote networks	Remote networks to connect to the local area networks. Click on ⊕ on the right-hand side to add your entry to the list.  All of the configured local networks are connected to all of the configured remote networks. For IKEv1 connections and IKEv2 connections with the option IKEv2 compatibility mode enabled, the maximum number of combinations is limited to 25. There is no limit for IKEv2 with the option IKEv2 compatibility mode disabled.
Virtual IP pool	The remote site is assigned an IP address from the configured IP pool.
Virtual IP	Assign a specific IP address to the remote site.  The options Remote networks , Virtual IP pool and Virtual IP should not be used together
IKEv2 compatibility mode	Instead of sending all configured local and remote networks through a single tunnel, a single tunnel is created for each connection between two networks (as with IKEv1). This option only applies to IKEv2 connections.

On the **Authentication** tab you can configure the presets for the following fields:

Table 15: Authentication

Input box	Description
Authentication type	Specify the authentication type. Possible values: <ul style="list-style-type: none"> > Certificate – authentication is based on a local and a remote certificate. > Certificate Authority – authentication is performed through a local and a remote certificate signed by the selected CA. > PSK (preshared key) – authentication is based on the entry of a password.
PSK (preshared key)	For authentication type PSK (preshared key) only – specify the required password here.
Local certificate	The certificate of the firewall for authentication. This must contain a private key.
Local identifier	If this field is empty, PSK authentication automatically uses the outgoing IP address of the firewall and, for certificate authentication the default is the distinguished name (DN) of the selected local certificate. <ul style="list-style-type: none"> > For PSK authentication, the following values are allowed: IP addresses, fully qualified domain names (FQDN), e-mail addresses (FQUN), and free text between quotation marks (""). > For certificate authentication, the following values are allowed: The distinguished name (DN) of the selected certificate, wildcard DN – all DN items must be present (in the correct

Input box	Description
	order), but may be specified as a wildcard (e.g. CN=*) – any subject alternative names (SAN) of the selected certificate.
Remote certificate	Only with authentication type "Certificate": Certificate of the remote site.
Certificate authority	Only with authentication type "Certificate Authority": A CA whose signed certificates can be used for authentication.
Remote identifier	<p>If this field is empty, PSK authentication automatically uses the IP address of the remote gateway (if set). For certificate authentication, the distinguished name (DN) of the selected remote certificate.</p> <ul style="list-style-type: none"> > For PSK authentication, the following values are allowed: IP addresses, fully qualified domain names (FQDN), e-mail addresses (FQUN), and free text between quotation marks ("). > For certificate authentication, the following values are allowed: The distinguished name (DN) of the selected certificate, wildcard DN – all DN items must be present (in the correct order), but may be specified as a wildcard (e.g. CN=*) – any subject alternative names (SAN) of the selected certificate.
EAP / XAUTH	Enables the use of additional user authentication. XAUTH for IKEv1 uses the local user database or a RADIUS server (depending on whether RADIUS is enabled in the IPSec settings or not). EAP for IKEv2 only works with an external RADIUS server, which must be activated in the IPSec settings. The RADIUS server is configured in the IPSec settings

The buttons available at the bottom right of the edit box depend on whether you are adding a new VPN IPSec connection or editing an existing connection. For a new network connection, click **Create** to add the connection to the list of available IPSec network connections, or **Cancel** to cancel the creation of a new network connection.

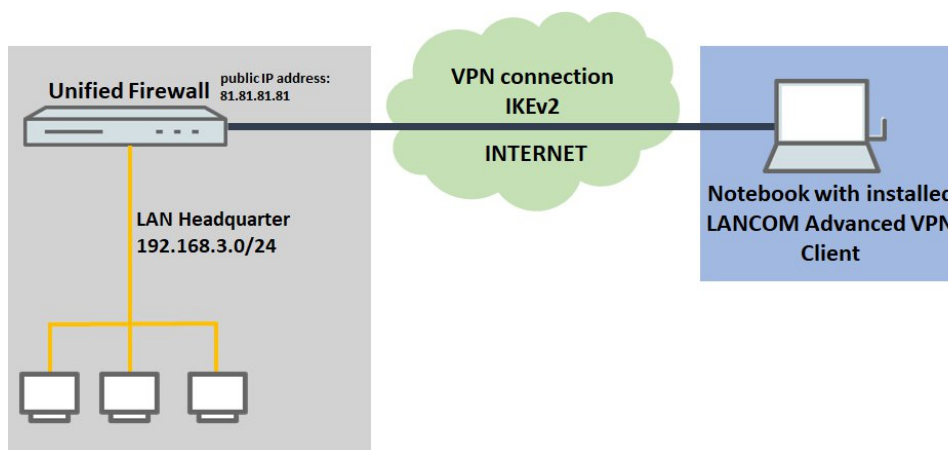
If you have made changes, you can use the buttons at the bottom right of the edit window to save them (**Save**) or discard them (**Reset**). Otherwise you can close the window (**Close**).

Click **✓ Activate** in the toolbar at the top of the desktop to apply your configuration changes.

Setting up an IKEv2 VPN connection with the LANCOM Advanced VPN Client

Scenario: The LANCOM R&S[®] Unified Firewall is connected directly to the Internet and has a public IPv4 address:


- > A company wants its sales representatives to have access to the corporate network via an IKEv2 client-to-site connection.
- > The notebooks used by the sales representatives have the LANCOM Advanced VPN Client installed on them.
- > The company headquarters has a LANCOM R&S[®] Unified Firewall as a gateway with an Internet connection with the fixed public IP address 81.81.81.81.
- > The local network at the headquarters has the IP address range 192.168.3.0/24.



Configuration steps on the LANCOM R&S® Unified Firewall

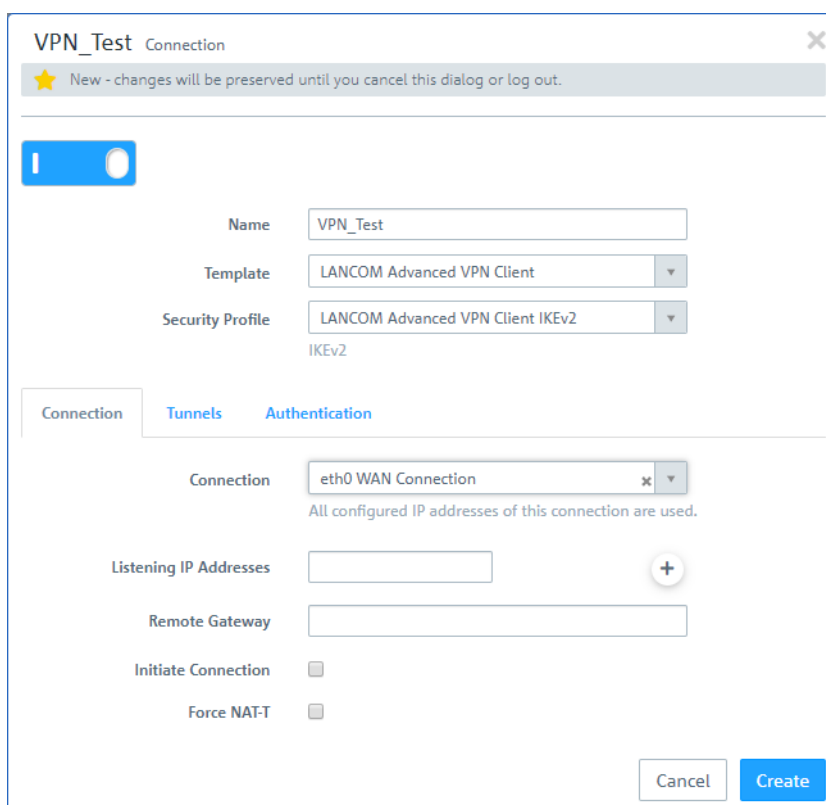
1. Connect to the configuration interface of the Unified Firewall and navigate to **VPN > IPsec > IPsec Settings**.
2. Enable IPsec by using the slider button at the top left to switch it on. Save this change.
3. Change to **VPN > IPsec > Connections** and click **+** to create a new IPsec connection.
4. Save the following parameters:

- Name: Enter a descriptive name.

 The name may only contain letters, numbers and underscores.

- Template: Select the "LANCOM Advanced VPN Client".

- Network connection: From the drop-down menu, select the WAN object used for the Internet connection.



5. Change to the Tunnel tab and enter the following parameters:
 - Local networks: Enter the local network in CIDR notation (Classless Inter-Domain Routing) with which the VPN client should communicate.
 - Virtual IP pool: Remove the default virtual IP pool by clicking on the right-hand x.

- Virtual IP: Assign an IP address from the local network to the VPN client. This IP address is assigned to the VPN client each time it dials-in using the IKE config mode.

VPN_Test Connection

★ New - changes will be preserved until you cancel this dialog or log out.

☒ I

Name: VPN_Test

Template: LANCOM Advanced VPN Client

Security Profile: LANCOM Advanced VPN Client IKEv2

IKEv2

Connection | Tunnels | Authentication

Local Networks: 192.168.3.0/24

Remote Networks:

Virtual IP Pool:

Virtual IP: 192.168.3.24

IKEv2 Compatibility Mode: ☐

Cancel Create

6. Change to the Authentication tab and enter the following parameters:
- Authentication type: Select "PSK (preshared key)".
 - PSK (Preshared Key): Set a preshared key.
 - Local identifier: Set the local identifier.
 - Remote identifier: Set the remote identifier.

! The local and remote identifiers must not match!

VPN_Test Connection

★ New - changes will be preserved until you cancel this dialog or log out.

Name: VPN_Test

Template: LANCOM Advanced VPN Client

Security Profile: LANCOM Advanced VPN Client IKEv2

Authentication Type: ☐ Certificate, ☐ Certificate Authority, ☒ PSK (Preshared Key)

PSK (Preshared Key): 12345678

Local Certificate: [Dropdown]

Local Identifier: test@centralsite

Remote Certificate: [Dropdown]

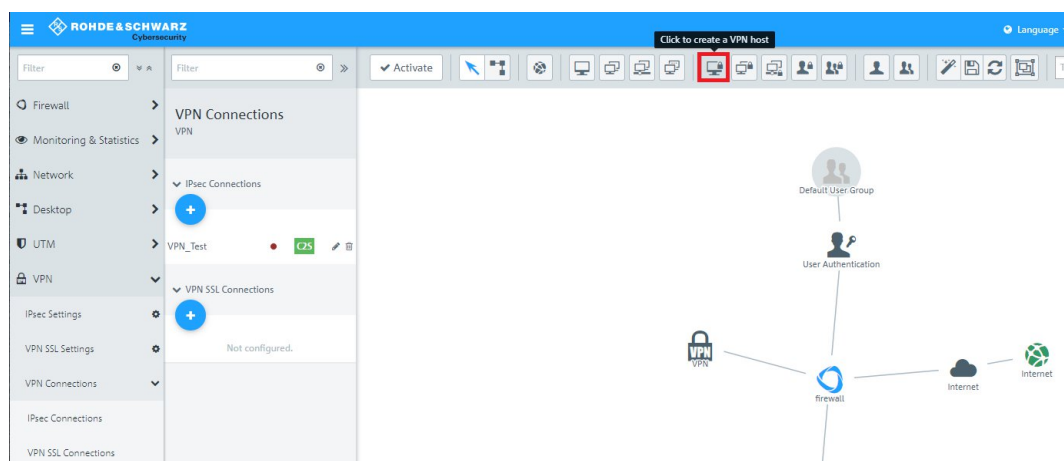
Remote Identifier: client@centralsite

EAP/XAUTH: ☐

Cancel Create

7. Click Create to create the connection.

8. To create a new VPN host, click .



9. Save the following parameters:

- Name: Enter a descriptive name.
- VPN connection type: Select the type IPsec.

- IPsec connection: From the drop-down menu under IPsec, select the VPN connection created in steps 3 on page 27 - 7 on page 29.

Client_Test VPN Host

★ New - changes will be preserved until you cancel this dialog or log out.

Name: Client_Test

Description:

Tags:


Color: [Blue]

Icon: Computer, Notebook, Server

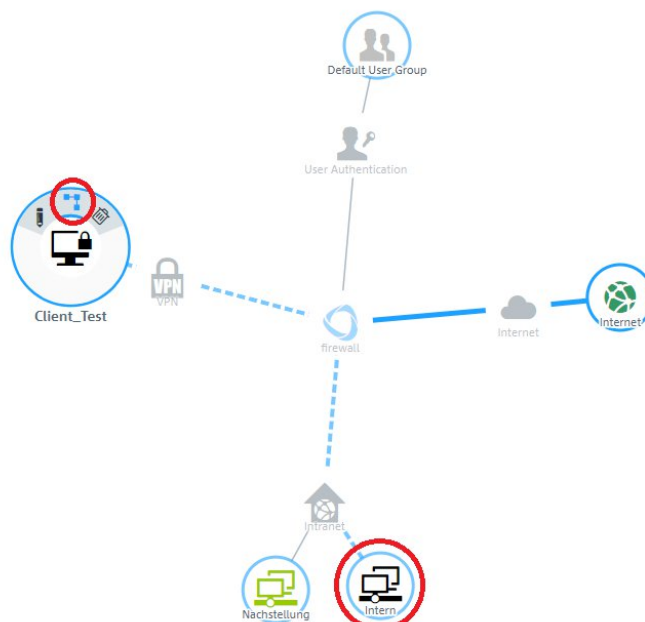
VPN Connection Type: ☒ IPsec ☐ VPN-SSL

IPsec Connection: VPN_Test

Cancel Create

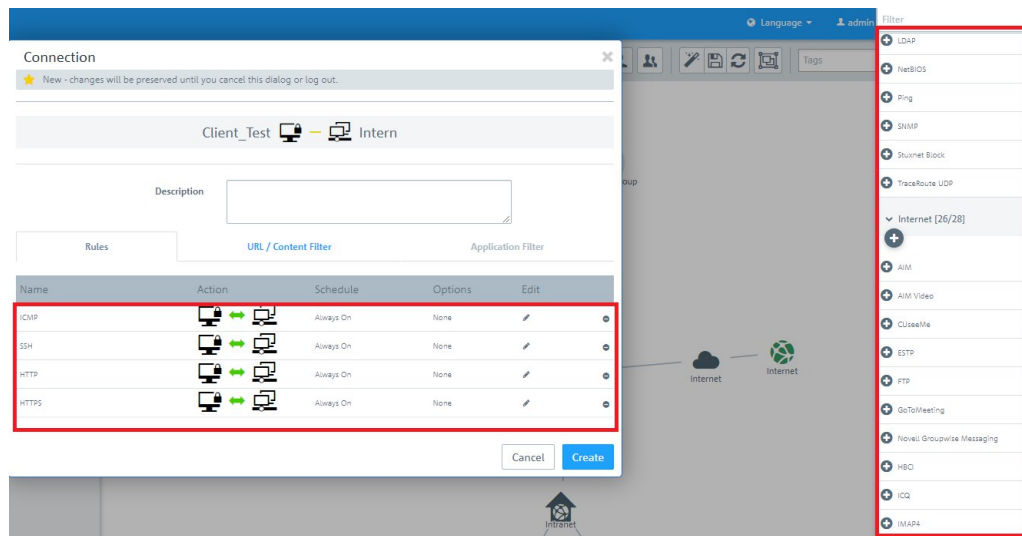
10. In the VPN host click on  and, to open the firewall objects, click on the network object that the LANCOM Advanced VPN Client should access.

Repeat this step for every internal network that the LANCOM Advance VPN Client should be able to access.

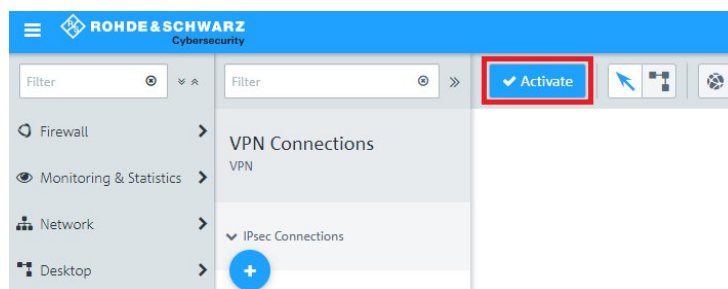


11. Use  to assign the required protocols to the VPN host.

- i** A LANCOM R&S® Unified Firewall uses a deny-all strategy. You therefore have to explicitly allow communication.



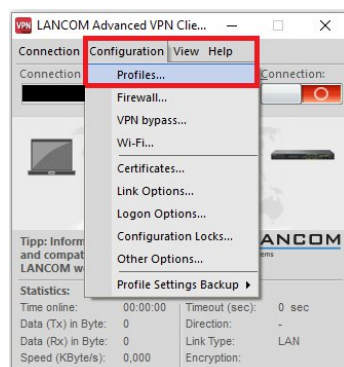
12. Finally, implement the configuration changes by clicking **Activate**.



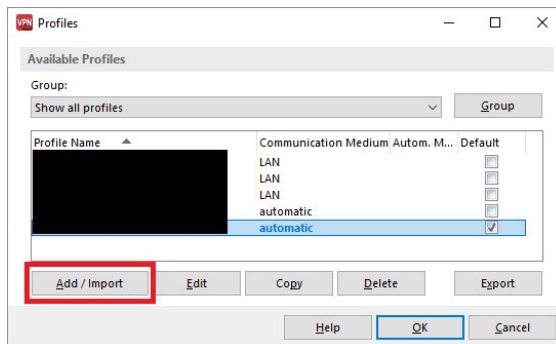
13. This concludes the configuration steps on the Unified Firewall.

Configuring the LANCOM Advanced VPN Client:

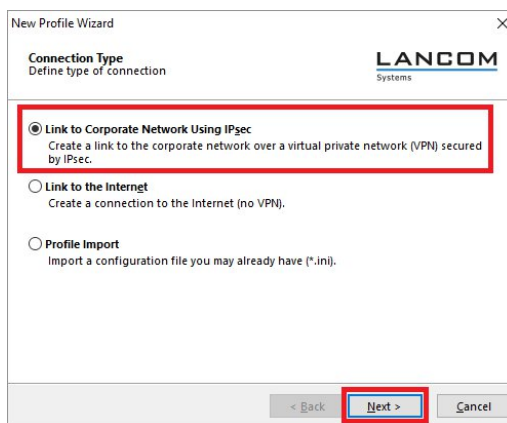
1. Open the LANCOM Advanced VPN Client and navigate to the menu **Configuration > Profiles**.



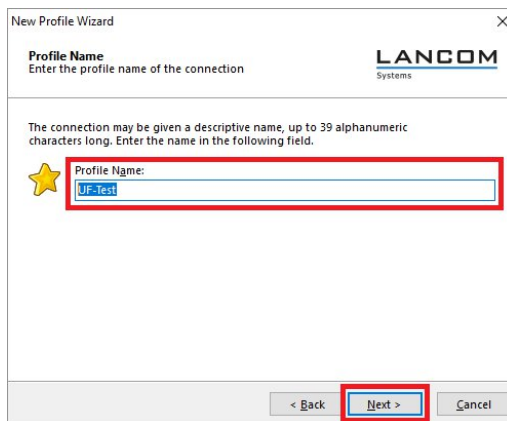
- Click on **Add / import** to create a new VPN connection.




- Select **Link to corporate network using IPSec**.

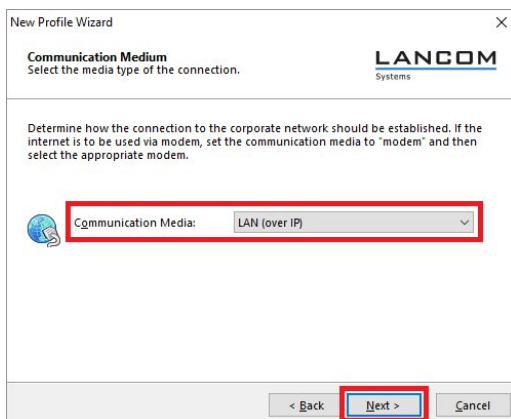


- Enter a descriptive name.



- Select the connection medium.

-  If you are using changing communication media (e.g. LAN and WLAN), use the option Communication media automatic.



New Profile Wizard

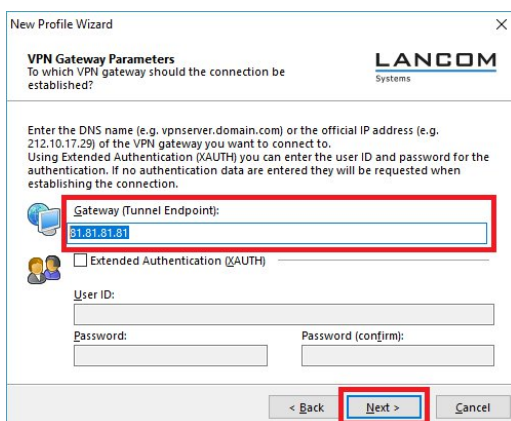
Communication Medium
Select the media type of the connection.

Determine how the connection to the corporate network should be established. If the internet is to be used via modem, set the communication media to "modem" and then select the appropriate modem.

Communication Media: LAN (over IP)

< Back Next > Cancel

6. Enter the public IP address or the DynDNS name of the Unified Firewall.



New Profile Wizard

VPN Gateway Parameters
To which VPN gateway should the connection be established?

Enter the DNS name (e.g. vpnserver.domain.com) or the official IP address (e.g. 212.10.17.29) of the VPN gateway you want to connect to. Using Extended Authentication (XAUTH) you can enter the user ID and password for the authentication. If no authentication data are entered they will be requested when establishing the connection.

Gateway (Tunnel Endpoint): 81.81.81.81

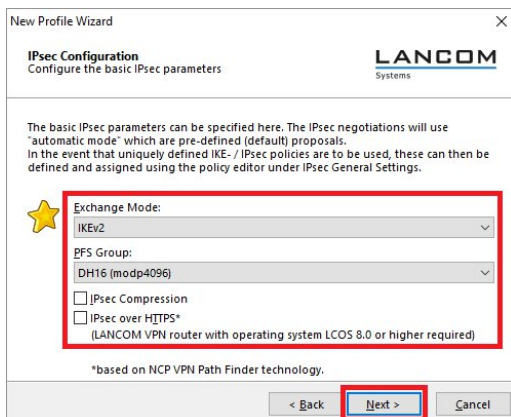
☐ Extended Authentication (XAUTH)

User ID:

Password: Password (confirm):

< Back Next > Cancel

7. Set the **Exchange Mode** to "IKEv2" and the **PFS Group** to "DH16 (modp4096)". Disable the option **IPSec-over-HTTPS**.



New Profile Wizard

IPsec Configuration
Configure the basic IPsec parameters

The basic IPsec parameters can be specified here. The IPsec negotiations will use "automatic mode" which are pre-defined (default) proposals. In the event that uniquely defined IKE-/IPsec policies are to be used, these can then be defined and assigned using the policy editor under IPsec General Settings.

Exchange Mode: IKEv2

PFS Group: DH16 (modp4096)

☐ IPsec Compression

☐ IPSec over HTTPS*
(LANCOM VPN router with operating system LCOS 8.0 or higher required)

*based on NCP VPN Path Finder technology.

< Back Next > Cancel

8. Save the following parameters:

- > **Type:** From the drop-down menu, select the Identity Type Fully Qualified Username (FQUN).
- > **ID:** Store the remote identifier assigned in step 6 on page 28

- **Shared secret:** Enter the Preshared key set in step 6 on page 28.

New Profile Wizard

Pre-shared Key
Common Secret for Authentication

LANCOM Systems

Enter the appropriate value for the IKE ID according to the selected ID type.

A shared secret or pre-shared key is used to encrypt the connection. This then needs to be identically configured on both sides (VPN client and VPN gateway).

Local Identity (IKE)

Type: Fully Qualified Username

ID: client@headquarter

Pre-shared Key

Shared Secret: Confirm Secret:

< Back Next > Cancel

9. From the drop-down menu, select the "IKE Config Mode" so that the VPN client automatically receives the IP address from the LANCOM R&S® Unified Firewall.

New Profile Wizard

IPsec Configuration - IP Addresses
Assigning the IP address to the client

LANCOM Systems

Specify which IP address the client is going to use. By selecting "Use IKE Config Mode" the client's IP address is dynamically assigned by the VPN gateway.

Furthermore, define where the DNS / WINS servers (if used) can be found.

IP Address Assignment

IKE Config Mode

IP Address: 0.0.0.0

DNS / WINS Servers

DNS Server: 0.0.0.0 WINS Server: 0.0.0.0

< Back Next > Cancel

10. In order to use the function Split Tunneling, enter the target network to be reached via the VPN tunnel.

! If split tunneling is not configured, all traffic is transferred over the VPN tunnel while it is established, including traffic intended for the local network or the Internet. This can lead to problems with the communication!

New Profile Wizard

IPsec Configuration - Split Tunneling
Define the remote IP networks to be reached through the IPsec tunnel.

LANCOM Systems

Enter the remote IP networks the tunnel should be used for. Without entries tunneling will always be used.

Remote Networks	Remote IP Net Masks
192.168.3.0	255.255.255.0

Add Edit Delete

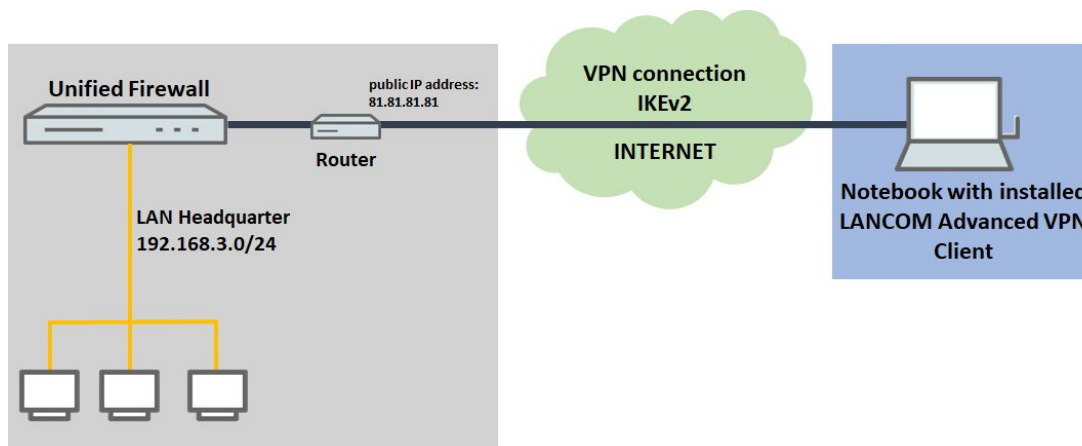
< Back Finish Cancel

11. This concludes the configuration steps in the LANCOM Advanced VPN Client.

Additional steps for a "parallel" solution

Scenario: The LANCOM R&S® Unified Firewall is connected to the Internet via an upstream router:

- A company wants its sales representatives to have access to the corporate network via an IKEv2 client-to-site connection.
- The notebooks used by the sales representatives have the LANCOM Advanced VPN Client installed on them.
- The company headquarters has a LANCOM R&S® Unified Firewall as the gateway and an upstream router for the Internet connection. The router has the fixed public IP address 81.81.81.81.
- The local network at the headquarters has the IP address range 192.168.3.0/24.

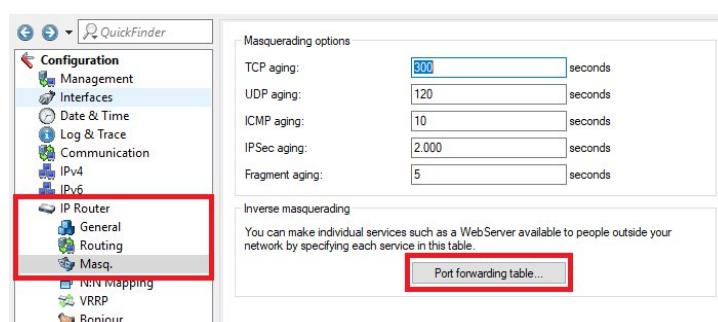


This scenario additionally requires port and protocol forwarding to be set up on the upstream router.

IPSec requires the use of the UDP ports 500 and 4500 as well as the protocol ESP. These must be forwarded to the Unified Firewall. Forwarding the UDP ports 500 and 4500 automatically causes the ESP protocol to be forwarded.

- ❗ If the UDP ports 500 and 4500 and the ESP protocol are forwarded to the LANCOM R&S® Unified Firewall, an IPSec connection to the LANCOM router can only be used if it is encapsulated in HTTPS (IPSec-over-HTTPS). Otherwise, no IPSec connection will be established.

1. Open the configuration for the router in LANconfig and switch to the menu item **IP-Router > Masq. Port forwarding table**.



2. Save the following parameters:
 - **First port:** Specify the port 500.
 - **Last port:** Specify the port 500.
 - **Intranet address:** Enter the IP address of the LANCOM R&S® Unified Firewall in the intermediate network between LANCOM R&S® Unified Firewall and the LANCOM router.

> **Protocol:** From the drop-down menu, select UDP.

3. Create a further entry and specify the UDP port 4500.

4. Write the configuration back to the router.

8.1.2 VPN-SSL


VPN over SSL provides a fast and secure way to get a roadwarrior connected. The biggest advantage of VPN-SSL is that all traffic passes through a TCP or UDP port and no other special protocols are required.

Your LANCOM R&S® Unified Firewall is able to offer VPN access to remote client computers (C2S, “client-to-site”) or a secure connection between two remote networks (S2S, “site-to-site”) by means of the VPN-SSL protocol.


VPN SSL settings

Under **VPN > VPN SSL Settings**, you can enable VPN-SSL and configure the general settings on your LANCOM R&S® Unified Firewall:


Input box	Description
I/O	A slider button indicates whether VPN SSL is enabled (I) or disabled (O). Click on the slider button to change the status of this option.
Host certificate	Select a host certificate that your LANCOM R&S® Unified Firewall uses for all VPN SSL connections.
DNS	Optional: Enter a DNS server to be used by clients for client-to-site connections.
WINS	Optional: Enter a WINS server to be used by clients for client-to-site connections.
Timeout	Enter the timeout in seconds. The tunnel is disconnected if there is no data flow before the timeout expires. The default is 0. The tunnel is thus kept open permanently.
Log Level	Set the event log level here. For troubleshooting, event log level 5 is recommended.
Routes	<p>Enter routes for the VPN SSL tunnels to be created by the clients or the remote end of the connection. These routes will be used for all VPN SSL connections.</p> <p>Click on Add to add the route to the list. You can edit or delete any entry in the list by clicking on the appropriate icon.</p> <p>Please refer to Icons and buttons for further information.</p>

Input box	Description
	 When you edit an entry, a checkmark will appear to the right of the entry. Click the checkmark to accept the change.


On tab **Client-to-Site**:

Input box	Description
Protocol	Select the protocol with the appropriate radio button.
Port	Specify the VPN SSL listening port to be used for incoming connections.  This port number also has to be specified in the client software.
Address pool	Specify the address range from which IP addresses are assigned to clients. This address range must not overlap with your local networks.
Encryption algorithm	Use the drop-down list to select the encryption algorithm to use for C2S connections over VPN SSL.
Key renegotiation	To increase security, a VPN SSL connection renegotiates the session key while the connection is in progress. Enter the interval for key renegotiation in seconds.
Compression	Optional: Uncheck this box to disable LZO (Lempel-Ziv-Oberhumer, an algorithm for lossless data compression). This checkbox is enabled by default.

On tab **Site-to-Site**:

Input box	Description
Protocol	Select the protocol with the appropriate radio button.
Port	Specify the VPN SSL listening port to be used for incoming connections.  The same port number must be specified at the remote end of the connection.
Address pool	Specify the address range from which IP addresses are to be used for S2S connections. This address range must not overlap with your local networks.
Encryption algorithm	Use the drop-down list to select the encryption algorithm to use for S2S connections over VPN SSL.
Key renegotiation	To increase security, a VPN SSL connection renegotiates the session key while the connection is in progress. Enter the interval for key renegotiation in seconds.
Compression	Optional: Uncheck this box to disable LZO (Lempel-Ziv-Oberhumer, an algorithm for lossless data compression). This checkbox is enabled by default.

If you have made changes, you can use the buttons at the bottom right of the edit window to save them (**Save**) or discard them (**Reset**). Otherwise you can close the window (**Close**).

Click  **Activate** in the toolbar at the top of the desktop to apply your configuration changes.

VPN SSL connections

You can create and manage VPN SSL connections under **VPN > VPN Connections > VPN SSL Connections**.

Your LANCOM R&S[®] Unified Firewall is able to provide VPN access by means of VPN-SSL to remote clients (client-to-site) and to create a secure tunnel between two remote networks (site-to-site).

Overview of VPN SSL connections

Navigate to **VPN > VPN Connections > VPN SSL Connections** to display the list of VPN SSL connections available on the system in the object bar.



In the expanded view, the table columns display the **Name** of the VPN SSL connection, the **Certificate** used for the connection, as well as the **Type** and the **Status** of the connection. Use the buttons in the last column to view and modify the settings for a VPN SSL connection or to delete a connection from the system.

Please refer to [Icons and buttons](#) for further information.

VPN SSL connection settings

Under **VPN > VPN Connections > VPN SSL Connections** you can add a VPN SSL connection or edit an existing connection.


With the settings under **VPN SSL Connections** you can adjust the following parameters:

Input box	Description
I/O	A slider button indicates whether the VPN SSL connection is enabled (I) or disabled (O). Click on the slider button to change the status of this connection. Newly created connections are enabled by default.
Name	Enter a unique name for this connection. The name has to consist of alphanumeric characters (i.e. letters excepting ä, ö, ü and ß, numbers and special characters).
Certificate	<p>Select the server certificate for VPN SSL connections from the drop-down list.</p> <p> The VPN certificate must be signed by the same Certificate Authority (CA) at all locations. It is therefore advisable to administer the VPN certification authority and the VPN certificates at one location and to export the VPN certificates from there to all other locations.</p>
Connection type	<p>Select the connection type and the function of the LANCOM R&S® Unified Firewall by selecting the appropriate radio button.</p> <p>You can choose from the following three types:</p> <ul style="list-style-type: none"> > Client-to-Site – A C2S connection is established (e.g. for full tunneling). <p> This connection type can, for example, be used with the OpenVPN client, primarily to connect mobile clients to your local network.</p> <ul style="list-style-type: none"> > Site-to-Site (Server) – An S2S connection is established with your LANCOM R&S® Unified Firewall acting as a server. > Site-to-Site (Client) – An S2S connection is established. Your LANCOM R&S® Unified Firewall acts as a client.



The items displayed in the settings depend on the connection type selected:

You can configure the following items for client-to-site connections:


Input box	Description
Set default gateway	Check this box to use the VPN SSL tunnel as the default route (for example, for full tunneling).
Client IP	Optional: Enter the IP address where the client can be reached.
Additional remote networks	<p>The local area networks to which the client sets up connection routes must be specified in valid CIDR notation (IP address followed by a slash "/" and the number of bits specified in the subnet mask, e.g. 192.168.1.0/24).</p> <p>Click on Add to add a network to the list.</p> <p>You can edit or delete any entry in the list by clicking on the appropriate icon.</p>

Input box	Description
	<p>Please refer to Icons and buttons for further information.</p> <hr/> <p> When you edit an entry, a checkmark will appear to the right of the entry. Click the checkmark to accept the change.</p>

For site-to-site connections where your LANCOM R&S® Unified Firewall acts as a server, you can configure the following items:

Input box	Description
Address pool	Specify the address range from which IP addresses will be used for this connection. The address range is specified in the VPN SSL settings. Please refer to VPN-SSL on page 36 for further information.
Remote IP	Optional: Enter the IP address of the remote end of the connection.
Remote Networks	<p>Specify the networks available at the remote end of the connection. Once the connection is successfully established, the server creates routes to these networks.</p> <p>Click on Add to add a network to the list.</p> <p>You can edit or delete any entry in the list by clicking on the appropriate icon.</p> <p>Please refer to Icons and buttons for further information.</p> <hr/> <p> When you edit an entry, a checkmark will appear to the right of the entry. Click the checkmark to accept the change.</p>
Additional Local Networks	<p>Specify any additional local networks. Once the connection is successfully established, the server creates routes to these networks.</p> <p>Click on Add to add a network to the list.</p> <p>You can edit or delete any entry in the list by clicking on the appropriate icon.</p> <p>Please refer to Icons and buttons for further information.</p> <hr/> <p> When you edit an entry, a checkmark will appear to the right of the entry. Click the checkmark to accept the change.</p>


For site-to-site connections where your LANCOM R&S® Unified Firewall acts as a client, you can configure the following items:

Input box	Description
Address pool	Specify the address range from which IP addresses will be used for this connection. The address range is specified in the VPN SSL settings. Please refer to VPN-SSL on page 36 for further information.
Server Address	<p>Enter the IP address where the remote end of the connection can be reached.</p> <p>Click on Add to add a network to the list. If you add more than one network, an automatic failover will be triggered if the first network becomes unreachable. In this case, your LANCOM R&S® Unified Firewall will try to reach the other networks in the list one by one until a network is found.</p> <p>You can edit or delete any entry in the list by clicking on the appropriate icon.</p> <p>Please refer to Icons and buttons for further information.</p> <hr/> <p> When you edit an entry, a checkmark will appear to the right of the entry. Click the checkmark to accept the change.</p>
Server Port	Enter the port number used at the remote end of this connection.

Input box	Description
Try establishing connection for	Specify the timeout in minutes after which no further connection attempts will be made. If this option is set to 0, the connection attempts will continue without interruption.

The buttons available at the bottom right of the edit box depend on whether you are adding a new VPN SSL connection or editing an existing connection. For a new connection, click **Create** to add the connection to the list of available VPN SSL connections, or **Cancel** to discard your changes.

If you have made changes, you can use the buttons at the bottom right of the edit window to save them (**Save**) or discard them (**Reset**). Otherwise you can close the window (**Close**).

Click  **Activate** in the toolbar at the top of the desktop to apply your configuration changes.