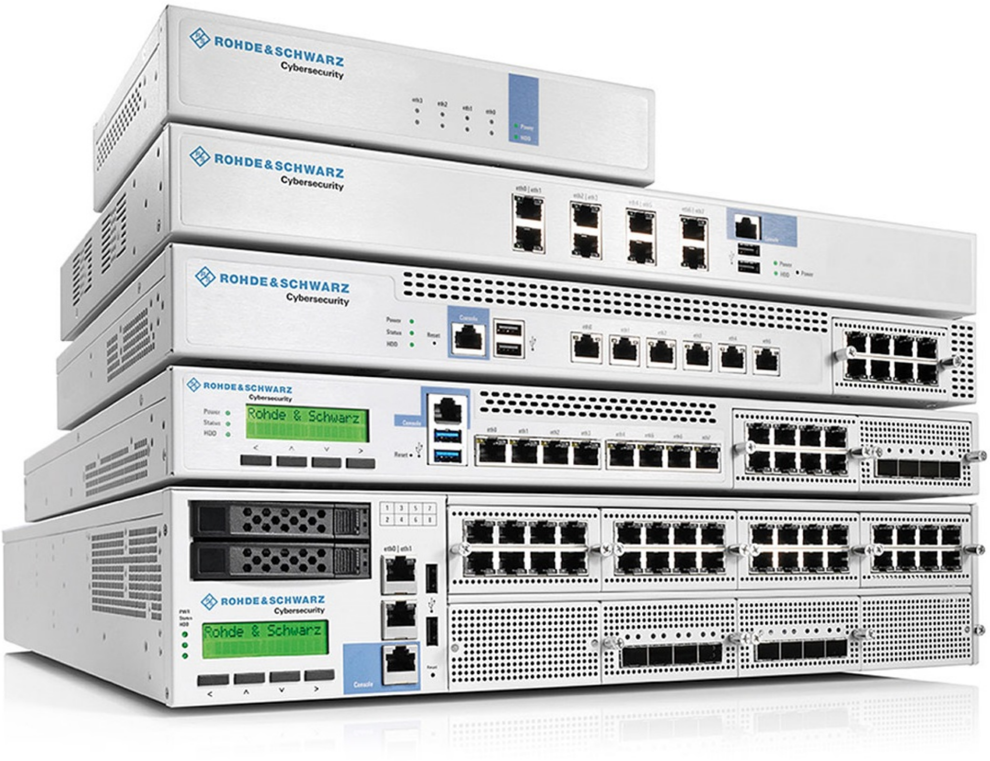
R&S®Unified Firewalls

User Manual



3646402602

User Manual

Version 03

This document applies to the R&S®Unified Firewalls software version 10.2.1. It describes the following R&S®Unified Firewalls models:

- R&S®Unified Firewalls GP-U
- R&S®Unified Firewalls GP-E
- R&S®Unified Firewalls GP-S
- R&S®Unified Firewalls GP-T
- R&S®Unified Firewalls UF
- R&S®Unified Firewalls UF-T

This product uses several valuable open source software packages. For more information, see the *Open Source Acknowledgement* document, which you can obtain separately.
The open source software is provided free of charge. You are entitled to use the open source software in accordance with the respective license conditions as provided in the *Open Source Acknowledgement* document.
Rohde & Schwarz would like to thank the open source community for their valuable contribution to embedded computing.

Mühldorfstr. 15, 81671 Munich, Germany
Phone: +49 (0) 89 41 29 - 0
Email: cybersecurity@rohde-schwarz.com
Internet: cybersecurity.rohde-schwarz.com

3646.4026.02 | Version 03 | R&S®Unified Firewalls

Throughout this user manual, Rohde & Schwarz products are indicated without the ® symbol, e.g. R&S®Unified Firewalls is indicated as R&S Unified Firewalls.

Contents

1 About This Manual

The *R&S Unified Firewalls User Manual* describes the innovative firewall solution from Rohde & Schwarz Cybersecurity GmbH. R&S Unified Firewalls integrates firewall, intrusion prevention, application control, web filtering, malware protection and many more functions in a single system.

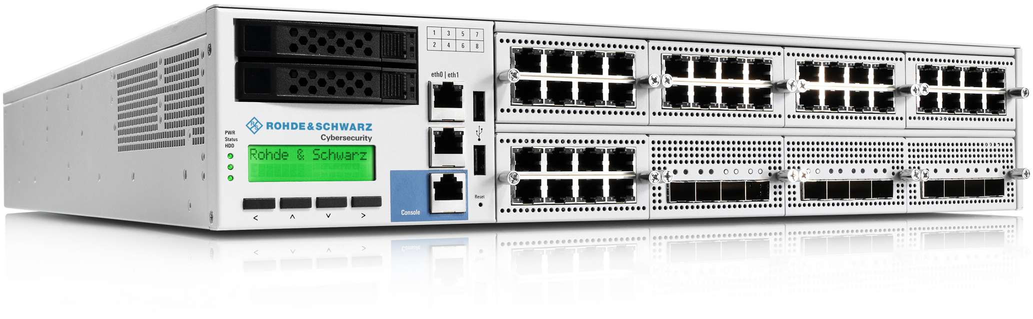


Figure 1-1: Sample R&S Unified Firewalls UF-2000.

This document applies to all R&S Unified Firewalls models.

There are license-based features that distinguish individual product models from one another. For further information about your specific model, see the information on the relevant data sheet.

See the topics below for further information about this document.

1.1 Audience

This manual is for the networking or computer technician responsible for installing and configuring R&S Unified Firewalls systems and employees that use the web client to define traffic filtering rules.

To use this document effectively, you must have the following skills depending on your responsibilities:

- To install and configure the hardware, you must be familiar with telecommunications equipment and installation procedures. You also have to have good experience as a network or system administrator.
- To define filtering rules, you need to understand basic TCP/IP networking concepts.

1.2 What’s in This Manual

The contents of this manual are designed to assist you in configuring R&S Unified Firewalls.

This document includes the following chapters:

- Chapter 2, "Getting Started", on page 11
  Log on to R&S Unified Firewalls to set up the system for your network.
- Chapter 3, "User Interface", on page 19
  The sections in this chapter describe the components of the user interface of R&S Unified Firewalls.

We are committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to doc.ipoque@rohde-schwarz.com. When submitting your feedback, include the document title and the document number located at the bottom of each chapter's page.

1.3 Conventions

This chapter explains the typographic conventions and other notations used to represent information in this manual.

Elements of the web-based graphical user interface (GUI, or »web client«) are indicated as follows:

Convention	Description
"Graphical user interface elements"	All names of graphical user interface elements on the screen, such as menu items, buttons, checkboxes, dialog boxes, list names are enclosed by quotation marks.
"Top-level menu item > submenu element"	A sequence of menu commands is indicated by greater than symbols between menu items and the whole sequence is enclosed by quotation marks. Select the submenu element from the top-level menu item.
[Keys]	Key names are enclosed in square brackets.
`List options, literal text, filenames, commands, program code`	List options, literal text, filenames, commands, coding samples and screen output are distinguished by their fixed-width font.
Links	Links that you can click (e.g. references to other parts within this manual) are displayed in blue font.
References	References to parts of the product documentation are displayed in italics.

Notes

The following types of notes are used in this manual to indicate information that expands on or calls attention to a particular point:

This note is a little hint that can help make your work easier.

This note contains important additional information.

NOTICE

This note contains information that is important to consider. Non-observance can damage R&S Unified Firewalls or put your network security at risk.

1.4 Related Resources

This section describes additional documentation and other resources for information on R&S Unified Firewalls.

Refer to the following related documents and resources:

- ***Data Sheets*** summarize the technical characteristics of the different R&S Unified Firewalls hardware models.
- ***Release Notes*** provide the latest information on each release.
- Our website at cybersecurity.rohde-schwarz.com provides a wealth of information about our products and solutions as well as the latest company news and events.

For additional documents such as technical specifications, please visit the *myrscs portal* at myrscs.rohde-schwarz.com.

2 Getting Started

This document provides all the required information on how to set up and configure your R&S Unified Firewalls device.

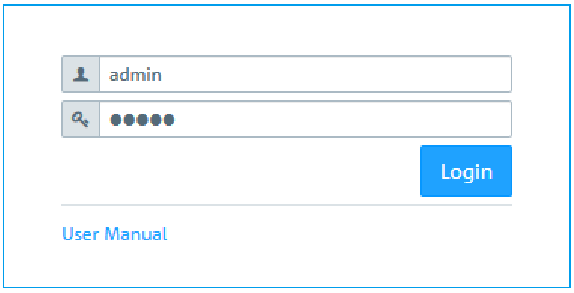
To get started, please follow the steps described below.

When first started after delivery or a new installation, R&S Unified Firewalls runs as a test version for 30 days. For further information, see Chapter 3.4.1.5, "License", on page 38.

2.1 Logging in

1. Unpack your preinstalled R&S Unified Firewalls device.
2. Connect a patch cable to the port labeled "eth1" on the front of your R&S Unified Firewalls device and to the Ethernet port on your computer.
3. Configure your computer with a static IP address in the range from 192.168.1.1/24 to 192.168.1.253/24.
4. Power on your R&S Unified Firewalls device.
5. Start a web browser on your computer.
6. Enter https://192.168.1.254:3438 in the address bar of your browser.
7. Create an exception for the certificate warning.

   The R&S Unified Firewalls login page appears.
8. On the login page of the R&S Unified Firewalls web client, enter `admin` as the "User Name" and the factory default "Password" `admin`.



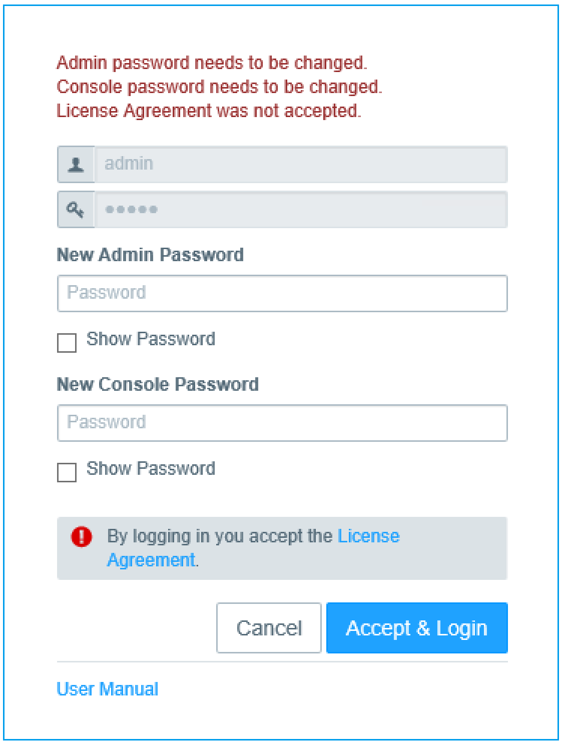
admin

●●●●●

Figure 2-1: Logging on to the R&S Unified Firewalls web client.

9. Click "Login".

10. After your first login using the standard credentials, the system prompts you to accept the End User License Agreement (EULA) and to change the following two passwords:
    - The *admin* user password – You need the user password to log on to the R&S Unified Firewalls web client.
    - The console password – You need the console password to log on to R&S Unified Firewalls using SSH.



Admin password needs to be changed.
Console password needs to be changed.
License Agreement was not accepted.

admin
•••••

New Admin Password
Password
□ Show Password

New Console Password
Password
□ Show Password

By logging in you accept the License Agreement.

Figure 2-2: Changing the credentials and accepting the EULA.

The new user password and the console password must consist of at least six and can have up to 255 characters (allowed are letters of the English alphabet, integers and special characters).

Note: This step is mandatory.

11. To save the new passwords and to accept the EULA, click "Accept & Login".

    The web client appears.

2.2 Configuring Your Internet Connection

1. Connect a patch cable to the port labeled "eth0" on the front of your R&S Unified Firewalls device and to the LAN port of the device that you received from your provider to access the Internet (e.g. your router, DSL or cable modem).

2. In the navigation pane on the left side of the web client, navigate to "Network > Connections".

   The item list bar on the right of the navigation bar opens.

3. Click » in the upper right corner of the item list bar to see which network connection is assigned to which interface.

   The item list bar expands.

4. Delete the "Default connection on eth0" by clicking 🗑 (Click to delete) in the last table column in the same row.

5. Depending on the type of your Internet access, proceed corresponding to one of the following three approaches:

Dial-up Connection

1. Navigate to "Network > Interfaces > PPP Interfaces".
2. In the item list bar, click ⊕ (Create a new item) to create a new PPP interface.

   The "PPP Interface" dialog opens, allowing you to configure a PPP interface.

3. From the "Master Interface" drop-down list, select "eth0".
4. Unless stated otherwise by your provider, leave the other settings on default value.
5. Click "Create".

   The "PPP Interface" dialog closes. The new interface is added to the list of available PPP interfaces in the item list bar.

6. Navigate to "Network > Connections > PPP Connections".
7. In the item list bar, click ⊕ (Create a new item) to create a new PPP connection.

   The "PPP Connection" dialog opens, allowing you to configure a PPP connection.

8. Enter a "Name" for your PPP connection.
9. Enter the credentials predefined by your provider.
10. Unless stated otherwise by your provider, leave the other settings on default value.
11. Click "Create".

    The "PPP Connection" dialog closes. The new connection is added to the list of available PPP connections in the item list bar.

12. Click "✔ Activate" in the toolbar at the top of the desktop to apply your configuration changes.

    You have successfully configured your Internet connection.

Cable or Router Connection with Dynamic IP

1. Navigate to "Network > Connections > Network Connections".

2. In the item list bar, click ⊕ (Create a new item) to create a new network connection.

   The "Network Connection" dialog opens, allowing you to configure a network connection.

3. Enter a "Name" for your network connection.
4. Under "Interface", select "eth0" from the drop-down list.
5. Under "Type", select "DHCP" from the drop-down list.
6. Select the "Obtain DNS Server" checkbox.
7. Select the "Obtain Domain" checkbox.
8. Click "Create".

   The "Network Connection" dialog closes. The new connection is added to the list of available network connections in the item list bar.

9. Click "✔ Activate" in the toolbar at the top of the desktop to apply your configuration changes.

   You have successfully configured your Internet connection.

Static Internet Connection with Static IP

1. Navigate to "Network > Connections > Network Connections".
2. In the item list bar, click ⊕ (Create a new item) to create a new network connection.

   The "Network Connection" dialog opens, allowing you to configure a network connection.

3. Enter a "Name" for your network connection.
4. Under "Interface", select "eth0" from the drop-down list.
5. Under "Type", select "Static" from the drop-down list.
6. Under "IP Addresses", enter the IP address and the subnet mask.
7. Click ⊕ on the right of the entry to add it to the list of IP addresses.
8. Go to the "WAN" tab.
9. Select the "Set Default Gateway" checkbox.
10. Under "Default Gateway", enter your default gateway IP address.
11. Click "Create".

    The "Network Connection" dialog closes. The new interface is added to the list of available network connections in the item list bar.

12. Navigate to "Network > DNS Settings".

    The "DNS Settings" dialog opens, allowing you to configure the DNS settings of your R&S Unified Firewalls.

13. Clear the "Acquire DNS server" checkbox.

The "1. Nameserver"/"2. Nameserver" input fields become editable.

14. Under "1. Nameserver"/"2. Nameserver", enter the IP addresses of the DNS server(s) provided by your provider.
15. Click "Save" to store your settings.

    The "DNS Settings" dialog closes.
16. Click "✓ Activate" in the toolbar at the top of the desktop to apply your configuration changes.

    You have successfully configured your Internet connection.

2.3 Enabling Internet Access

Creating an Internet Object

1. Navigate to "Desktop > Desktop Objects > Internet Objects".
2. In the item list bar, click ⊕ (Create a new item) to create a new Internet object.

   The "Internet Object" dialog opens, allowing you to configure an Internet object.
3. Under "Object Name", enter a name for your Internet object.
4. From the "Connections" drop-down list, select your Internet connection.
5. Click "Create".

   The "Internet Object" dialog closes. The new object is added to the list of available Internet objects in the item list bar.

For more information, see Chapter 3.4.4.2, "Desktop Objects", on page 101.

Configuring Your Local Network Connection

1. Connect a patch cable to one of the ports labeled "ethX" (except "eth0" as it is used for the Internet connection) on the front of your R&S Unified Firewalls device and to one of the Ethernet ports on your network switch.
2. Navigate to "Network > Connections > Network Connections".
3. In the item list bar, click ⊕ (Create a new item) to create a new network connection.

   The "Network Connection" dialog opens, allowing you to configure a network connection.
4. Enter a "Name" for your network connection.
5. Under "Interface", select the port to which you have connected your network switch from the drop-down list.
6. Under "Type", select "Static" from the drop-down list.

7. Under "IP Addresses", enter the IP address of this connection in CIDR notation (IP address followed by a slash »/« and the number of bits set in the subnet mask, for example `192.168.50.1/24`) to match your local network.
8. Click "Create".

   The "Network Connection" dialog closes.

Creating a Network Object

1. Navigate to "Desktop > Desktop Objects > Networks".
2. In the item list bar, click ⊕ (Create a new item) to create a new network object.

   The "Network" dialog opens, allowing you to configure a network object.
3. Enter a "Name" for the network object.
4. Select the "Interface" of the network connection that you have just edited.
5. Under "Network IP", enter the IP address of your local network.
6. Click "Create".

   The "Network" dialog closes. The new object is added to the list of available network objects in the item list bar.

For more information, see Chapter 3.4.4.2, "Desktop Objects", on page 101.

Configuring Firewall Rules for Internet Access

1. Set up a connection between the network object and the Internet object that you have just created:

   a) Click the ┐ button in the toolbar at the top of the desktop.
   The desktop objects which can be selected for this connection and possible connections between them are highlighted and marked by dotted circles and lines.
   b) Select the network object as the source object of the connection by clicking the corresponding desktop object.
   c) Select the Internet object as the target object of the connection by clicking the corresponding desktop object.

   You are automatically navigated to "Desktop > Desktop Connections" and the "Connection" editor panel opens.
   Alternatively, you can click the ┐ button in the circular menu of the source object on the desktop and then select the target object.
2. Set up a firewall rule with HTTP and/or HTTPS, depending on your needs:

a) In the "Rules" tab of the "Connection" editor panel, a list of services to which the firewall rule can be applied are displayed in the service selection list bar on the right side of the browser window. The list bar is subdivided into categories of services which serve a similar purpose. Use the "Filter" input field at the top of the service selection list bar to quickly find HTTP and/or HTTPS. As you type in the input field, R&S Unified Firewalls reduces the list to show only those services and service groups that contain the characters you are typing.
   Add "HTTP" and "HTTPS" from the "Internet" category by clicking the ⊕ button in front of the services.
   The selected services are removed from the service selection list bar and are displayed in the table in the "Rules" tab.
b) Click "Create".
   The "Connection" dialog closes. The new desktop connection is added to the list of available desktop connections in the item list bar.

For more information, see Chapter 3.3, "Firewall Rule Settings", on page 25.

Activating the Desktop Configuration

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

You have successfully enabled Internet access from your local network through your R&S Unified Firewalls.

3 User Interface

The sections in this chapter describe the components of the user interface of R&S Unified Firewalls.

The web client of R&S Unified Firewalls requires a minimum display resolution of 1024 × 786 pixels (XGA).

The following browser versions (or newer) are supported, with JavaScript enabled:

- Google Chrome 10
- Chromium 10
- Mozilla Firefox 12

Chapter 3.1, "Web Client Components", on page 19 provides an overview of the main components of the web client.

Chapter 3.2, "Icons and Buttons", on page 23 explains the meaning of the icons and buttons commonly used on the user interface and throughout this manual.

Chapter 3.3, "Firewall Rule Settings", on page 25 describes how to set up a firewall rule for a connection between two desktop objects.

Chapter 3.4, "Menu Reference", on page 28 reflects the arrangement of the menu items in the navigation bar on the left side of the user interface. For information on the available options, see the corresponding section.

3.1 Web Client Components

The web client of R&S Unified Firewalls uses a standard tri-pane page layout with a common header area, a navigation pane on the left and a main content pane (desktop) on the right.

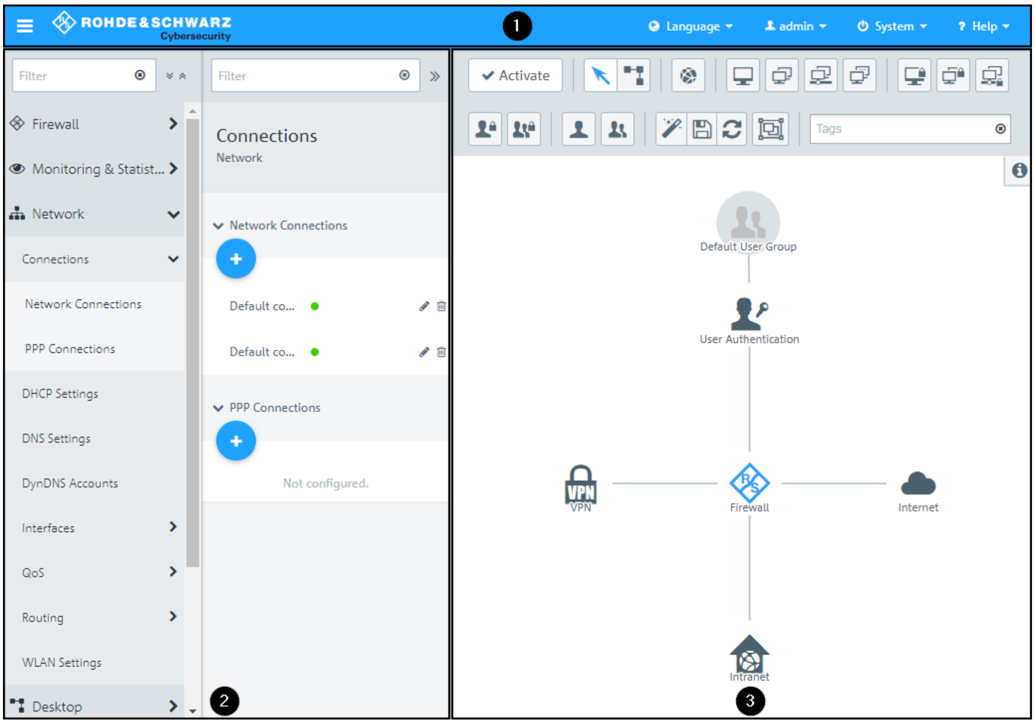


Figure 3-1: R&S Unified Firewalls web client.

1 = Header area
2 = Navigation pane
3 = Desktop

The information displayed in each area is described in the following sections.

3.1.1 Header Area

The header area (1) contains the following elements (from left to right):

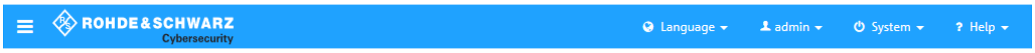


Figure 3-2: R&S Unified Firewalls web client header area.

- the ☰ button to hide or show the navigation bar (the navigation bar is displayed by default, see Chapter 3.1.2, "Navigation Pane", on page 21),
- the Rohde & Schwarz Cybersecurity GmbH logo,
- a language menu that allows you to select the language to be used in the web client,
- a user menu to end the current user session and return to the logon page,
- a system menu to reboot or shut down / power off R&S Unified Firewalls, and
- a help menu with links that provide access to a PDF version of the *R&S Unified Firewalls User Manual* and to the Rohde & Schwarz Cybersecurity GmbH support website. Depending on your browser settings, the PDF file is either displayed in a new tab or window, or downloaded.

In addition, the header area displays unsaved configuration changes if you close an editor panel by pressing the [Esc] key on your computer keyboard. Unsaved changes are not displayed if you close an editor panel by clicking the ✖ button in the upper right corner of the panel, however.

The PDF version of the *R&S Unified Firewalls User Manual* is also available from the logon page. Click the "User Manual" link to access the file.

3.1.2 Navigation Pane

The navigation pane (2) is on the left side of the web client and consists of two parts. The links in the left navigation bar provide access to the R&S Unified Firewalls settings. The item list bar on the right is used to display information on the current desktop configuration.

Both bars contain a "Filter" input field at the top which helps you quickly find a particular menu item or item list entry. Each input field works for the bar it is part of only. As you type in one of the input fields, R&S Unified Firewalls reduces the corresponding list to show only those menu items or item list entries that contain the characters you are typing. Click ⊗ in the input field to delete the search string and display an unfiltered view of the bar.

You can expand all menus in the navigation bar at once by clicking ︾ or collapse them by clicking ︽ in the upper right corner of the navigation bar. Furthermore, you can hide the navigation bar to maximize the desktop area by clicking ≡ in the header area. For further information, see Chapter 3.1.1, "Header Area", on page 20.

The information displayed in the item list bar depends on, firstly, the menu item selected in the navigation bar and, secondly, how much information you desire to be displayed. You can unfold more detailed information by clicking » or reduce the amount of information presented by clicking « in the upper right corner of the item list bar.

See Chapter 3.4, "Menu Reference", on page 28 for details on the options available in each view.

3.1.3 Desktop

The desktop (3) fills the main portion of the screen below the header area and to the right of the navigation pane. The nodes and connections highlighted here depend on the item selected in the navigation pane or on the desktop.

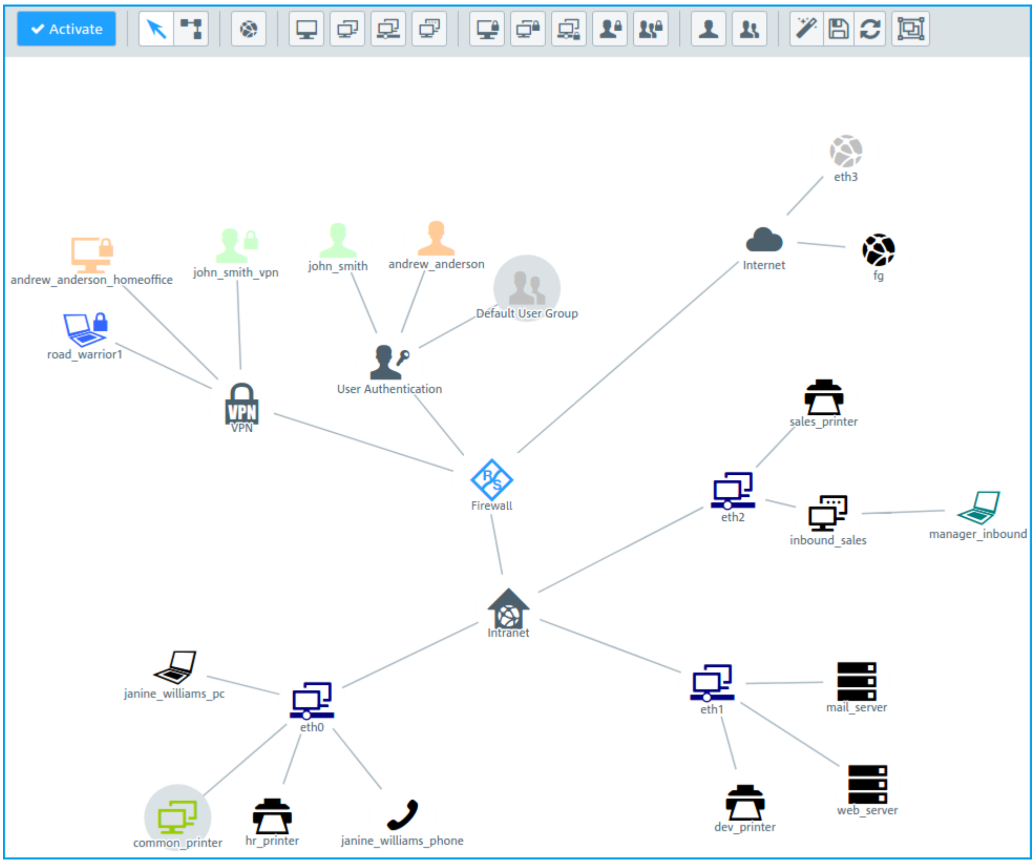


Figure 3-3: R&S Unified Firewalls web client desktop.

On the desktop, you always have a complete overview of your entire configured network. You can edit various settings in this pane or view the details of a configuration.

A toolbar at the top of the desktop provides quick access to frequently used functions (from left to right):

- If the system configuration changes, the "✔ Activate" button in the first section of the toolbar is highlighted, prompting you to update your configuration. Click this button to save your current desktop configuration changes and to activate them on your R&S Unified Firewalls.
- The two buttons in the second section of the toolbar allow you to switch back and forth between the selection and the connection tool. Use the selection tool for all actions on the desktop, such as moving objects or selecting certain functions. With the connection tool, you can create or edit a connection between two desktop objects. For further information, see Chapter 3.3, "Firewall Rule Settings", on page 25.
- You can create an object on the desktop by clicking the respective desktop object button in the next four sections of the toolbar. An editor panel automatically opens where you can enter the data which is required for the object.
- You can customize the desktop layout by dragging the objects to the desired positions where they are automatically pinned. Use the buttons in the seventh section

of the toolbar to save and restore your customized layout or to arrange the objects automatically.

- The "Tags" filter input field in the last section of the toolbar helps you quickly identify desktop objects on the desktop, based on previously assigned desktop tags. Click the input field to open a drop-down list containing the names of previously configured desktop tags. You can either select one if the list items directly to add it to the filter input field or use the input field to search for a particular desktop tag. As you type in the input field, R&S Unified Firewalls reduces the drop-down list to show only those list items that contain the characters you are typing. You can add as many desktop tags as you like to the filter input field.
  Depending on your selection of desktop tags, R&S Unified Firewalls reduces the number of nodes on the desktop to display only those desktop objects which include at least one of the selected desktop tags. Desktop nodes along the path from the "Firewall" root node to a node matching the selected desktop tags are always displayed, even if their tag set does not match the search criteria.
  Click ⊗ in the input field to delete the search string or all selected desktop tags and display an unfiltered view of the desktop. For further information, see Chapter 3.4.4.4, "Desktop Tags", on page 114.

All toolbar buttons use mouse-over pop-up labels for easy identification.

When you left-click a desktop object, several buttons appear in the circular menu, depending on the kind of desktop object. These buttons allow you to adjust the settings for an existing object and to create or edit a connection between two existing objects. Furthermore, you can hide or display objects attached to an object, unpin an object from a specific location on the desktop or remove an object from the desktop.

For further information, see Chapter 3.2, "Icons and Buttons", on page 23.

3.2 Icons and Buttons

This section explains the icons and buttons commonly used on the user interface and throughout this manual.

Icon/Button	Description
☰	Hide and show the navigation bar.
↖	Move objects or select objects and functions on the desktop.
🔗	Create or edit a connection between two desktop objects.
🌐	Create an Internet object.
🖥	Create a host.
🗗	Create a hosts group.
🖧	Create a network.
🗗	Create an IP range.
🖥	Create a VPN host.

Icon/Button	Description
🖧🔒	Create a VPN group.
🖧🔒	Create a VPN network.
👤🔒	Create a VPN user.
👥🔒	Create a VPN user group.
👤	Create a user.
👥	Create a user group.
🪄	Discard all manual desktop layout changes and apply an automatic layout.
💾	Save the current desktop layout.
⟳	Restore the last saved desktop layout. Restore a backup. Replace a certificate by importing a new certificate.
⛶	Fit the entire network to the desktop.
⚙	Marks a menu item with settings to configure in the navigation bar. Marks a table column with actions available for a table entry.
📌	Unpin the desktop object to be able to move it along with the desktop node that it is associated with via drag & drop on the desktop.
✎	View and adjust the settings for a desktop object, a list item or a table entry.
⧉	Create an item list or a table entry based on a copy of an existing entry.
🗑	Delete a desktop object or an item list entry from the system after a positive response to the confirmation request popping up. Permanently revoke a certificate.
⊖	Delete a custom firewall rule from the system. Remove a firewall rule with a predefined service from the firewall rules table.
⇥	Import a certificate or a blacklist/whitelist from a file. Sign a certificate signing request.
↦	Export a certificate or a blacklist/whitelist to a file.
⤓	Import a backup from a file.
⤒	Export a backup to a file.
⊕	Create a list item in the item list bar.
›	Unfold a menu item to view subordinate items in the navigation bar. Unfold a web filter category to view its subcategories. Unfold a service category for firewall rules to view its subservices. Unfold a statistics chart or table.

Icon/Button	Description
⌄	Hide subordinate menu items in the navigation bar. Hide subcategories of a web filter category. Hide subservices of a service category for firewall rules. Hide a statistics chart or table.
»	Unfold more detailed information in the item list bar.
«	Reduce the amount of information given in the item list bar.
︽	Collapse all menus in the navigation bar. Expand a desktop node to view the desktop objects associated with it.
︾	Expand all menus in the navigation bar. Collapse a desktop node to hide the desktop objects associated with it.
✅	Indicates that a certificate is still valid.
⚠	Indicates that a certificate has expired.
✔	Verify a certificate.
❚❚	Suspend a certificate or CA temporarily.
▶	Resume a certificate that was previously suspended.
↻	Recreate (renew) a certificate with an updated validity range.
✖	Close a pop-up window.
⊗	Clear all search criteria of a filter to show all results.

3.3 Firewall Rule Settings

This section describes how to create a firewall rule for a connection between two desktop objects.

Setting Up a Connection

To set up a connection between two desktop objects, perform the following steps:

1. Click the ⊶ button in the toolbar at the top of the desktop.

   The desktop objects which can be selected for this connection and possible connections between them are highlighted and marked by dotted circles and lines.

2. Select the source object of the connection by clicking the corresponding desktop object.

3. Select the target object of the connection by clicking the corresponding desktop object.

   The "Connection" editor panel opens, displaying, if applicable, already existing firewall rules for this connection.

Alternatively, you can click the ⇆ button in the circular menu of the source object on the desktop and then select the target object.

Setting Up a Firewall Rule

To set up a firewall rule, perform the following steps:

1. In the "Rules" tab of the "Connection" editor panel, select at least one of the services to which you want to apply the firewall rule.
   The services that are available for the connection are displayed in the service selection list bar on the right side of the browser window. The list bar is subdivided into categories of services which serve a similar purpose. You can collapse and expand the categories by clicking the corresponding icon.
   For further information, see Chapter 3.2, "Icons and Buttons", on page 23.
   The "Filter" input field at the top of the service selection list bar helps you quickly find a particular service or service group. As you type in the input field, R&S Unified Firewalls reduces the list to show only those services and service groups that contain the characters you are typing. Click ⊗ in the input field to delete the search string and display an unfiltered view of the list.
   a) There are two ways to add services to a firewall rule:
      - To add an individual service, click the ⊕ button in front of the corresponding service in the service selection list bar.
      - To add all services belonging to a category at once, click the ⊕ (Add filtered services) button directly below the header of the respective category.

      The selected services are displayed in the table in the "Rules" tab.
   b) To adjust the settings of a firewall rule, click the ✎ (Click to edit this rule) button.

   An editor panel for the particular service opens.

2. The editor panel displays the following information and allows you to configure the following elements of the firewall rule:
   a) Under "Description", you can enter additional information regarding the firewall rule for internal use.
   b) In the "Ports/Protocols" tab, you can see which ports and protocols were defined to be used for the service. For further information, see Chapter 3.4.4.6, "Services", on page 116.
   c) In the "Schedule" tab, you can specify the time when the firewall rule is active. The tab provides the following options:
      - Set specific times and weekdays using the sliders.
      - Click "Always On" – the rule is always active.
      - Click "Always Off" – the rule is always inactive.

d) The "Advanced" settings tab provides the following options:

Field	Description
"Proxy"	For firewall rules with predefined services only if the predefined services allow a proxy (HTTP, HTTPS, FTP, SMTP, SMTPS, POP3 or POP3S): Select this checkbox to activate the proxy for this rule. For firewall rules with user-defined services only: From the drop-down list, select a proxy for this rule. To remove the proxy, click ✖ to the right of the selected proxy.
"NAT / Masquerading"	Specify the desired direction (`bidirectional`, `left-to-right` or `right-to-left`) for NAT/masquerading or disable (`Off`) the feature for this rule by selecting the respective radio button. The default setting depends on the source and target objects selected for the connection.
"New source IP"	Optional: If you have multiple outgoing IP addresses, specify the IP address to be used for Source NAT. If you do not specify the IP address, the system automatically chooses the main IP address of the outgoing interface.
"Enable DMZ / Port Forwarding for this service"	If the target of the firewall rule is a single host object, you can select this checkbox to enable DMZ and port forwarding for this rule.
"External IP address"	Optional: Specify the destination IP address of the traffic to be manipulated. The DMZ rule only applies to this traffic. This IP address must be one of the firewall's IPs.
"External Port"	Displays the original destination port of the traffic to be manipulated, depending on the port defined in the "Ports/Protocols" tab.
"Destination IP address"	Displays the new destination IP address of the traffic (after its manipulation).
"Destination Port"	Optional: Specify the destination port of the traffic (after its manipulation).

e) The buttons at the bottom right of the editor panel allow you to confirm your changes to an existing rule ("OK"), reject the editing of an existing rule ("Cancel") and discard your changes ("Reset").

The configured rule is displayed in the table in the "Rules" tab. To delete a rule from the table, click the ⊖ (Click to remove this rule) button in the last column.

3. For further information on the "URL / Content Filter" and "Application Filter" tabs, see Chapter 3.4.4.1, "Desktop Connections", on page 100.

4. The buttons at the bottom right of the editor panel allow you to shut ("Close") the editor panel as long as no changes have been made and to store ("Save") or to discard ("Reset") your changes.

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

For further information, see Chapter 3.2, "Icons and Buttons", on page 23.

3.4 Menu Reference

This reference chapter describes each menu item in the navigation bar on the left side of the browser window. The license acquired from Rohde & Schwarz Cybersecurity GmbH determines which menu items are available on R&S Unified Firewalls. Features that are not included in your R&S Unified Firewalls license are grayed out in the navigation bar.

Refer to the sections below for information on the options available in each view.

3.4.1 Firewall

Use the "⛯ Firewall" settings to configure your R&S Unified Firewalls for your local environment. In addition, you can set up access to R&S Unified Firewalls from external networks or the Internet and connect your R&S Unified Firewalls to an R&S Firewall Command Center server.

3.4.1.1 Administrators

Use the "Administrators" settings to define administrators and their access to certain services.

For more detailed information on administrators, see the following sections.

Administrators Overview

Navigate to "Firewall > Administrators" to display the list of administrators that are currently defined on the system in the item list bar.

The plus button ⊕ above the list allows you to add new administrators.

In the expanded view, the first table column displays the "Name" of the administrator. The "Admin" column shows one of the following status indicators:

- Green – The administrator has been granted access to the web client.
- Orange – The administrator has not been granted access to the web client.

The buttons in the last column allow you to view and adjust the settings for an existing administrator. Furthermore, the buttons allow you to create an administrator based on a copy of an existing administrator or delete an administrator from the system.

For further information, see Chapter 3.2, "Icons and Buttons", on page 23.

Administrators Settings

Under "Firewall > Administrators", you can add a new or edit an existing administrator.

You cannot delete or rename the default user `admin`. Furthermore, you cannot withdraw this user's access rights to the web client.

The "Administrator" panel allows you to configure the following elements:

Field	Description
"Name"	Enter a unique name for the administrator.
"Description"	Optional: Enter additional information regarding the administrator for internal use.

On the "Client Access" tab:

Field	Description
"Granting access"	Select this checkbox to grant the administrator access to the web client.
"Password"	For newly added administrators only if the "Granting access" checkbox is selected: Enter a password and confirm it. For edited administrators only if the "Change" checkbox is selected: Enter a password and confirm it.
"Change"	Optional and for edited administrators only if the "Granting access" checkbox is selected: Select this checkbox to change the administrator's password.
"Show Password"	Optional and for newly added administrators only if the "Granting access" checkbox is selected: Select this checkbox to verify the password. Optional and for edited administrators only if the "Change" checkbox is selected: Select this checkbox to verify the password.
"Require password change after next login"	Optional and for newly added administrators only if the "Granting access" checkbox is selected: Select this checkbox if you want the administrator to change the password after the next logon. Optional and for edited administrators only if the "Change" checkbox is selected: Select this checkbox if you want the administrator to change the password after the next logon.

On the "Webclient Permissions" tab, you can specify what the administrator is allowed to do in specified areas of the web client.

You can choose between the following permissions by selecting the respective radio button:

- "Forbidden" – The administrator cannot access the specified area of the web client.
- "Read/Open" – The administrator can open and read the entities in the specified area of the web client but cannot change them.
- "Write/Execute" – The administrator has full access to the entities in the specified area of the web client.

The buttons at the bottom right of the editor panel depend on whether you add a new or edit an existing administrator. For a newly configured administrator, click "Create" to add the administrator to the list of available administrators or "Cancel" to discard your changes. To edit an existing administrator, click "Save" to store the reconfigured administrator or "Reset" to discard your changes. You can click "Close" to shut the editor panel as long as no changes have been made on it.

3.4.1.2 Backup

Your R&S Unified Firewalls stores settings in configuration files which are automatically created whenever settings are changed in the web client. The options under "Backup" allow you to schedule regular backups of the current system configuration, to back up the system configuration manually and to restore previous configurations.

Backups can be created once a license has been imported (that is to say, not during the test period of 30 days).

For more detailed information on backups, see the following sections.

Automatic Backup Settings

The "Auto Backup" settings allow you to set up a connection to a remote backup server on which you want to store automatically created backups. Furthermore, this panel lets you schedule how often the firewall configuration is backed up automatically. There are no restrictions on the amount or interval of backup creation.

Before you proceed, make sure that you set the time zone for your R&S Unified Firewalls as described under Chapter 3.4.1.7, "Time Settings", on page 43. Otherwise, the backups are created according to Europe - Berlin (CET/UTC +1) instead of the time specified by you in the automatic backup settings.

Navigate to "Firewall > Backup > Auto Backup" to open an editor panel to display and edit the settings for automatic backups.

The "Auto Backup" panel allows you to configure the following elements:

Field	Description
"Server Address"	Enter the IP address of the remote backup server on which you want to store automatically created backups.
"Username"	Enter the name of the user on the remote backup server.
"Password"	Enter the user's password for the remote backup server if necessary.
"Show Password"	Optional: Select this checkbox to verify the user's password.
"Server Type"	Select the respective radio button to specify which network protocol is used to upload the backups to the server. The option is set to "FTP" by default, but you can adjust the settings to "SCP" as necessary.
"Filename"	Enter a name for automatically created backup files.

Field	Description
"Encryption Password"	Enter a password for the encryption of the backup files. The password can consist of up to 32 characters (allowed are letters of the English alphabet, integers and the special characters `\-][/.,~!@#$%^*()_+:?><}{`).
"Show Encryption Password"	Optional: Select this checkbox to verify the encryption password.
"Options"	Select the respective radio button to specify what is added to the filenames to distinguish the backups from each other. The option is set to "Append current date to filename" by default, but you can adjust the settings to the other value as necessary: ● "Append current date to filename" – The date and the timestamp of the creation of a backup is added to the filename (e.g. `Backup_20171130-1527.bak`). As these filenames never repeat, old backup files are never overwritten. ● "Max. file count" – A number (backup number) is added to the filename. Specify the maximum number of backup files to be stored by entering an integer in the input field below this option. The option is set to `20` by default. Once the defined number is reached, counting starts anew and the oldest backup file is automatically overwritten.
"Schedule"	Specify how often the firewall configuration is backed up automatically. Under "Start", click the input field to set the date and time of the first backup to be created automatically. A pop-up window with a calender and input fields for setting the date and time opens. You can enter a date in the MM/DD/YYYY format or use the date picker to set a date. You can also set a time by entering the time in the hh:mm:ss format. Under "Interval" and "Unit", define how often the configuration is backed up automatically. Set the interval by entering a number or using the up and down arrows. The option is set to `1` by default. Then, select one of the unit options from the drop-down list. The option is set to `days` by default, but you can adjust the settings to one of the other values as necessary: ● `once` ● `hours` ● `days` ● `months` Click "Add" to add the schedule to the list. You can edit or delete single entries in the list by clicking the corresponding button next to an entry. For further information, see Chapter 3.2, "Icons and Buttons", on page 23. **Note:** If you edit a schedule, a check mark appears on the right of the entry. Click the check mark to be able to save the settings for automatic backups.

To check the connection to the configured backup server, click the "Test Server Settings" button at the bottom left of the editor panel. The system tries to save a test file (`file name_test`) on the backup server. If this test is successful, a text file is saved on the server and a pop-up window with a success message appears. You can delete this text file after the test.

If you modify the settings, click "Save" to store your changes or "Reset" to discard them. Otherwise, click "Close" to shut the editor panel.

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

Backup Export

The "Export" settings allow you to create and export a manual backup of the current firewall configuration. Use this function, for example, to reload a configuration after a system update.

Navigate to "Firewall > Backup > Export" to open an editor panel to create and transfer a manual backup to your computer so you can restore the configuration contained in it later if necessary.

The "Export" panel allows you to configure the following elements:

Field	Description
"Encryption Password"	Enter a password for the encryption of the backup file and confirm it. The password can consist of up to 32 characters (allowed are letters of the English alphabet, integers and the special characters `\-][/.,~!@#$%^*()_+:?><}{`).
"Show Password"	Optional: Select this checkbox to verify the password.
"Use auto backup password"	Optional: Select this checkbox if you want to use the encryption password set for the creation of automatic backup files (see "Automatic Backup Settings" on page 30) instead of entering a new one.

If you want to export the backup file, click "Export". Otherwise, click "Cancel" to shut the editor panel.

Backup Import

R&S Unified Firewalls allows you to upload a previously downloaded backup file to restore the system configuration (e.g. after a new installation).

Navigate to "Firewall > Backup > Import" to load and activate a firewall configuration from a backup file that was created earlier.

To upload an automatically created backup file stored on the backup server, you first have to transfer the backup file from the backup server to your local disk.

The "Import" panel allows you to configure the following elements:

Field	Description
"Backup File"	Click "Select" to open the local disk search. Select an R&S Unified Firewalls backup file to transfer from your local disk. Click "Open" to close the local disk search. The name of the backup file appears in the field.
"Password"	Enter the encryption password which you chose for the export of the file.
"Show Password"	Optional: Select this checkbox to verify the password.

If you want to import the backup file, click "Import". Otherwise, click "Cancel" to shut the editor panel.

If the upload is successful, a success message appears. Confirm that you want to reboot the system by clicking "Reboot". The system restarts, logs you out and opens the R&S Unified Firewalls logon page. Enter your logon credentials and click "Login". The web client appears.

3.4.1.3 Command Center

R&S Firewall Command Center allows you to administrate multiple R&S Unified Firewalls devices in one application.

Navigate to "Firewall > Command Center" to open an editor panel to connect your R&S Unified Firewalls to an R&S Firewall Command Center server via a VPN connection.

To establish the VPN connection, you need VPN certificates for all devices that were signed by the same certificate authority (CA). Therefore, it is advisable to manage the VPN CA and the VPN certificates on one site and then to export and import the VPN certificates from there to the other sites.

For information on how to create, export and import certificates, see Chapter 3.4.7.2, "Certificates", on page 150.

The "Command Center" panel allows you to configure the following elements:

Field	Description
I/O	A slider switch indicates whether the connection to R&S Firewall Command Center is active (I) or inactive (O). By clicking the slider switch, you can toggle the state of the connection. The connection to R&S Firewall Command Center is deactivated by default.
"Host"	Enter the host name or IP address under which R&S Firewall Command Center is reachable from R&S Unified Firewalls.
"Port"	Enter the port number under which R&S Firewall Command Center is reachable (usually port number `11940`).
"Command Center CA"	From the drop-down list, select the CA that was used to sign the R&S Firewall Command Center certificate.

Field	Description
"Firewall Certificate"	From the drop-down list, select the VPN certificate for R&S Unified Firewalls.
"Latitude"/"Longitude"	Optional: Enter the coordinates of the location of your R&S Unified Firewalls using decimal degrees notation, e.g. `53.555483`. The coordinates are used to display your R&S Unified Firewalls on a map in R&S Firewall Command Center. For further information, see the *R&S Firewall Command Center User Manual*.

The buttons at the bottom right of the editor panel allow you to shut ("Close") the editor panel as long as no changes have been made and to store ("Save") or to discard ("Reset") your changes.

For further information, see the *R&S Firewall Command Center User Manual*.

3.4.1.4 High Availability

The "High Availability" (HA) settings allow two independent R&S Unified Firewalls systems to be connected in a master/slave configuration on a dedicated interface. The so-called HA cluster provides failover capability. If the master machine becomes unavailable, the standby (slave) machine assumes its duties.

The master and slave systems are connected via a Cluster Interconnect cable that allows them to communicate with one another and monitor the status of the paired system. The master machine synchronizes its configuration to the slave. On the slave machine, certain rules are applied which allow network communication with the master machine only. If the slave system fails to detect a »heartbeat« signal from the master, it takes over the role of the master system (in the event of a power outage or hardware failure/shutdown).

When the slave machine takes over, it removes the special block rules and sends out a Gratuitous ARP request. The switch which is connected to R&S Unified Firewalls must allow the arping command. On the client machine in the network, it may take a few seconds before its ARP cache is updated and the new master is reachable.

The following figure illustrates a typical network environment with a redundant master/ slave configuration for High Availability.

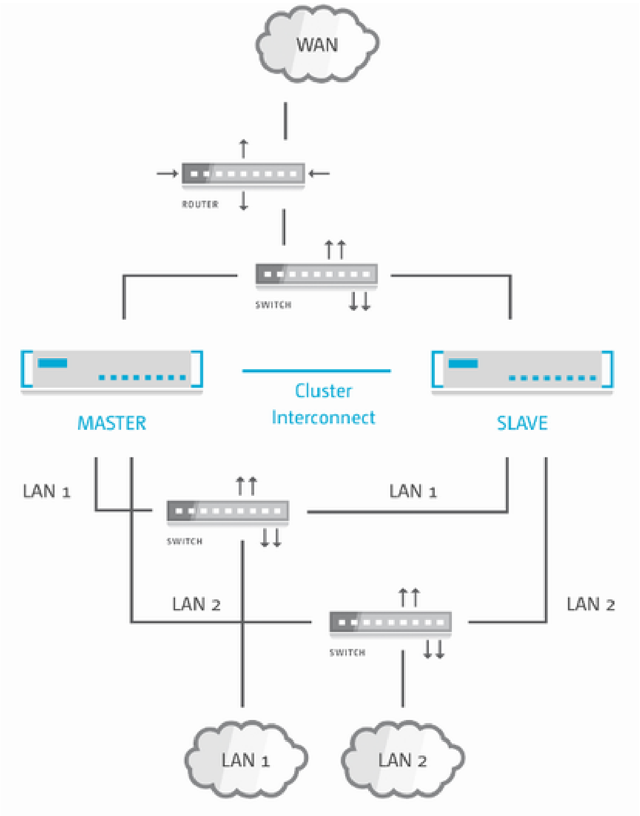


Figure 3-4: Sample network setup for High Availability.

High Availability is not available for the R&S Unified Firewalls GP-U 50/100 and UF-50/100 product models.

For more detailed information on High Availability, see the following sections.

High Availability Settings

Use the "High Availability" settings to specify the connection parameters for the master/ slave configuration.

The High Availability feature requires two identical systems of the same hardware type (for example UF-200 with UF-200 or GP-U 200 with GP-U 200) and software version. Furthermore, a free network interface (NIC) is required on both systems. In other words, you need a network interface that is not currently used by any other interface (like VLAN or bridge) or any network connection. For more information, see Chapter 3.4.3.5, "Interfaces", on page 84 and "Network Connections" on page 73. The same NIC must be used on both systems for Cluster Interconnection.

The master system synchronizes its initial configuration and any subsequent configuration changes to the slave system to ensure that the same configuration is used in the event of failure.

High Availability can only be activated if no background processes, such as updates or backups, are running.

Navigate to "Firewall > High Availability" to open an editor panel to set up High Availability.

The "High Availability" panel allows you to configure the following elements:

Field	Description
I/○	A slider switch indicates whether High Availability is active (I) or inactive (○). By clicking the slider switch, you can toggle the state of High Availability. High Availability is deactivated by default.
"Status"	Displays the High Availability status of R&S Unified Firewalls. The status can be one of the following: ● `Disabled` – High Availability is not enabled on the firewall. ● `No connection` – High Availability is enabled on the firewall but the other firewall cannot be reached. ● `Not synced` – High Availability is enabled on the firewall, the other firewall can be reached but the configuration from the master system has not been synchronized to the standby (slave) system yet. ● `Synchronized and ready` – High Availability is enabled on the firewall, the other firewall can be reached and is synchronized.
"Initial Role"	Select the respective radio button to specify the role which R&S Unified Firewalls is to play in the HA cluster: ● "Master" – R&S Unified Firewalls is active and synchronizes its configuration to R&S Unified Firewalls being the slave. ● "Slave" – R&S Unified Firewalls is not active (i.e. it cannot be reached using the web client) but the master machine synchronizes its configuration to it.
"HA Interface"	From the drop-down list, select the interface to be used for the HA cluster communication. This interface cannot be used for any other firewall services. **Note:** The same interface (NIC) must be used on both R&S Unified Firewalls systems for Cluster Interconnection.
"Local IP"	Enter the IP address which you want to assign to the HA interface on R&S Unified Firewalls in CIDR notation (IP address followed by a slash »/« and the number of bits set in the subnet mask, for example `192.168.50.1/24`).
"Remote IP"	Enter the IP address under which R&S Unified Firewalls can reach the other R&S Unified Firewalls of the HA cluster.

"Local IP" and "Remote IP" must be in the same subnet. HA cluster communication over routed networks is not supported.

If you modify these settings, click "Save" to store your changes or "Reset" to discard them. Otherwise, click "Close" to shut the editor panel.

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

Before you connect the slave system to the master with the Cluster Interconnect cable and configure High Availability on the slave, the configuration of the master system must be complete and activated.

Connect the slave system with the same »WAN« and »LAN« network components as the master system (see Figure 3-4).

Only the master system can be reached and configured using the web client.

If you want to change the High Availability configuration (for example to change the HA interface), first disable High Availability, then change the configuration. Then, turn High Availability back on with the new configuration.

To remove the slave system from the High Availability configuration and operate it as a standalone system, reinstall your R&S Unified Firewalls. For further information, see "Disabling High Availability Configurations" on page 38.

Updating High Availability Configurations

Always update both systems (master and slave). Otherwise, High Availability does not work correctly.

When High Availability is enabled, proceed as follows to update the master and slave systems:

1. Disable High Availability. For more information, see "Disabling High Availability Configurations" on page 38.
2. Update both systems separately. For more information, see Chapter 3.4.1.8, "Updates Settings", on page 44.
3. Enable High Availability. For more information, see "High Availability Settings" on page 35.

Disabling High Availability Configurations

To disable High Availability, perform the following steps:

1. Switch off the standby (slave) machine.
2. Disconnect the Cluster Interconnect cable between the master and slave systems.
3. Reinstall the standby (slave) system via USB flash drive.
4. On the master system:
   a) Log on to the web client.
   b) Under "Firewall > High Availability":
      - Use the slider switch to disable High Availability.
      - Click "Save" to store your settings.
      - Click "✔ Activate" in the toolbar at the top of the desktop to apply your configuration changes.

   Note: If you disconnect the Cluster Interconnect cable without switching off the standby (slave) machine, the slave takes over and the old master runs as master as well. Both machines deliver the same services on the network which has unintended effects. So, it is advisable not to disconnect the Cluster Interconnect cable while both master and slave system are still on.

3.4.1.5 License

The exact feature set of R&S Unified Firewalls depends on the license acquired from your vendor.

When first started after delivery or a new installation, R&S Unified Firewalls runs as a test version for 30 days. You can see that it is a test version in the notification on the "License Manager" panel under "Firewall > License". During this period of time, it is not possible to create backups. After this period of time, the firewall remains active with your configuration. However, you are not able to make any changes and the HTTP and HTTPS protocols are blocked.

The following licensable features can be included in an R&S Unified Firewalls license:

- Antispam (UTM license)
- Antivirus (UTM license)
- Application Filter
- Content Filter
- IDS/IPS (UTM license)
- WLAN

Navigate to "Firewall > License" to open an editor panel to view the validity period of your R&S Unified Firewalls license and additional feature licenses or to upload a new license.

In fixed intervals, the system checks the expiration dates of the license and individual feature licenses in the license file. When a license expires, all licensable features are deactivated until a new license is acquired and uploaded via the web client under "Firewall > License". The new license has to comply with the software version number of R&S Unified Firewalls and the hardware.

To upload a new license, perform the following steps:

1. Click "Select File" behind the "License File" input field.

   The local disk search opens.

2. Select a new license file from the local disk.
3. Click "Open".

   The local disk search closes.

4. Click "License" to upload the license file.

   The license is uploaded. If the upload is successful, all licenses and the information about them are automatically entered in R&S Unified Firewalls and a success message appears.

5. Confirm that you want to log out by clicking "OK".

   The system logs you out and opens the R&S Unified Firewalls logon page.

6. Enter your logon credentials.
7. Click "Login".

   The web client appears.

3.4.1.6 Firewall Access

The "Firewall Access" settings allow you to define how R&S Unified Firewalls can be accessed from external networks or the Internet. In addition, you can determine how R&S Unified Firewalls reacts, for example, to ping requests.

The "Firewall Access" settings only apply to external access to R&S Unified Firewalls for defined users. Accessing R&S Unified Firewalls from the internal network is always possible.

Navigate to "Firewall > Firewall Access" to determine whether and how access from external networks or the Internet to R&S Unified Firewalls is allowed.

For more detailed information on the "Firewall Access" settings, see the following sections.

Ping Settings

The "Ping Settings" allow you to specify how R&S Unified Firewalls handles ICMP echo requests (ping) to the firewall from the internal network and the Internet.

Navigate to "Firewall > Firewall Access > Ping Settings" to open an editor panel to display and edit the ping settings.

Field	Description
"Ping (ICMP to Firewall)"	Select the respective radio button to specify how R&S Unified Firewalls handles ICMP echo requests to the firewall from the internal network and the Internet. The option is set to `Allow` by default, but you can adjust the settings to the other value as required: ● `Deny` – R&S Unified Firewalls does not respond to ICMP echo requests to the firewall from the internal network and the Internet. ● `Allow` – R&S Unified Firewalls reponds to ICMP commands to the firewall from the internal network and the Internet. **Note:** While blocking ICMP echo requests can improve the security of R&S Unified Firewalls, it also makes any troubleshooting in the network difficult. Therefore, if an error occurs in the network, we recommended setting this option to `Allow` before you start troubleshooting.

If you modify the settings, click "Save" to store your changes or "Reset" to discard them. Otherwise, click "Close" to shut the editor panel.

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

SSH Settings

The "SSH Settings" allow you to configure SSH access to your R&S Unified Firewalls from the Internet.

Navigate to "Firewall > Firewall Access > SSH Settings" to open an editor panel to display and edit the SSH settings.

The "SSH Settings" panel allows you to configure the following elements:

Field	Description
I/○	A slider switch indicates whether the SSH service is active (I) or inactive (○). By clicking the slider switch, you can toggle the state of the service. The SSH service is activated by default.
"Port"	Set the listening port by entering the port number. The default setting is port 22.
"Password Authentication"	Password authentication allows you to login to R&S Unified Firewalls via SSH using a password. Password authentication is activated by default. **Note:** Password authentication can only be deactivated if at least one SSH public key is actively used for key authentication.

Field	Description
"SSH Public Keys"	This table displays the SSH public keys that are used to authenticate a user without a password. Click "Add" to open the "SSH Key" panel and add a new key. On this panel, you can define the following settings: ● In the "Key" field, enter or paste the SSH public key. ● In the "Title" field, enter a name for the SSH public key. **Note:** R&S Unified Firewalls only supports keys in Secure Shell (SSH) Public Key File Format. The buttons at the bottom right of the editor panel allow you to confirm your changes ("OK") and to discard your changes ("Cancel"). The "SSH Key" panel shuts automatically. The SSH public key appears as a list entry ("Fingerprint"). You can edit or delete single entries in the list by clicking the corresponding button next to an entry. For further information, see Chapter 3.2, "Icons and Buttons", on page 23. **Tip:** You can use these authentication methods ("Password Authentication", "SSH Public Keys") alone or in combination.
"Access Restrictions"	This table displays user-defined IP addresses or IP networks that can be allowed access to R&S Unified Firewalls (whitelist mode). Select the checkbox next to an entry to allow access. To add an IP address or network to the list, enter a "Title" and "Source" and click "Add". The new entry is added to the list and is activated automatically. The following entries are predefined and cannot be removed: ● "Local Networks" represents the internal access and is activated by default. ● "Internet" provides SSH access to R&S Unified Firewalls from the Internet. **Note:** In certain circumstances, this may grant attackers access to R&S Unified Firewalls. Therefore, we do not recommend using this option as a permanent solution. ● "VPN Tunnels" The following default entries include network sections for the customer support. These entries are deactivated by default. ● "Rohde & Schwarz Internet Gateway" ● "Rohde & Schwarz Cybersecurity Customer Support"

If you modify the settings, click "Save" to store your changes or "Reset" to discard them. Otherwise, click "Close" to shut the editor panel.

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

Webclient Settings

The "Webclient Settings" allow you to configure external web access to your R&S Unified Firewalls from the Internet.

Navigate to "Firewall > Firewall Access > Webclient Settings" to open an editor panel to display and edit the webclient settings.

The "Webclient Settings" panel allows you to configure the following elements:

Field	Description
"Port"	Set the listening port by entering the port number. The default setting is port 3438.
"Webclient Certificate"	Select a webclient certificate that is used to verify the SSL connection. **Note:** If you do not select a webclient certifcate, an auto-generated, self-signed system certificate is used. The system certificate is not part of the certificate management. To avoid certificate warnings from your browser when connecting to the webclient, select a certificate that was signed by a CA trusted by your browser.
"Access Restrictions"	This table displays user-defined IP addresses or IP networks to allow access for these addresses only (whitelist mode). Enter a "Title" and "Source". Click "Add" to add the IP address to the list. The following entries are read-only, but can be activated or deactivated. ● "Local Networks" represents the internal access and is activated by default. ● "Internet" provides SSH access to R&S Unified Firewalls from the Internet. **Note:** In certain circumstances, this may grant attackers access to R&S Unified Firewalls. Therefore, we do not recommend using this option as a permanent solution. ● "VPN Tunnels" The following default entries include network sections for the customer support. The entries are deactivated by default. ● "Rohde & Schwarz Internet Gateway" ● "Rohde & Schwarz Cybersecurity Customer Support" Optional: Clear the checkbox next to an entry to restrict access for it. **Note:** The webclient access is the main access type to the server. You have to select at least one entry in the list of IP addresses.

If you modify the settings, click "Save" to store your changes or "Reset" to discard them. Otherwise, click "Close" to shut the editor panel.

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

3.4.1.7 Time Settings

R&S Unified Firewalls works with time-sensitive rules. Furthermore, the system time is particularly important for services such as logging that rely on accurate timestamps. Therefore, it is necessary to set the date and time correctly.

Navigate to "Firewall > Time Settings" to open an editor panel to display and edit the system date and time settings.

The "Time Settings" panel allows you to configure the following elements:

Field	Description
"Time Zone"	From the drop-down list, select one of the predefined time zones. The time zone is set to `(+01:00) Europe - Berlin` by default, but you can adjust the settings to one of the other values as required.
"Current Time"	Check the current system date (MM/DD/YYYY) and time (hh:mm:ss) of R&S Unified Firewalls.
"Date & Time"	Optional: Click the input field to set a new system date or time manually. A pop-up window with a calender and input fields for changing the date and time opens. You can enter a date in the MM/DD/YYYY format or use the date picker to set a new date. You can also set a new time by entering the time in the hh:mm:ss format. **Note:** To set the system time manually, NTP has to be disabled (in other words, the "NTP Client" checkbox must be cleared). Otherwise, the time will be reset automatically as soon as the system sends the next NTP request.
"NTP Client"	Optional: Select the checkbox to use remote network time protocol servers to set the system date and time automatically.

Field	Description
"NTP Servers"	Optional and only available if the "NTP Client" checkbox is selected: You can either use the predefined NTP servers or add your own NTP servers to the list. The standard NTP servers are: de.pool.ntp.org and europe.pool.ntp.org. You can add as many NTP servers as you like. Enter the IP address or the fully qualified domain name of an NTP server in the input field. Then, click "Add" to put the NTP server on the list. You can edit or delete single entries in the list by clicking the corresponding button next to an entry. For further information, see Chapter 3.2, "Icons and Buttons", on page 23. **Note:** If you edit an NTP server, a check mark appears on the right of the entry. Click the check mark to be able to save the settings of the NTP server. **Note:** If more than one NTP server is configured, R&S Unified Firewalls automatically synchronizes the system clock with the server that transmits the best time signal.
"Serve as local NTP server"	Optional and only available if the "NTP Client" checkbox is selected: Select this checkbox if you want to make the system time of R&S Unified Firewalls available in the internal network. R&S Unified Firewalls then acts as an internal, local NTP server.

If you modify these settings, click "Save" to store your changes or "Reset" to discard them. Otherwise, click "Close" to shut the editor panel.

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

3.4.1.8 Updates Settings

The "Updates Settings" panel allows you to keep R&S Unified Firewalls up to date at all times. New software, hotfixes, security updates and new functions can be automatically downloaded from the update server and installed on the firewall quickly and easily. In addition, the update system is equipped with various functions for notifying the system administrator if there are new updates available. Furthermore, you can view the history of imported updates.

To prevent any unauthorized or malicious updates from being installed on the firewall, all R&S Unified Firewalls updates are signed digitally. Only updates with a valid signature are displayed and installed.

Navigate to "Firewall > Updates Settings" to open an editor panel to display the list of available updates with information about them and their status on the "Updates" tab.

The "Filter" input field allows you to narrow the list of results in the table below it. As you type in the input field, R&S Unified Firewalls automatically refreshes the list to show only those entries that contain the characters you are typing as a name, type or description. Click ⊗ in the input field to delete the search string and display an unfiltered view of the list.

The table columns of the updates list contain the following information:

Column	Description
"Name"	Displays the name of the available update.
"Type"	Displays the type of update. The update system differentiates between four types of updates: ● `security` – contains corrections concerning the security of the firewall ● `recommended` – contains corrections as well as performance and stability optimizations ● `hotfix` – contains corrections for the firewall modules but also new functions ● `upgrade` – contains an upgrade to the next R&S Unified Firewalls software version
"Description"	Displays a text field with further information about the update. The text field can be unfolded to view all information relating to the update by clicking it.
"Reboot"	Indicates whether a reboot of the system is required after the update has been installed successfully.
"Release Date"	Displays the date when the update was released.
"Status"	Distinguishes between `new` updates and updates which have already been installed. **Note:** An update cannot be installed more than once.
"Action / Dependency"	If all dependencies are met, the "Install" action is allowed. Otherwise, a list of dependencies is displayed. To meet the dependencies, install the listed updates.

Click "Refresh Updates List" to update the list of available updates with the latest versions manually.

The "Settings" tab allows you to configure the following elements:

Field	Description
"Search for New Updates Automatically"	Select this checkbox to refresh the list of available updates with the latest versions automatically.
"Interval"	From the drop-down list, select the desired frequency with which the list of updates is refreshed. The option is set to `Daily` by default, but you can adjust the settings to one of the other values as required: ● `Hourly` ● `Daily` ● `Weekly`

Field	Description
"Update Time"	Enter the date and time for the first automatic refresh of the updates list and the first automatic update. If you click the input field, a pop-up window with a calender and input fields for changing the date and time opens. You can enter a date in the format MM/DD/YYYY or use the date picker to set a new date. You can also set a new time by entering the time in the format hh:mm:ss. **Note:** All subsequent updates are carried out at the time set here if the automatic installation of updates described below is enabled.
"Install Updates Automatically"	Select the respective radio button to specify which updates you want to be imported and installed automatically on R&S Unified Firewalls. This function is limited to security and recommended hotfixes. The option is set to `None` by default, but you can adjust the settings to one of the other values as required.
"Update Servers"	The standard update server is: http://cybersecurity.rohde-schwarz.com/updateserver/updates. You can add as many update servers as you like. Enter the URL of an update server and click "Add" to put the update server on the list. **Note:** If the URL contains a fully qualified domain name (FQDN), you need to configure the DNS settings. Otherwise, the FQDN cannot be resolved. You can edit or delete single entries in the list by clicking the corresponding button next to an entry. For further information, see Chapter 3.2, "Icons and Buttons", on page 23. **Note:** If you edit an update server, a check mark appears on the right of the entry. Click the check mark to be able to save the settings of the update server.

The "History" tab displays the update history of R&S Unified Firewalls.

If you modify the settings on the "Updates Settings" panel, click "Save" to store your changes or "Reset" to discard them. Otherwise, click "Close" to shut the panel and return to the overview of your entire configured network.

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

NOTICE

For information on the installation of system updates in a High Availability configuration, see "Updating High Availability Configurations" on page 37.

Important: Always update both systems (master and slave). Otherwise, High Availability does not work correctly.

3.4.1.9 User Authentication

The "User Authentication" settings determine the list of users who can be authorized to utilize your network resources, such as Internet access and VPN tunnels. Furthermore, these settings allow you to set up local users and to connect R&S Unified Firewalls to an external directory service from where it can retrieve individual users and user groups. This allows you to set firewall regulations not just for computers but also for individual users and user groups.

Navigate to "Firewall > User Authentication" to display the list of users that are currently defined on the system in the item list bar.

For more detailed information on user authentication, see the following sections.

Technical Background and Preparations

Purpose of user authentication

With user authentication, firewall rules can be assigned to users when they are logged on. Only one user per IP address can be logged on. If another user logs on from an IP address which is already in use for a session, the other logged-on user is logged out and the new user is logged on.

Logging on to the firewall

R&S Unified Firewalls runs a special web server which only processes user logons. It receives the user name and password. With a user database which is created locally on R&S Unified Firewalls, an authentication service first verifies whether the user name and password are admissible. If this logon fails and a Microsoft Active Directory server or an openLDAP server are configured on R&S Unified Firewalls, the authentication service additionally queries those directory servers via Kerberos protocol to see whether the user can be authenticated. If the authentication was successful, the IP address from which the request was sent is assigned the firewall rules for this user.

Users who are registered in the local database of R&S Unified Firewalls can change their password over the web server. The password can consist of up to 248 characters. Longer passwords are accepted nevertheless, but they are cut off automatically.

Certain computers, such as terminal servers on which many users work at the same time or servers to which only administrators log on, can be excluded from the user authentication. Web servers and the authentication service then do not accept any user logons from the IP addresses of these computers.

Since all users have the same IP address on a terminal server, R&S Unified Firewalls cannot identify individual users in the network. For this purpose, Microsoft offers the so-called Remote Desktop IP Virtualization for Server 2008 R2 and newer versions. With this application, every user obtains their own IP address from a pool of IP addresses, similar to DHCP.

Authentication server

For smaller companies without central user management, R&S Unified Firewalls provides local user management. You can always use the local user database. However, it is also possible to use an external directory service, such as Microsoft Active Directory server or an openLDAP server. Both Microsoft Active Directory and openLDAP use the Kerberos protocol to validate the credentials provided by any of the user authentication clients.

Active directory groups

If you are using a Microsoft Active Directory server for authentication, the Active Directory groups are displayed in the user authentication item list bar as well. Active Directory groups are a powerful tool to set up and maintain security policies for each user. For example, you can allocate Active Directory users to certain Active Directory groups and then create firewall rules for these groups on R&S Unified Firewalls.

Logging on

There are three different ways users can log on to R&S Unified Firewalls:

- "Logging on using a web browser" on page 48
- "Logging on using the R&S Unified Firewalls User Authentication Client" on page 49
- "Logging on using the R&S Unified Firewalls Single Sign-On Client" on page 51

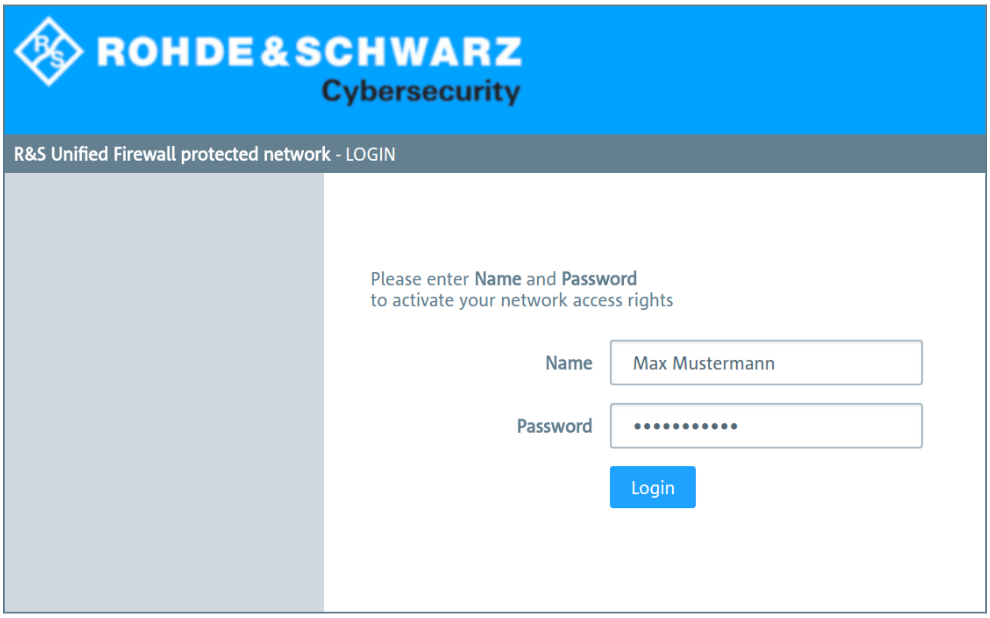
Logging on using a web browser

Once users have been set up as desktop objects and firewall rules for these users have been configured, they can act according to the rules using the so-called landing page. The logon via web browser method works with any browser and is SSL-encrypted.

To log on to R&S Unified Firewalls via a web browser, perform the following steps:

1. Start a web browser.
2. Make sure cookies are activated.
3. Enter the IP address of your R&S Unified Firewalls, for example `https://192.168.12.1` (using the default port 443), in the address bar.

   A special web page presenting the R&S Unified Firewalls landing page appears.



Please enter Name and Password
to activate your network access rights

Name: Max Mustermann

Password: •••••••••••

Figure 3-5: User authentication using a web browser

4. Enter the "Name".
   Note: If the user is an LDAP user, the user's login name has to exactly match the user name specified in the sAMAccountName attribute of the user. Otherwise, the name in the user-specific firewall rules will not correspond to the user logging on to the client and the rules will not match.
5. Enter the "Password" of the user.
6. Click "Login".

   The authentication is carried out.

NOTICE

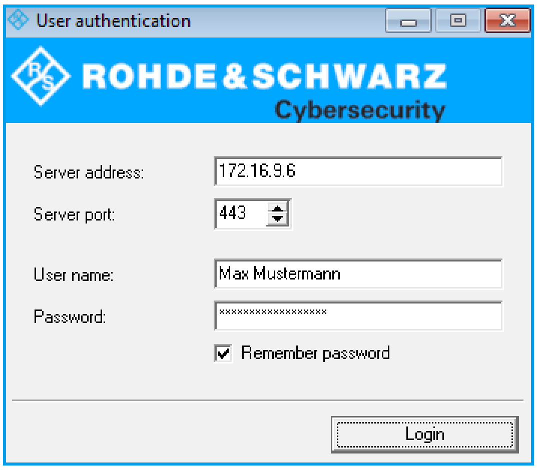
For security reasons, the browser window that was used to log on must remain open during the whole session. Otherwise, the user is logged out automatically after one minute. This is to prevent unauthorized persons from accessing the firewall from a computer where a user forgot to log out of.

Logging on using the R&S Unified Firewalls User Authentication Client

The Windows-based R&S Unified Firewalls User Authentication client provided with R&S Unified Firewalls is located in the `UAClient` directory on the USB flash drive.

To log on to R&S Unified Firewalls using the R&S Unified Firewalls User Authentication client, perform the following steps:

1. Install the R&S Unified Firewalls User Authentication client.
2. Start the R&S Unified Firewalls User Authentication client.



User authentication

ROHDE&SCHWARZ Cybersecurity

Server address: 172.16.9.6

Server port: 443

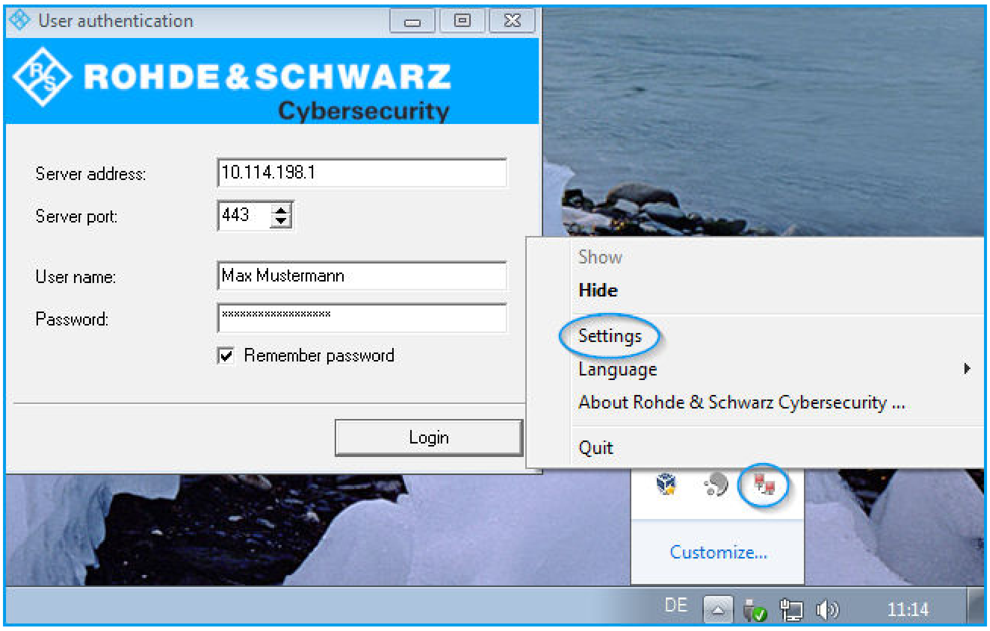
User name: Max Mustermann

Password: ******************

☑ Remember password

Figure 3-6: User authentication using the R&S Unified Firewalls User Authentication client.

3. Under "Server Address", enter the IP address of your R&S Unified Firewalls.
4. Enter the "User Name".
   Note: If the user is an LDAP user, the user's login name has to exactly match the user name specified in the sAMAccountName attribute of the user. Otherwise, the name in the user-specific firewall rules will not correspond to the user logging on to the client and the rules will not match.
5. Enter the "Password" of the user.
6. Optional: Select the "Remember password" checkbox if you want the password to be saved for future logons.
7. Optional: Adjust the period of time for reconnection under "Settings" by right-clicking the system tray icon in the Windows taskbar.



Server address: 10.114.198.1
Server port: 443
User name: Max Mustermann
Password: ******************
☑ Remember password
Login

Figure 3-7: Adjusting the settings of the R&S Unified Firewalls User Authentication client.

8. Click "Login".

   The authentication is carried out.

NOTICE

For security reasons, it is strongly recommended to update the R&S Unified Firewalls User Authentication client to the latest version available. However, a compatibility mode that allows older versions of the R&S Unified Firewalls User Authentication client to work with R&S Unified Firewalls version 10 can be enabled. For more information, see "User Authentication Settings" on page 54.

Logging on using the R&S Unified Firewalls Single Sign-On Client

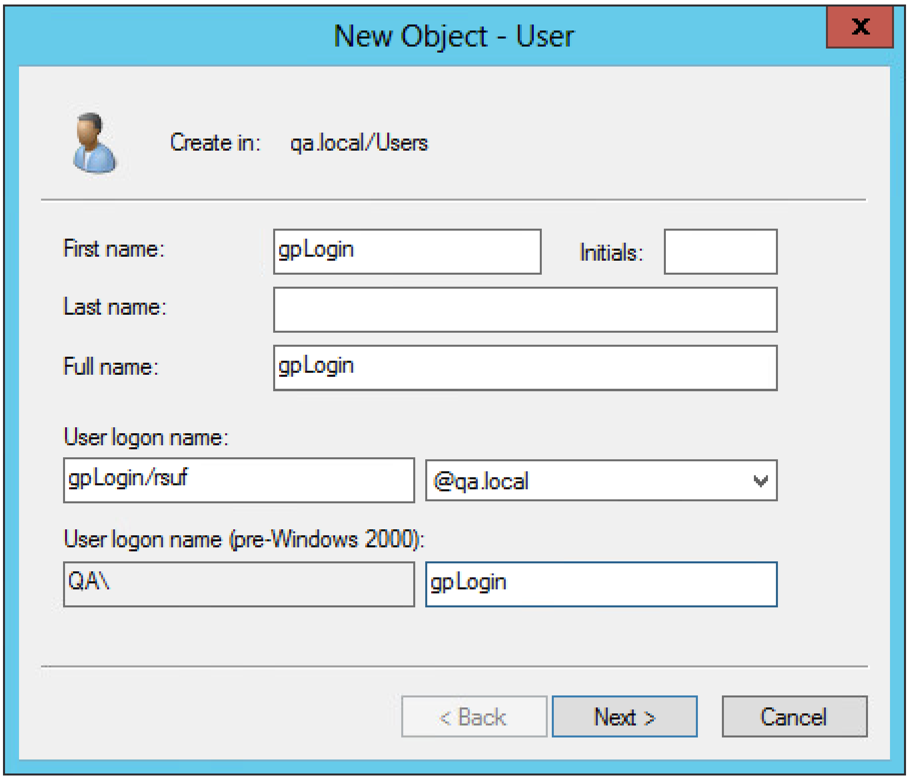
When using Single Sign-On (SSO), domain users from the Active Directory domain log on to a Windows client. Firewall rules configured on R&S Unified Firewalls concerning these users are then automatically applied.

To realize SSO with R&S Unified Firewalls in an Active Directory environment, the following preconditions have to be met:

1. As Kerberos is time-critical, make sure to set the same time/NTP server for all components of SSO (domain controller, Windows client and R&S Unified Firewalls).
2. Creating the user `gpLogin`
   It is necessary to create a normal domain user in the user management under "CN=Users" in the Active Directory. This user is then assigned a so-called Service

Principal Name (SPN) which is needed for the authentication of R&S Unified Firewalls on the server. The user does not need any specific rights.

a) Open the domain controller.



Create in: qa.local/Users

First name: gpLogin

Initials:

Last name:

Full name: gpLogin

User logon name: gpLogin/rsuf @qa.local

User logon name (pre-Windows 2000): QA\ gpLogin

Figure 3-8: Creating a new user – user logon name.

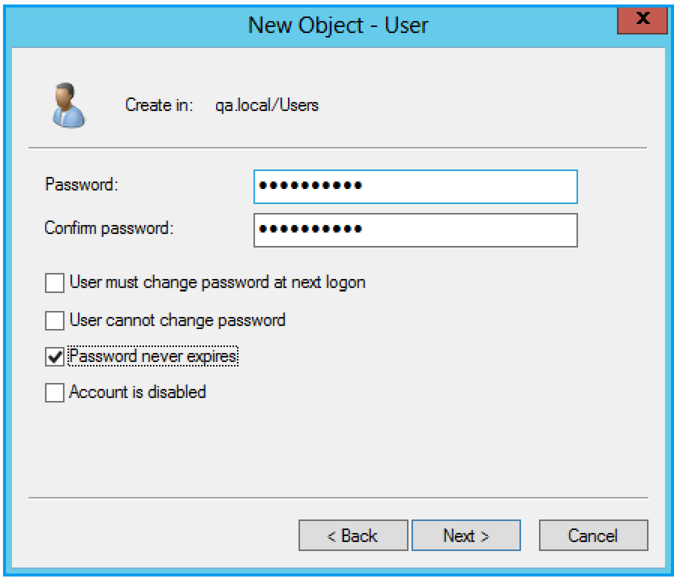
b) Under "First name", enter `gpLogin`.
With this name, it is easier to find the user later in the user overview.

c) Under "User logon name", enter `gpLogin/<firewall name>`.
In the example above, the host name (`<firewall name>`) of R&S Unified Firewalls is `rsuf` and, therefore, the user logon name is `gpLogin/rsuf`.

d) Under "User logon name (pre-Windows 2000)", enter `gpLogin`.

e) Click "Next".

f) Enter a password for the user and confirm it.



New Object - User

Create in: qa.local/Users

Password: ••••••••••

Confirm password: ••••••••••

□ User must change password at next logon

□ User cannot change password

☑ Password never expires

□ Account is disabled

Figure 3-9: Creating a new user – user password.

g) Select the "Password never expires" checkbox.
h) Click "Next".
i) Verify the information relating to the new user by clicking "Finish".

The user `gpLogin` is created.

3. Using the `gpLogin` user to query the Active Directory
   In the "User Name" input field under "Authentication Server", enter `gpLogin`.

4. Configuring the Service Principal Name (SPN)
   Assign an SPN to the newly created user so that R&S Unified Firewalls is able to create a position of trust regarding the domain controller. To do so, run the following command on the domain controller: `setspn -A gpLogin/rsuf gpLogin`

5. Generating a Kerberos Key
   Using the R&S Unified Firewalls Single Sign-On client, a user's logon on the Windows domain can be forwarded to R&S Unified Firewalls. With the Kerberos key, your R&S Unified Firewalls is able to check the forwarded information and activate the user-specific firewall rules. To generate a Kerberos key, perform the following steps:

   a) Log on to R&S Unified Firewalls.
   b) Navigate to "Firewall > User Authentication > Settings".
      The "User Authentication Settings" editor panel opens.
   c) Enable the user authentication settings by toggling the slider switch to "I".
   d) On the "Kerberos" tab, click the "Create Kerberos Key" button to generate the Kerberos key.

   The Active Directory is queried to validate the specified AD user and to obtain the relevant information, such as the Kerberos key version number. With that information, R&S Unified Firewalls is able to generate a valid Kerberos key locally.

6. Activating SSO on R&S Unified Firewalls
   To enable SSO on R&S Unified Firewalls, perform the following steps:
   a) On the "Kerberos" tab, select the "Active" checkbox.
   b) Click "Save" to store your settings.
7. Preparing the Windows client

   You can find the Windows Installer Single Sign On ZIP archive at https://www.rohde-schwarz.com/cybersecurity/rsuf-downloads. There are three ways to install the R&S Unified Firewalls Single Sign-On client:
   - Copy the `UAClientSSO.exe` standalone application to your desired target location
   - Run the `UAClientSSOSetup.exe` setup program and install the `UAClientSSO.exe` standalone application under `C:\Program Files\R&S Cybersecurity\UA Client\3.0\`
   - Deploy the client through the domain, using the `UAClientSSO.msi` Microsoft installer in a group policy object

   Note: In all cases, the `UAClientSSO.exe` standalone application will be installed on the Windows PC. It can then be executed given the following parameters:
   - The host name of R&S Unified Firewalls (for more information, see "User Authentication Settings" on page 54)
   - The IP address of R&S Unified Firewalls in the network of the client computer

   Example: The host name of R&S Unified Firewalls is rsuf. Its IP address in the network of the client computer is 192.168.0.1. The target path for the installation of the R&S Unified Firewalls Single Sign-On client then is `C:\Program Files\R&S Cybersecurity\UA Client\3.0\UAClientSSO.exe rsuf 192.168.0.1`.

User Authentication Settings

The "User Authentication Settings" allow you to activate and deactivate user authentication in general. Furthermore, you can specify the connection parameters for the directory server that is used to manage the LDAP users and groups on your network.

Navigate to "Firewall > User Authentication > Settings" to open an editor panel to define the general settings for user authentication and the directory service.

The "User Authentication Settings" panel allows you to configure the following elements:

Field	Description
I/O	A slider switch indicates whether user authentication is active (I) or inactive (O). By clicking the slider switch, you can toggle the state of user authentication. User authentication is disabled by default.

On the "General" tab:

Field	Description
"Log Logins"	Select this checkbox if you want to log all logons to R&S Unified Firewalls. You can view all logon events under "Monitoring & Statistics > Logs > System Log".
"Login Mode"	Select one of the following four options: ● "Single Login (deny new login)" – No user can be logged on from more than one IP address at the same time. ● "Single Login (disconnect old login)" – Any previous logons are first disconnected when the user logs on from another IP address. ● "Multiple Logins" – A user can be logged on from up to 254 different IP addresses at the same time. ● "Multiple Logins (with warning in report)" – A user can be logged on from up to 254 different IP addresses at the same time and alerts are recorded in the report.
"Web Login Port"	Set the HTTPS port for the web logon by entering the port number or using the up and down arrows. The default setting is port `443`.
"Compatibility Mode"	Select this checkbox if you are using user authentication clients older than version 3.0.0 to log on to R&S Unified Firewalls. **Notice:** By selecting this checkbox you are putting your network security at risk. For more information, see Chapter 3.4.1.9, "User Authentication", on page 47.
"Show Landing Page"	Optional: Select this checkbox to display a landing page when an unauthorized user tries to access the Internet.

For each IP address, only one user logon is supported, even if multiple logons are activated.

On the "Authentication Server" tab, you can specify on the type of database to be used. You can use the local user database on R&S Unified Firewalls independently or in addition to a Microsoft Active Directory server or an openLDAP server with Kerberos as an external user database.

If you select `Microsoft Active Directory Server`, you can configure the following elements:

Field	Description
"Host"	Enter the host name or the IP address of the directory server. **Note:** If you enter the host name of the directory server, you need to configure the DNS settings. Otherwise, the host name cannot be resolved.
"Port"	Enter the directory server's port number to be used for communication. You can also select the port number by using the up and down arrows.
"User Name"	Enter the name of a user with read rights to retrieve the list of users of the domain from the Active Directory. This field must be the sAMAccountName attribute of the user. The user has to be placed in "CN=Users". For more information, see "Logging on using the R&S Unified Firewalls Single Sign-On Client" on page 51.
"Password"	Enter the password of the user that has read rights. **Tip:**We recommend to create a dedicated user for this purpose.
"Domain Name"	Enter the domain name of the Active Directory.

To test the configured Microsoft Active Directory server settings, click "Test AD Settings".

If you select `OpenLDAP Server`, you can configure the following elements:

Field	Description
"Server Address"	Enter the host name or the IP address of the directory server. **Note:** If you enter the host name of the directory server, you need to configure the DNS settings. Otherwise, the host name cannot be resolved.
"Port"	Enter the directory server's port number to be used for communication. You can also select the port number by using the up and down arrows.
"User DN"	Enter the user DN of an account that has read rights. **Tip:** It is not mandatory to provide the full user DN. Upon clicking "Save", the system automatically adds the domainComponents from the "Base DN" entry.
"Password"	Enter the password of the user that has read rights.
"Base DN"	Enter a distinguished name (base DN) as a sequence of relative distinguished names (RDN) separated by commas, such as three domainComponents: `dc=ldap,dc=example,dc=com`, to define the location within the directory from where the directory search should start.
"User Query"	Optional: Specify the filter to be used to retrieve the list of users.

Field	Description
"User ID"	Optional: Define the attribute where the user identifier is retrieved from. The user names displayed in the web client are actually coming from this attribute of the LDAP User. The user ID is retrieved from the `sAMAccountName` attribute by default.
"User Name"	Optional: Define the attribute where the user name is retrieved from.
"User Group"	Optional: Define the attribute where the user group is retrieved from.
"User Primary Group"	Optional: Define the attribute where the user primary group is retrieved from.
"Mail Query"	Optional: Specify the filter to be used to retrieve the list of mails.
"Mail Name"	Optional: Define the attribute where the mail name is retrieved from.
"Group Query"	Optional: Specify the filter to be used to retrieve the list of groups.
"Group Name"	Optional: Define the attribute where the group name is retrieved from.
"Group ID"	Optional: Define the attribute where the group identifier is retrieved from.
"Group Primary ID"	Optional: Define the attribute where the group primary identifier is retrieved from.
"Group Parent"	Optional: Define the attribute where the group parent is retrieved from.

Upon clicking "Save", the system completes all optional fields which you did not specify with default values.

If you wish to use Kerberos for Single Sign-On, the name of the user must be `gpLogin`. For more information, see "Logging on using the R&S Unified Firewalls Single Sign-On Client" on page 51.

On the "Kerberos" tab:

Field	Description
"Active"	Select this checkbox to activate the Kerberos service.
"Kerberos Key"	Displays the service name, the host name and the domain related to the userPrincipalName of the most recently created Kerberos key, also known as keytab. For more information, see "Logging on using the R&S Unified Firewalls Single Sign-On Client" on page 51.

Field	Description
"Host Name"	If necessary, adjust the host name of your R&S Unified Firewalls.
"Domain"	If necessary, adjust the domain of your R&S Unified Firewalls so that it matches the domain of the Active Directory.

Users

Just like computers, users and LDAP groups can be set up on the desktop as individual users or user groups.

For these desktop objects, you then define the rules which are to be assigned to the users as soon as they log on. If users log on from a computer to which certain rules are assigned, the rules of this computer and their personal rules are applied to these users. You can select users and LDAP groups from the local user database on R&S Unified Firewalls and from the openLDAP or Active Directory authentication server and add them to the user groups on the desktop. There is also a special "Default User Group" which can be selected on the desktop. To this user group, no users are added. It comprises all of the users who are able to log on but have not been set up as individual users or members of other user groups on the desktop. If such a default user group is set up on the desktop and if you have assigned rules to it, users who is later created in the Active Directory server are automatically allocated to this default user group. After logon, these new users are automatically assigned the default rules without any additional administration effort for each individual user.

LDAP Groups

It is possible to connect R&S Unified Firewalls to an external directory server using the Lightweight Directory Access Protocol (LDAP) to retrieve user groups from there. You can include these user groups in group-specific firewall rules.

LDAP can be used by medium to large companies to access directory services and to manage user data.

Connect to a directory server as described under "User Authentication Settings" on page 54.

Navigate to "Firewall > User Authentication > LDAP Groups" to display the list of LDAP groups that are currently defined on the directory server in the item list bar.

To make LDAP groups in this list available for use in connections and group-specific firewall rules, the groups have to be assigned to a user group desktop object. For more information, see "User Groups" on page 106.

LDAP Users

It is possible to connect R&S Unified Firewalls to an external directory server using the Lightweight Directory Access Protocol (LDAP) to retrieve users from there. You can include these users in user-specific firewall rules.

LDAP can be used by medium to large companies to access directory services and to manage user data.

Connect to a directory server as described under "User Authentication Settings" on page 54.

Navigate to "Firewall > User Authentication > LDAP Users" to display the list of LDAP users that are currently defined on the directory server in the item list bar.

To make LDAP users in this list available for use in connections and user-specific firewall rules, the users must be assigned to a user desktop object. For more information, see "User Groups" on page 106.

Local Users

R&S Unified Firewalls offers local user administration for smaller companies without central administration. Use the "Local Users" settings to specify the usernames and passwords. This way, you can define and manage users.

Navigate to "Firewall > User Authentication > Local Users" to display the list of local users that are currently defined on the system in the item list bar.

In the expanded view, the table columns display the "Name" of the local user and a "Description", if one was entered. The buttons in the last column allow you to view and adjust the settings for an existing local user, create a new user based on a copy of an existing local user, or delete a user from the system.

For further information, see Chapter 3.2, "Icons and Buttons", on page 23.

Under "Firewall > User Authentication > Local Users", you can add a new or edit an existing local user.

The "Local User Authentication" panel allows you to configure the following elements:

Field	Description
"User Name"	Enter a unique name for the local user. This name will be the logon name. **Important:** The user's logon name has to exactly match the "User Name" (case-sensitive). Otherwise, the name in the user-specific firewall rules will not correspond to the user logging on to the client and the rules will not match.
"Description"	Optional: The information given here is for internal use for the administrator only.
"Password"	Enter a password for the user and confirm it. The password must consist of at least six characters.
"Show Password"	Optional: Select this checkbox to verify the password.
"Require password change after next login"	Optional: Select this checkbox if you want to require the user to change the password after the next logon. If selected, the web server will redirect the user from the logon page to a page for changing the password.

The buttons at the bottom right of the editor panel depend on whether you add a new local user or edit an existing user. For a newly configured local user, click "Create" to add the new user to the list of available local users or "Cancel" to reject the creation. To edit an existing local user, click "Save" to store the reconfigured user or "Reset" to discard your changes. You can click "Close" to shut the editor panel as long as no changes have been made on it.

The local users defined here are available for use in desktop objects, for example VPN users.

Unassigned Users

Navigate to "Firewall > User Authentication > Unassigned Users" to view LDAP users that are assigned to user desktop objects but who R&S Unified Firewalls is not able to retrieve where they used to be from the directory service.

Application Examples

Using a Windows domain

If you have a Windows domain, you can connect the user authentication to the Windows domain controller.

To connect the user authentication to the Windows domain controller, perform the following steps:

1. Navigate to "Firewall > User Authentication".
2. Click the "Authentication Server" tab.
3. Enter the data of your domain controller.

   All users in the specified domain appear on the user list.
4. Drag user icons onto the configuration desktop and assign rules to them.

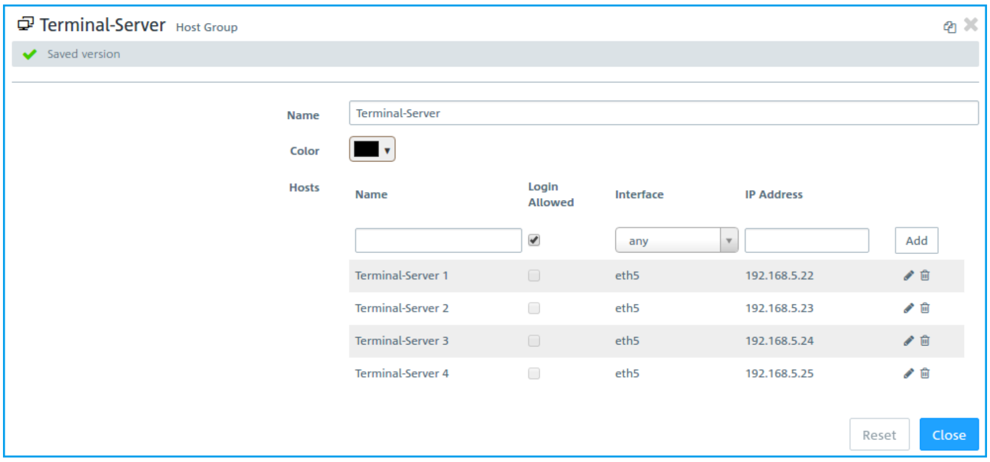
   To log on, users must enter the URL with `https://` and the IP address of the firewall in the address bar of their browser. A logon page appears. After a successful logon, the firewall rules for the user are assigned to the supplied IP address. When the browser window is closed, the session cookie expires and the rules lose their validity.

Excluding the Terminal Server from User Authentication

If you are using a terminal server, exclude it from the user authentication. Otherwise, after one user has logged on, all previous users are logged out.

To exclude the terminal server from the user authentication, perform the following steps:

1. Click the host group icon in the toolbar at the top of the desktop.
2. Clear the checkbox in the "Login Allowed" column.



Terminal-Server Host Group

✓ Saved version

Name: Terminal-Server

Color: ■ ▾

Hosts

Name	Login Allowed	Interface	IP Address	
	☑	any ▾		Add
Terminal-Server 1	□	eth5	192.168.5.22	
Terminal-Server 2	□	eth5	192.168.5.23	
Terminal-Server 3	□	eth5	192.168.5.24	
Terminal-Server 4	□	eth5	192.168.5.25	

Figure 3-10: Object settings – terminal server.

If your users do need authentication on the terminal server, you can activate Remote Desktop IP Virtualization on the terminal server. This way, all users are assigned their own IP address during a session.

3.4.2 Monitoring & Statistics

The "👁 Monitoring & Statistics" settings display detailed information about the traffic flowing through R&S Unified Firewalls and allow you to set up remote SNMP and syslog servers to forward log messages generated by different message sources. Furthermore, you can configure how to deal with the different kinds of events that R&S Unified Firewalls can detect and whether to create statistics for each of them or not.

3.4.2.1 Statistics Settings

Navigate to "Monitoring & Statistics > Settings" to customize the statistics.

The "Settings" panel allows you to configure how to deal with the different kinds of events that R&S Unified Firewalls can detect and whether to create statistics for each of them or not. From the drop-down lists, select one of the following options to deal with the various event types:

Mode	Description
Disabled	No data is collected for this event type.
Create Statistics	Data from occurring events is collected to create statistics.

Mode	Description
Send Raw Data to External Syslog	Data from occurring events is collected to create statistics and passed on to a configured external syslog server.
Save Raw Data Locally	Data from occurring events is collected to create statistics, passed on to a configured external syslog server and stored on the device. **Note:** This mode can cause the storage of the device to fill up rapidly.

Hover the mouse over the ❶ next to the event type label to find an explanation of what graph a particular event is used for. Use the "All Event Types" drop-down list to set all event types simultaneously to the same mode.

The buttons at the bottom right of the editor panel allow you to shut ("Close") the editor panel as long as no changes have been made and to store ("Save") or to discard ("Reset") your changes.

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

3.4.2.2 Connection Tracking

The "Connection Tracking" panel allows you to view and interact with the in-kernel connection tracking system to get a list of all active connections on R&S Unified Firewalls.

Navigate to "Monitoring & Statistics > Connection Tracking" to open an editor panel to display the list of connections that are currently tracked through the system.

The filter section allows you to narrow the list of results in the table below it. First, select one of the options in a drop-down list or type in one of the input fields. Then, click "Reload" to refresh the list to show only those entries that contain the selected option or the characters you have typed. Click ✖ in the drop-down list or ⊗ in the input field to delete the selected option or the search string or click "Reset Filter" to delete all entries and display an unfiltered view of the list.

The filter options are AND-connected.

The table columns of the currently active connections list contain the following information:

Column	Description
#	Displays a consecutive number for the table row.
"Protocol"	Displays the IP protocol type used by the connection. The type can be either TCP or UDP.
"TTL"	Displays how long (in seconds) the conntrack entry has to live. Once this time span has elapsed, the entry is discarded.

Column	Description
"TCP State"	Displays the current state of the TCP connection. The TCP state can be one of the following: ● SYN_SENT ● SYN_RECV ● ESTABLISHED ● FIN_WAIT ● CLOSE_WAIT ● LAST_ACK ● TIME_WAIT ● CLOSE ● LISTEN
"Source"	Displays the source IP address and port of the connection request.
"Destination"	Displays the destination IP address and port of the connection request.
"Packets"	Displays the number of packets sent in the original direction for the given connection. In this case, original direction means from source to destination.
"Bytes"	Displays the number of bytes sent in the original direction for the given connection. In this case, original direction means from source to destination.
"State"	Displays the state of the connection in the original direction. In this case, original direction means from source to destination.The state can be one of the following: ● ASSURED ● ESTABLISHED - This connection has been established. ● EXPECTED - This is an expected connection. That is, there have not yet been any matching packets, but the firewall expects such packets soon. ● FIXED_TIMEOUT ● INVALID - This connection does not follow the expected behavior of a connection and is, therefore, considered invalid. ● NEW - This connection is starting. ● RELATED - This connection has already been expected. ● SEEN_REPLY - The first answer packet from the destination was seen, but the handshake has not yet been completed. ● UNREPLIED - An initial packet from the source was seen, but it has not yet been replied. ● UNSET ● UNTRACKED - This connection is not tracked.

Column	Description
"State (Reply)"	Displays the state of the connection in the reply direction. In this case, reply direction means from destination to source.The state can be one of the following: ● `ASSURED` ● `ESTABLISHED` - This connection has been established. ● `EXPECTED` - This is an expected connection. That is, there have not yet been any matching packets, but the firewall expects such packets soon. ● `FIXED_TIMEOUT` ● `INVALID` - This connection does not follow the expected behavior of a connection and is, therefore, considered invalid. ● `NEW` - This connection is starting. ● `RELATED` - This connection has already been expected. ● `SEEN_REPLY` - The first answer packet from the source was seen, but the handshake has not yet been completed. ● `UNREPLIED` - An initial packet from the destination was seen, but it has not yet been replied. ● `UNSET` ● `UNTRACKED` - This connection is not tracked.
"Source (Reply)"	Displays the source IP address and port expected of the return packets (usually the same as under "Destination").
"Destination (Reply)"	Displays the destination IP address and port expected of the return packets (usually the same as under "Source").
"Packets (Reply)"	Displays the number of packets sent in the reply direction for the given connection. In this case, reply direction means from destination to source.
"Bytes (Reply)"	Displays the number of bytes sent in the reply direction for the given connection. In this case, reply direction means from destination to source.
"Mark"	Displays the connection mark. The mark is set by R&S Unified Firewalls.
"Used"	Displays the conntrack `Use` field.

Click "Reload" to refresh the connections list in the table.

The "Close" button at the bottom of the editor panel allows you to shut the panel and return to the complete overview of your entire configured network.

3.4.2.3 Logs

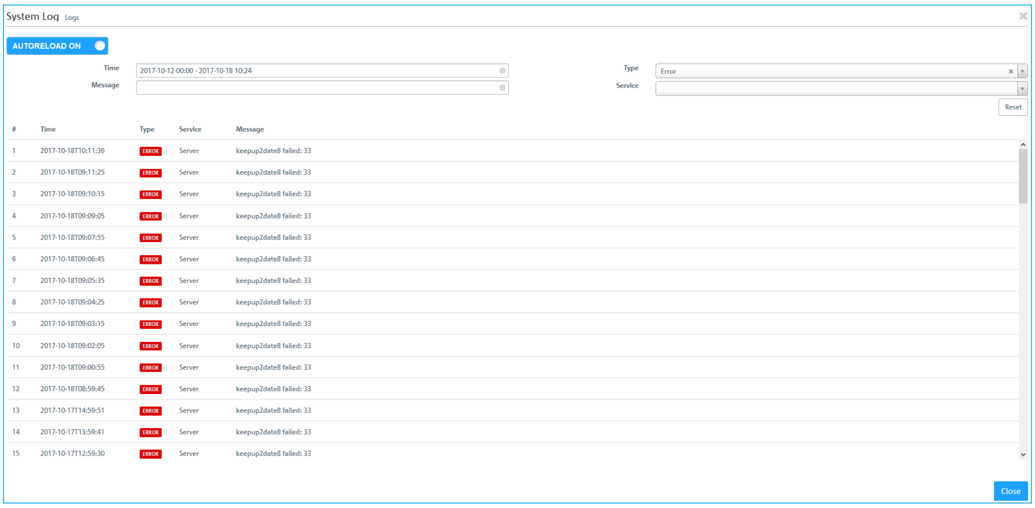
R&S Unified Firewalls stores records of system events, status information, errors and other communication in a log database. The "Logs" panels display the contents of the logs. If a problem occurs, you may be able to find technical details about the cause of the problem by viewing these logs.

The logs are automatically reloaded to get the latest entries by default. You can disable the automatic reload to focus on older entries by clicking the "AUTORELOAD ON" slider switch. Then you can manually update the list of items in the logs by clicking "Manual Reload". To enable automatic reload again, click the slider switch to turn it on.

The filter options above the tables allow you to narrow the list of results to display only items that include a certain search string. Toggle the options to specify search criteria in the input fields. The "Message" and "User" filters return all results that contain the input string, whereas the remaining filter fields return exact matches only. The available options depend on the log type. With filter options set, the logs are always automatically reloaded.

To filter the contents of a log by a customized time range, click the "Time" input field. A new window on which you can either select a predefined or enter a custom time range opens. By clicking "Custom", a calendar and drop-down lists for changing the date and time appear. Set the date and time as desired. Click "Apply" to save your changes and view the filtered log or "Cancel" to discard your changes.

To view the complete logs again, delete all search criteria by clicking "Reset", the ✖ button on the right side of a selected drop-down list entry or the ⊗ button in the input fields.



System Log Logs

AUTORELOAD ON

Time: 2017-10-12 00:00 - 2017-10-18 10:24

Message:

Type: Error

Service:

#	Time	Type	Service	Message
1	2017-10-18T10:11:36	ERROR	Server	keepup2date8 failed: 33
2	2017-10-18T09:11:25	ERROR	Server	keepup2date8 failed: 33
3	2017-10-18T09:10:15	ERROR	Server	keepup2date8 failed: 33
4	2017-10-18T09:09:05	ERROR	Server	keepup2date8 failed: 33
5	2017-10-18T09:07:55	ERROR	Server	keepup2date8 failed: 33
6	2017-10-18T09:06:45	ERROR	Server	keepup2date8 failed: 33
7	2017-10-18T09:05:35	ERROR	Server	keepup2date8 failed: 33
8	2017-10-18T09:04:25	ERROR	Server	keepup2date8 failed: 33
9	2017-10-18T09:03:15	ERROR	Server	keepup2date8 failed: 33
10	2017-10-18T09:02:05	ERROR	Server	keepup2date8 failed: 33
11	2017-10-18T09:00:55	ERROR	Server	keepup2date8 failed: 33
12	2017-10-18T08:59:45	ERROR	Server	keepup2date8 failed: 33
13	2017-10-17T14:59:51	ERROR	Server	keepup2date8 failed: 33
14	2017-10-17T13:59:41	ERROR	Server	keepup2date8 failed: 33
15	2017-10-17T12:59:30	ERROR	Server	keepup2date8 failed: 33

Figure 3-11: Sample filtered system log.

The "Close" button at the bottom of the log panels allows you to shut the log panels and return to the complete overview of your entire configured network.

For more detailed information on the different types of logs, see the following sections.

Audit Log

The "Audit Log" provides a journal of every configuration change made to R&S Unified Firewalls (e.g. update VPN settings) or action performed by it (e.g. import a backup) and who it was triggered by. The "Monitoring" right is required to view the log. For further information on web client permissions, see "Administrators Settings" on page 28.

The columns of the table contain the following information:

Column	Description
"Time"	The timestamp of the log entry.
"Action"	The action type which can be one of the following: ● `Call` – perform a special operation (e.g. import a backup) ● `Delete` – delete a configuration item (e.g. delete an obsolete IPsec connection) ● `Insert` – insert a new configuration item (e.g. insert a host group) ● `Update` – change a configuration item (e.g. adjust the antivirus settings)
"User"	The name of the user that created the entry, such as `admin`.
"Message"	The log message itself. The content of the message depends on the "Action" type selected: ● If the "Action" is `Call`, then the "Message" starts with the API endpoint that was called. ● If the "Action" is `Delete`, then the "Message" states the name and internal type of the configuration item that was removed. ● If the "Action" is `Insert`, then the "Message" states the name and internal type of the created configuration item. It also shows the full payload of the message used to create the configuration item, showing the specific settings that were used. ● If the "Action" is `Update`, then the "Message" states the name and internal type of the changed configuration item. It also lists the specific changes that were made to a specific path (displayed in italics). The path identifies the actual setting of a configuration item that was altered.

System Log

The "System Log" displays a list of recent system messages.

The columns of the table contain the following information:

Column	Description
"Time"	The timestamp of the log entry.
"Type"	The message type which can be one of the following: ● `OK` – the service is working correctly ● `Error` – an error occured and an error message is displayed

Column	Description
"Service"	The name of the service that created the entry. Possible filters are: ● `Server` – firewall services, including kernel, DHCP server, DNS server, SNMP server and WLAN access point messages ● `VPN` – IPSec and SSL tunnels ● `Internet` – NTP, DynDNS and DSL connection status ● `User` – terminal login, SSH login and superuser privilege operations (sudo) ● `Connections` – connections that were successfully finished. These messages will only be stored if Connection Finished in the "Monitoring & Statistics > Settings" is set to Save Raw Data Locally. ● `Proxy` – messages regarding web and mail proxies ● `Updates` – all messages regarding the firewall software ● `Appfilter` – application filter messages ● `IDPS` – IDS/IPS messages ● `Alerts` – all security relevant alerts, irrespective of the generating engine (e.g. when the anti-malware engine detects a virus or when the IDS/IPS engine detects a thread) **Note:** Alerts will only be shown in the `Alerts` category, even if they also belong to another category. **Example:** `Appfilter` generates an alert. The alert will only be shown in `Alerts`, but not in `Appfilter`.
"Message"	The log message itself. Select `Alerts` in the "Service" column to filter IDS/IPS log messages. **Tip:** You can use the log messages to add an IDS/IPS rule to the list of ignored rules on the "Rules" tab of the "IDS/IPS" editor panel. Click ⚙ in the respective IDS/IPS log message. A drop-down list opens. Select the "Ignore rule" entry. The IDS/IPS rule is automatically added to the list of ignored rules on the "Rules" tab of the "IDS/IPS" editor panel. For further information, see Chapter 3.4.5.4, "IDS/IPS", on page 126.

3.4.2.4 SNMP Settings

SNMP (Simple Network Management Protocol) is a networking protocol that is used to offer and receive status information across a network. The participants of the SNMP based information exchange are the SNMP manager (e.g. Nagios) and the SNMP clients (devices such as your R&S Unified Firewalls that are meant to be monitored by the SNMP manager).

While the SNMP manager requests, receives and monitors information, the SNMP clients respond to information requests (e.g. "What is the current CPU load/memory usage of the device?"). Status information offered by managed devices is organized like a tree (the so-called Management Information Base, short *MIB*), with each leaf being a retrievable piece of information. Every single leave can be addressed and requested individually via its own unique numeric address. A file containing a mapping of these numeric address snippets to meaningful names, and thereby a declaration of all information available on a managed device, can be provided to the SNMP manager to increase human usability (e.g. `29577.1.1` represents `RSCS.SystemLoad.cpuLoad`).

The "SNMP Settings" allow you to configure the following elements:

Field	Description
I/○	A slider switch indicates whether SNMP is active (I) or inactive (○). By clicking the slider switch, you can toggle the state individually. SNMP is deactivated by default.
"Listening IP"	Optional: Enter a local IP address on which the service will be listening. If you retain the pre-defined default IP address `0.0.0.0`, requests will be accepted on all IP addresses.
"Listening Port"	Optional: Specify the port number on which the service will be listening. Port number `161` is pre-defined by default.
"Protocol Version"	From the drop-down list, select the version of the SNMP protocol to be used. Depending on the version selected, additional options become available. Version `v2c` is pre-selected by default.
"Community String"	Only available if the selected "Protocol Version" is `v2c`: Enter the pre-shared key that every SNMP manager/client has to use to authenticate to the SNMP service of the access zone.
"Show Community String"	Optional and only available if the selected "Protocol Version" is `v2c`: Select this checkbox to verify the pre-shared key.
"Username"	Only available if the selected "Protocol Version" is `v3`: Enter the username that every SNMP manager/client software has to use to identify to the SNMP service of the access zone. **Note:** The username is created and used by the SNMP service internally.
"Authentication Protocol"	Only available if the selected "Protocol Version" is `v3`: From the drop-down list, select the hashing algorithm that is used for authentication purposes. You can choose between the settings `No Authentication`, `MD5` and `SHA`.
"Authentication Password"	Only available if the selected "Protocol Version" is `v3` and the selected "Authentication Protocol" is `MD5` or `SHA`: Enter the password to be used for authentication. The password must consist of at least eight characters.
"Show Authentication Password"	Optional and only available if the selected "Protocol Version" is `v3` and the selected "Authentication Protocol" is `MD5` or `SHA`: Select this checkbox to verify the authentication password.
"Privacy Protocol"	Optional and only available if the selected "Protocol Version" is `v3` and the selected "Authentication Protocol" is `MD5` or `SHA`: From the drop-down list, select the algorithm to be used to encrypt the communication with the SNMP service. You can choose between the encryption algorithms `3DES` and `AES`. The option is set to `No Encryption` by default.
"Privacy Password"	Only available if the selected "Protocol Version" is `v3`, the selected "Authentication Protocol" is `MD5` or `SHA` and the selected "Privacy Protocol" is `3DES` or `AES`: Enter the password to be used to encrypt the communication with the SNMP service using the selected encryption algorithm.
"Show Privacy Password"	Optional and only available if the selected "Protocol Version" is `v3`, the selected "Authentication Protocol" is `MD5` or `SHA` and the selected "Privacy Protocol" is `3DES` or `AES`: Select this checkbox to verify the privacy password.
"Location"	Optional: Enter a fixed value which R&S Unified Firewalls returns for requests to certain Object Identifiers (OIDs) of the standard Management Information Base (MIB): `sysLocation`.
"Contact"	Optional: Enter a fixed value which R&S Unified Firewalls returns for requests to certain Object Identifiers (OIDs) of the standard Management Information Base (MIB): `sysContact`.

The buttons at the bottom right of the editor panel allow you to shut ("Close") the editor panel as long as no changes have been made and to store ("Save") or to discard ("Reset") your changes.

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

3.4.2.5 Statistics

The "Statistics" panels contain charts and tables. You can control several aspects of the presentation and data on these statistics.

The "Statistics" right is required to access the statistics and configure the settings related to them. For further information on web client permissions, see "Administrators Settings" on page 28.

When analyzing the statistics and configuring the settings related to them, the administrator must comply with data security regulations.

There are two ways to access the individual statistics panels:

- You can use the links in the navigation bar to navigate to the detailed statistics panels, e.g. via "Monitoring & Statistics > Statistics > Blocked Connections".
- You can click the "Details" link in the top right corner of one of the chart panels on the "Statistics" overview. The link forwards you to the detailed statistics panel for that chart. For further information, see "Overview" on page 71.

Working with statistics

There are two kinds of statistics:

- Counters are displayed as line charts on the "Blocked Connections" and "Blocked Content" statistics panels, each of them containing multiple counters.
- Toplists provide a ranking for different events types and are displayed as a pie chart or an area chart, depending on the selected data period. Data for the `Day` period is displayed as a pie chart, while data for `Month` and `Year` is displayed as a stacked area chart.

A tabular display of the graphical data complements each statistics panel. In the case of counters, the data table always displays the same data as the chart. Each statistics element creates a column in the data table. In the case of toplists, the data table displays the values of the statistics elements.

The charts and tables in the statistics panels share common functions to adjust the data display and allow you to focus on the data you are most interested in:

- Under "Period" in the header area of the statistics panels, you can set the desired temporal scope of the data to be displayed. Use the buttons to toggle between the different data periods available. You can choose between `Day`, `Month` and `Year`. The option is set to `Day` by default.
- Toplists typically contain an input field in the header area of the panels. Use the "Entries" field to adjust the maximum number of items to be displayed in the chart.

The option is set to 5 entries by default. You can enter a different value or use the up and down arrows in the input field to change the value.
Note: Regardless of the value set for the chart, the data table always displays up to 1000 entries.

- The charts and tables can be collapsed and expanded by clicking the corresponding icon in the header area of a chart or table, e.g. giving more space to the table or hiding unnecessary details. For further information, see Chapter 3.2, "Icons and Buttons", on page 23.
- Click ☰ in the top right corner of a chart to access various export options (print view, PNG, JPEG, SVG, PDF, CSV and XLS) for the data displayed in the chart.
Note: If you use the spreadsheet export function available for the toplist charts, only the data used by that chart is exported, taking into account the value you have selected for the maximum number of toplist items.
- Line and area charts include a legend. The legend is color-coded and can be used as a filter for the chart. Click items in the legend below the chart to activate and deactivate them in the chart. If clicking has no effect and the legend item remains gray, data collection for the underlying event type was disabled in the statistics settings and, therefore, no data is available. For further information, see Chapter 3.4.2.1, "Statistics Settings", on page 61.
- Tooltips provide details on specific points in the graphical statistics. Hover the cursor of your mouse over the chart to see the exact values for a specific point in time.

The sections below provide further information on the data available in the statistics overview, on each detailed statistics panel and on the settings.

Blocked Connections

The "Blocked Connections" panel can display the following statistics:

Statistics Element (Event Type)	Description
"Rule Set Inbound" ("Blocked Inbound Traffic")	Number of connections blocked because of input rules
"Rule Set Outbound/Forward" ("Blocked Forwarded Traffic")	Number of connections blocked because of forwarding rules
"IPS/IDS" ("IDPS Alert")	Number of IDS/IPS alerts. If the IDS/IPS mode is set to "IDS", "IPS Drop" or "IPS Reject", then this statistics element displays the number of dropped packets. For further information, see Chapter 3.4.5.4, "IDS/IPS", on page 126.

Blocked Content

The "Blocked Content" panel can display the following statistics:

Statistics Element (Event Type)	Description
"Virus (Mail)" ("Malware Alert (Mail)")	Number of viruses detected in emails
"Virus (Other)" ("Malware Alert (HTTP and FTP)")	Number of viruses detected in HTTP or FTP traffic
"Spam" ("Spam Alert")	Number of spam emails detected

Statistics Element (Event Type)	Description
"Web Access" ("Web Content Blocked")	Web access blocked by content filter
"Appfilter" ("Appfilter Alert")	Number of alerts regarding blocked application-specific traffic

Overview

Navigate to "Monitoring & Statistics > Statistics > Overview" to view a summary of all available statistics charts. It can be considered a dashboard for "Statistics" and is intended to provide an initial answer to the most common questions regarding the events that R&S Unified Firewalls can detect.

The following special features apply only to this panel (diverging from the description of the individual statistics panels in "Working with statistics" on page 69):

- Under "Period" in the header area of the overview panel, you can select the desired temporal scope of the data to be displayed in all charts.
- You can click the "Details" link in the top right corner of an individual chart panel to be forwarded to the detailed statistics panel for the respective chart.
- The number of entries for toplist charts is set to a fixed value of `5`.

Top Domains Accessed

The "Top Domains Accessed" panel displays the Internet sites that were most frequently visited by users on the local network if you allow R&S Unified Firewalls to collect this kind of data by enabling the "Web Content Allowed" event type. These statistics are used to determine whether web-browsing habits match the company policy and the goals of the business.

Top Domains Blocked

The "Top Domains Blocked" panel displays the Internet sites that were most frequently blocked if you allow R&S Unified Firewalls to collect this kind of data by enabling the "Web Content Blocked" event type.

Top Traffic per Source

The "Top Traffic per Source" panel shows the traffic volume for the top data traffic sources if you allow R&S Unified Firewalls to collect this kind of data by enabling the "Connection Finished" event type.

3.4.2.6 Syslog Servers

R&S Unified Firewalls can be used to configure multiple external syslog servers to forward log messages generated by different message sources for reporting purposes.

Syslog messages are sent in cleartext (not encrypted) usually via port number 514 and either via the User Datagram Protocol (UDP) or the Transmission Control Protocol (TCP) to the remote syslog server.

For more detailed information on external syslog servers, see the following sections.

Syslog Servers Overview

Navigate to "Monitoring & Statistics > Syslog Servers" to display the list of remote syslog servers that are currently defined on the system in the item list bar.

In the expanded view, the table displays the server address of the external syslog server which consists of the IP address and the port. For example, the server address `192.168.124.5:514` represents the IP address `192.168.124.5` and the port number `514`. Furthermore, the "Protocol" type used for the transmission of the text message is displayed. The buttons in the last column allow you to view and adjust the settings for an existing external syslog server, create a syslog server based on a copy of an existing external syslog server or delete a remote syslog server from the system.

For further information, see Chapter 3.2, "Icons and Buttons", on page 23.

Syslog Servers Settings

The "Syslog Servers" settings allow you to specify connection details for multiple remote syslog servers to forward log messages generated by different message sources.

Under "Monitoring & Statistics > Syslog Servers", you can add a new or edit an existing remote syslog server.

The "Syslog Servers" settings allow you to configure the following elements:

Field	Description
"Destination IP"	Enter the IP address of the server.
"Destination Port"	Specify the port number to be used by entering an integer value.
"Transport Protocol"	Select the protocol type to be used from the drop-down list.

The buttons at the bottom right of the editor panel depend on whether you add a new remote syslog server or edit an existing server. For a newly configured server, click "Create" to add the server to the list of available remote syslog servers or "Cancel" to discard your changes. To edit an existing server, click "Save" to store the reconfigured server or "Reset" to discard your changes. You can click "Close" to shut the editor panel as long as no changes have been made on it.

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

3.4.3 Network

The "🖧 Network" settings allow you to organize your network by configuring interfaces, connections, WLAN, routing policies and DHCP settings. Furthermore, you can to set up the WAN access of your R&S Unified Firewalls by configuring DNS settings, DynDNS accounts and QoS settings.

3.4.3.1 Connections

The "Desktop Connections" settings allow you to configure network and PPP connections on R&S Unified Firewalls.

Network Connections

Use the "Network Connections" settings to configure network connections. The system offers default connections for all available Ethernet interfaces.

For more detailed information on network connections, see the following sections.

Network Connections Overview

Navigate to "Network > Connections > Network Connections" to display the list of network connections that are currently defined on the system in the item list bar.

In the expanded view, the first column of the table displays the "Name" of the network connection. The "Status" column shows one of the following status indicators:

- Green – The network connection is enabled.
- Gray – The network connection is disabled.
- Red – The network connection is disconnected.

Furthermore, the "Interface" that the network connection is assigned to and the connection "Type" are displayed. The buttons in the last column allow you to view and adjust the settings for an existing network connection, create a new connection based on a copy of an existing network connection or delete a network connection from the system.

For further information, see Chapter 3.2, "Icons and Buttons", on page 23.

Network Connections Settings

Use the "Network Connections" settings to configure custom network connections.

Under "Network > Connections > Network Connections", you can add a new or edit an existing network connection.

The "Network Connection" panel displays the following information and allows you to configure the following elements:

Field	Description
I/○	A slider switch indicates whether the network connection is active (I) or inactive (○). By clicking the slider switch, you can toggle the state of the connection. A new network connection is enabled by default.
"Name"	Enter a name for the network connection. **Note:** If you leave this field empty, the name will be generated automatically from the selected interface and the connection type.
"Interface"	From the drop-down list, select the interface that you want to assign to the connection. You may select an Ethernet, VLAN or bridge interface.

Field	Description
"Type"	From the drop-down list, select the connection type. This option is set to `Static` by default, but you can adjust the settings to the other value as required: ● `Static` – This mode is used to specify a fixed IP address for the connection. ● `DHCP` – This mode is used to assign IP addresses dynamically. **Note:** Once you click "Create" to establish the network connection, you will no longer be able to change the connection type. **Tip:** The elements on the "Network" tab described below differ depending on the selected connection type.
"Used by"	Displays the components that use the network connection.
"Status"	Displays the status of the network connection. The status can be one of the following: ● `up` – The network connection is enabled. ● `disabled` – The network connection is disabled. ● `disconnected` – The network connection is disconnected.

On the "Network" tab:

Field	Description
"IP Addresses"	Assign one or multiple IP addresses to the network connection. Enter an IP address in CIDR notation (IP address followed by a slash »/« and the number of bits set in the subnet mask, for example `192.168.50.1/24`). Click "Add" to add the IP address to the list. You can edit or delete single entries in the list by clicking the corresponding button next to an entry. For further information, see Chapter 3.2, "Icons and Buttons", on page 23. **Note:** If you edit an IP address, a check mark appears on the right of the entry. Click the check mark to be able to save the settings of the IP address. Click ▲/▼ to change the order of the IP addresses in the list. **Note:** The IP address which is listed first in the list is used as the default source IP address for NAT and for IPsec connections.
"Obtain Gateway"	Only available if the selected connection "Type" is `DHCP`: Select this checkbox if you want R&S Unified Firewalls to obtain a gateway for the connection from the DHCP server.
"Obtain DNS Server"	Only available if the selected connection "Type" is `DHCP`: Select this checkbox if you want R&S Unified Firewalls to obtain a DNS server for the connection.
"Obtain Domain"	Only available if the selected connection "Type" is `DHCP`: Select this checkbox if you want R&S Unified Firewalls to obtain a domain for the connection from the DHCP server.
"Obtained via DHCP"	Only available if the selected connection "Type" is `DHCP`: Displays one of the following states: ● If the connection is working, the IP address is displayed. ● `Connection not yet saved` – A new connection is being created. ● `Failed` – The DHCP connection could not be established.

On the "WAN" tab:

Field	Description
"Set Default Gateway"	Only available if the selected connection "Type" is `Static`: Select this checkbox if you want to set a default gateway for the network connection. **Note:** If you select `DHCP` as the connection "Type", this checkbox is always enabled and grayed out because the gateway is obtained from the DHCP server.
"Default Gateway"	Only available if the selected connection "Type" is `Static`: Enter the default gateway for this connection. **Note:** If you select `DHCP` as the connection "Type", this input field is grayed out and displays the gateway which is obtained from the DHCP server.
"Time Restrictions"	Optional: Select this checkbox if you want to set a time limit for which the connection is enabled. Click "Edit" to open the "Time Restriction" editor panel which provides the following options: ● Set specific times and weekdays using the sliders. ● "Always On" – The connection is always enabled. ● "Always Off" – The connection is always disabled. The buttons at the bottom right of the editor panel allow you to confirm your changes to the time restrictions ("OK") and to discard your changes ("Cancel"). The editor panel closes and the chosen option is displayed on the left of the "Edit" button: `Restricted.`, `Always On.` or `Always Off.`.
"Multi WAN Weight"	Specify how much of the Internet traffic is routed through this connection by entering a value from `1` to `256`. The higher the set value, the higher the percentage of Internet traffic routed through the connection. Setting the same value for all connections results in equal traffic distribution across all connections.
"Desktop Object"	From the drop-down list, select an Internet object that is used in firewall rules for this WAN connection. For further information, see "Internet Objects" on page 104.

On the "Failover" tab:

Field	Description
"Heartbeats"	Specify how the state of the connection is to be tested by adding tests. The default settings contain a ping test of the Google server (8.8.8.8). Click "Add" to add another test to the list. For information on configuring the reachability test, see "Heartbeat Settings" on page 76. You can edit or delete single entries in the list by clicking the corresponding button next to an entry. For further information, see Chapter 3.2, "Icons and Buttons", on page 23.
"Use as backup connection"	Optional: Select this checkbox if you want to configure the connection as a backup Internet connection.
"Backup connections"	Select any backup connection you wish to assign to the connection and specify its "Priority". If the current connection fails, R&S Unified Firewalls switches to the available backup connection with the highest priority. Click "Add" to add the backup connection to the list. You can edit or delete single entries in the list by clicking the corresponding button next to an entry. For further information, see Chapter 3.2, "Icons and Buttons", on page 23. **Note:** If you edit a backup connection, a check mark appears on the right of the entry. Click the check mark to be able to save the settings of the backup connection.

The buttons at the bottom right of the editor panel depend on whether you add a new network connection or edit an existing connection. For a newly configured network connection, click "Create" to add the connection to the list of available network connections or "Cancel" to reject the creation of a new network connection. To edit an existing network connection, click "Save" to store the reconfigured connection or "Reset" to discard your changes. You can click "Close" to shut the editor panel as long as no changes have been made on it.

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

Heartbeat Settings

Use the "Heartbeat" editor panel to set up automatic heartbeat tests to check the state of the connection. The panel allows you to configure the following elements:

Field	Description
"Type"	From the drop-down list, select the type of reachability test you want to run: ● `ping` – This mode sends ping signals to the target. ● `tcp_probe` – This mode tests the capacity of a TCP connection.
"Timeout"	Specify the timeout (in seconds) for the test.
"Number of tries"	Set the overall number of tries to be performed.
"Number of successful tries"	Set the number of successful tries required for a successful heartbeat.
"Arguments"	Specify the arguments to be used in the test, e.g. IP addresses that will be pinged.

If you have defined a backup Internet connection on the "Failover" tab and the automatic heartbeat test defines the state of the connection as `disconnected`, R&S Unified Firewalls automatically switches to the backup connection with the highest priority available.

The buttons at the bottom of the "Heartbeat" editor panel allow you to discard your changes to the heartbeat test ("Reset") and to run the connection test manually ("Test"). Furthermore, you can reject ("Cancel") or confirm your changes ("OK") to the test, close the editor panel and return to the "Network Connection" editor panel. The specified test is displayed as an entry in the list under "Heartbeats" on the "Failover" tab.

PPP Connections

Use the "PPP Connections" settings to configure existing connections using the Point-to-Point Protocol and to add new ones.

For more detailed information on PPP connections, see the following sections.

PPP Connections Overview

Navigate to "Network > Connections > PPP Connections" to display the list of PPP connections that are currently defined on the system in the item list bar.

In the expanded view, the columns of the table display the "Name" of the connection, whether it is "Active" or not, its "Interface", and the "Type" of connection. The buttons in the last column allow you to view and adjust the settings for an existing PPP connection, create a new connection based on a copy of an existing connection or delete a PPP connection from the system.

For further information, see Chapter 3.2, "Icons and Buttons", on page 23.

PPP Connections Settings

Under "Network > Connections > PPP Connections", you can add a new or edit an existing network connection.

The "PPP Connections" settings contain the following elements:

Field	Description
I/○	A slider switch indicates whether the PPP connection is active (I) or inactive (○). By clicking the slider switch, you can toggle the state of the connection. A new PPP connection is enabled by default.
"Name"	Specify the name of the network connection. If you leave this field empty, the name will be generated automatically from the selected interface and the connection type.
"Interface"	Assign an interface to the connection. You may only select a PPP interface that has not yet been used in another connection.

Field	Description
"Type"	Select the connection type from the drop-down list, depending on your Internet service provider: `PPPoE` or `PPTP`. Use the `PPPoE` mode to connect using the Point-to-Point Protocol over Ethernet. PPPoE is typically used to share a broadband connection, such as a single DSL line or cable modem. Use the `PPTP` mode to connect using the Point-to-Point Tunneling Protocol. **Note:** Once you click "Create" to establish the PPP connection, you will no longer be able to change the connection type. **Tip:** The elements on the "Configuration" tab differ depending on the selected connection type.
"Used by"	Displays the components that use the PPP connection.
"Status"	Displays the status (`up`, `disconnected` or `disabled`) of the connection.

On the "Configuration" tab:

Field	Description
"Auth. Method"	Select an authentication method for the connection, depending on your Internet service provider: ● `None` ● `auto` - Automatically selects the authentication method which best matches the Internet service provider. ● `pap-only` - password authentication ● `chap-only` - handshake authentication ● `ms-chap2` - handshake authentication for Microsoft
"Username"	Enter the username required to connect to your Internet service provider.
"Password"	Enter the password required to connect to your Internet service provider.
"PPTP Server IP"	If you chose PPTP as connection type, enter the IP address of the PPTP server.
"MPPE"	If you chose PPTP as connection type, select the Microsoft Point-to-Point Encryption key length: ● `mppe-40` ● `mppe-56` ● `mppe-128`
"Local IP"	Optional: Enter your local IP address only if your Internet service provider explicitly requires this.
"Remote IP"	Optional: Enter the remote IP address only if your Internet service provider explicitly requires this.
"AC Hardware Address"	Optional: Enter the hardware MAC address of the Access Concentrator used by your Internet service provider. Only do so if your Internet service provider explicitly requires this.
"Force disconnect"	Optional: Select this checkbox if you wish to enforce a disconnect process at a specified time. Enter the time in the `HH:MM:SS` format. Some Internet service providers force a disconnect at specific intervals (usually every 24 hours). With this setting enabled, R&S Unified Firewalls disconnects at a specific time thereby preventing the auto-disconnect from the Internet service provider. This allows you to control when the disconnect happens.

On the "WAN" tab:

Field	Description
"Time Restrictions"	Select this checkbox if you want to set a time limit for which the connection is enabled. Click "Edit" to open the "Time Restrictions" editor panel that provides the following options: ● Set specific times and weekdays using the sliders. ● "Always On" - The connection is always enabled. ● "Always Off" - The connection is always disabled.
"Multi WAN Weight"	Specify how much of the Internet traffic is routed through this connection by entering a value from `1` to `256`. The higher the set value, the higher the percentage of Internet traffic routed through the connection. Setting the same value for all connections results in equal traffic distribution across all connections.
"Desktop Object"	Select an Internet object that is used in firewall rules for this connection. For further information, see "Internet Objects" on page 104.

On the "Failover" tab:

Field	Description
"Heartbeats"	Specify how the reachability of the connection is to be tested by adding ping tests. The default settings contain a ping test of the Google server (8.8.8.8). Click "Add" to add another test to the list. For information on how to configure the reachability test, see "Heartbeat Settings" on page 79. You can edit or delete single entries in the list by clicking the corresponding button next to an entry. For further information, see Chapter 3.2, "Icons and Buttons", on page 23.
"Use as backup connection"	Select this checkbox if you want to configure the connection as a backup Internet connection.
"Backup connections"	Select any backup connection you wish to assign to the connection and specify their "Priority". If the current connection fails, R&S Unified Firewalls switches to the available backup connection with the highest priority. Click "Add" to add the backup connection to the list. You can edit or delete single entries in the list by clicking the corresponding button next to an entry. For further information, see Chapter 3.2, "Icons and Buttons", on page 23.

Heartbeat Settings

The "Heartbeats" settings allow you to configure automatic heartbeat tests to test the connection. The editor panel contains the following elements:

Field	Description
"Type"	Select the type of reachability test you want to run: ● `ping` - Sends ping signals to the target. ● `tcp_probe` - Tests the capacity of a TCP connection.
"Timeout"	Specify the timeout (in seconds) for the test.
"Number of tries"	Set the overall number of tries to be performed.

Field	Description
"Number of successful tries"	Set the number of successful tries required for a successful heartbeat.
"Arguments"	Specify the arguments to be used in the test, e.g. IP addresses that will be pinged.

Click "Test" to run the connection test manually. Click "OK" to save the settings and return to the "Network Connection" settings panel.

The buttons at the bottom right of the editor panel depend on whether you add a new PPP connection or edit an existing connection. For a newly configured PPP connection, click "Create" to add the connection to the list of available PPP connections or "Cancel" to discard your changes. To edit an existing PPP connection, click "Save" to store the reconfigured connection or "Reset" to discard your changes. You can click "Close" to shut the editor panel as long as no changes have been made on it.

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

3.4.3.2 DHCP Settings

Navigate to "Network > DHCP Settings" to configure the DHCP settings on R&S Unified Firewalls.

Field	Description
I/○	A slider switch indicates whether the DHCP settings are enabled (I) or disabled (○). By clicking the slider switch, you can toggle the state.
"Operation Mode"	Select if you want to set up a DHCP server or a DHCP relay. The remaining fields on the screen depend on the chosen operation mode.

DHCP Server Settings

With the DHCP server running on R&S Unified Firewalls, you can assign IP addresses and transfer them to other configuration parameters (gateway, DNS server, NTP server etc.). Alternatively, it is possible to forward DHCP requests to an existing DHCP server on another network.

Configure the following elements for the DHCP server:

Field	Description
"Default Lease Time"	Enter the default lease time (in seconds) to determine the amount of time that the IP address of a computer is valid.
"Maximum Lease Time"	Enter the maximum lease time (in seconds).
"Prevent IP Conflicts"	Select this checkbox to have the DHCP server ping an IP address to verify that it is not yet in use before assigning it to a new client.
"Interfaces"	This table displays all interfaces (Ethernet, VLAN and bridge) on which a static connection has been configured and their DHCP settings. Click ✎ to open the "DHCP Settings" editor panel for the respective interface.

The "DHCP Settings" editor panel of an interface allows you to configure the following elements:

Field	Description
I/○	A slider switch indicates whether the DHCP server is active (I) or inactive (○) on this interface. By clicking the slider switch, you can toggle the state of the DHCP server on this interface.

On the "General" tab:

Field	Description
"Network"	From the drop-down list, select the subnet whose IP addresses are distributed by the DHCP server. By selecting the subnet, the "Range Start IP" and the "Range End IP" input fields are automatically prefilled with the respective IP range.
"Range Start IP"	If the prefilled start IP address does not meet your requirements, adjust the entry to specify the range of IP addresses that are distributed to the client computers.
"Range End IP"	If the prefilled end IP address does not meet your requirements, adjust the entry to specify the range of IP addresses that are distributed to the client computers. **Note:** Make sure that the permanent IP addresses are not within the IP address range of the DHCP server as permanent IP addresses are not excluded automatically during dynamic address assignment. Otherwise, addresses may be assigned twice.
"Lease Time"	Specify the time (in minutes) that the IP address of a computer is valid. The default lease time is `60` minutes.
"Gateway"	If the prefilled gateway IP address to be pushed to the client does not meet your requirements, adjust the entry. The default gateway IP address is usually the IP address of your R&S Unified Firewalls.
"WINS server"	Optional: If there is a WINS server in the network, use this input field to communicate it to the clients.
"Preferred NTP server"/"Alternative NTP server"	Optional: Clients may use NTP servers to determine the exact time. This is particularly important for user authentication via Windows servers.
"Preferred DNS server"/"Alternative DNS server"	If R&S Unified Firewalls does not carry out name resolution, enter internal DNS servers that are located in the network or the Internet. Otherwise, the clients are allocated the IP address of R&S Unified Firewalls as their DNS server.
"DNS Search Domains"	Specify a DNS search domain that the DNS service uses to resolve hostnames that are not fully qualified domain names. Click ⊕ to add the DNS search domain to the list. You can edit or delete single entries in the list by clicking the corresponding button next to an entry. For further information, see Chapter 3.2, "Icons and Buttons", on page 23. **Note:** If you edit an entry, a check mark appears on the right of the entry. Click the check mark to apply your changes.

On the "Static IP Addresses" tab:

Field	Description
"MAC Address"/"IP Address"/"Host Name"	Specify a static IP address for a host in the network by entering the host's MAC address and IP address. Aditionally, you can enter the host name. Click "Add" to add the static IP address to the list. You can edit or delete single entries in the list by clicking the corresponding button next to an entry. For further information, see Chapter 3.2, "Icons and Buttons", on page 23. **Note:** If you edit an entry, a check mark appears on the right of the entry. Click the check mark to apply your changes.
"Add from ARP Cache"	From the drop-down list, select the addresses you want to add from the ARP cache.

Click "OK" to save the interface settings and return to the "DHCP Settings" panel.

DHCP Relay Settings

A DHCP relay redirects incoming requests to a DHCP server to another network as DHCP requests cannot be routed.

Field	Description
"DHCP Server IP Address"	Enter the IP address of the server to which the DHCP requests will be redirected.
"Relay through these interfaces"	Select one or more interfaces from which DHCP requests will be forwarded. Also, select the interface that the DHCP server is connected to.

The buttons at the bottom right of the editor panel allow you to shut ("Close") the editor panel as long as no changes have been made and to store ("Save") or to discard ("Reset") your changes.

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

3.4.3.3 DNS Settings

Navigate to "Network > DNS Settings" to configure the DNS settings of your R&S Unified Firewalls.

Usually, the DNS server settings are provided by the WAN connection. You should have to configure the DNS server settings only if you cannot obtain them over the WAN connection.

The "DNS Settings" panel allows you to configure the following elements:

Field	Description
"Acquire DNS server"	Select this checkbox to connect to a DNS server selected by the router or the provider. **Note:** In case you are using several Internet lines from different providers, make sure that the DNS servers you use can be reached from all lines. If necessary, use public DNS servers on the Internet.
"Nameserver"	Specify an alternative DNS server by entering its IP address.

The buttons at the bottom right of the editor panel allow you to shut ("Close") the editor panel as long as no changes have been made and to store ("Save") or to discard ("Reset") your changes.

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

3.4.3.4 DynDNS Accounts

To be able to connect to your R&S Unified Firewalls from the external network, for example using a VPN connection, the IP address of your device has to be recognized on the Internet. Using dynamic DNS (»DynDNS«), R&S Unified Firewalls retrieves a fixed hostname (for example `yourcompany.dyndns.org`) on the Internet, even if it has no fixed public IP address. This is accomplished by sending the current IP address to a DynDNS provider that maps it to a domain name so that the firewall is accessible using that domain name. If the IP address changes due to a DSL disconnect forced, for example, by your Internet service provider, the IP address is re-sent to the DynDNS provider. This ensures that the dynamic DNS always points to the current IP address.

To set up DynDNS on R&S Unified Firewalls, you require a configured DynDNS account with a DynDNS provider. Further information on dynamic DNS and the registration for the dynamic DNS process can be found at, for example, www.dyndns.org.

For more detailed information on dynamic DNS accounts, see the following sections.

DynDNS Accounts Overview

Navigate to "Network > DynDNS Accounts" to display the list of DynDNS accounts that are currently defined on the system in the item list bar.

In the expanded view, the columns of the table display the "Hostname" of the DynDNS account, the "Status" of the account and the "Server Type". The buttons in the last column allow you to view and adjust the settings for an existing DynDNS account, create an account based on a copy of an existing DynDNS account or delete an account from the system.

For further information, see Chapter 3.2, "Icons and Buttons", on page 23.

DynDNS Accounts Settings

Under "Network > DynDNS Accounts", you can add a new or edit an existing custom DynDNS account for WAN access in general.

The "DynDNS Account" settings allow you to configure the following elements:

Field	Description
I/○	A slider switch indicates whether the DynDNS account is active (I) or inactive (○). By clicking the slider switch, you can toggle the state of the DynDNS account. A new DynDNS account is enabled by default.
"Internet Connection"	From the drop-down list, select the Internet connection to be used by the account.
"Server Type"	From the drop-down list of supported DynDNS services, select the type of server to be used.
"Hostname"	DynDNS services provide a domain name entry under their authority. Consequently, a registered host always has the suffix of the service provider (for example `yourname.dynamicdns.org`). Enter the complete host name in this input field.
"Username"	Enter the user name with which your account is registered with the DynDNS provider.
"Password"	Enter the password with which your account is registered with the DynDNS provider.
"Show Password"	Optional: Select this checkbox to verify the password.
"Custom Server Address"	Optional: Enter the address of the server if your DynDNS provider requires the definition of a different server address.
"MX Record"	Optional: If you wish to use an MX record, enter its IP address or hostname.
"Wildcards"	Optional: Select this checkbox to activate the possibility to use wildcards in host names if you plan to use subdomains of your DynDNS account (for example, `*.yourname.dynamicdns.org` will resolve for any domains ending with `yourname.dynamicdns.org`).

The buttons at the bottom right of the editor panel depend on whether you add a new DynDNS account or edit an existing account. For a newly configured account, click "Create" to add the account to the list of available DynDNS accounts or "Cancel" to discard your changes. To edit an existing account, click "Save" to store the reconfigured account or "Reset" to discard your changes. You can click "Close" to shut the editor panel as long as no changes have been made on it.

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

3.4.3.5 Interfaces

Navigate to "Network > Interfaces" to configure Ethernet, VLAN, Bridge, PPP and WLAN interfaces. The item list bar displays an overview of all interfaces which are currently defined on the system.

Bond Interfaces

Use the "Bond Interfaces" settings to aggregate multiple physical Ethernet interfaces into one logical bond interface. Depending on its mode of operation, a bond interface offers the following two advantages:

- Load balancing – A bond interface provides increased bandwidth by using all aggregated Ethernet interfaces in parallel to transmit data.
- High availability – If one Ethernet interface fails, data can still be received and transmitted on the remaining Ethernet interfaces.

You can add as many bond interfaces as you like as long as there are available Ethernet interfaces that are not used by other interfaces or in any network connections.

For more detailed information on bond interfaces, see the following sections.

Bond Interfaces Overview

Navigate to "Network > Interfaces > Bond Interfaces" to display the list of bond interfaces that are currently defined on the system in the item list bar.

In the expanded view, the first column of the table displays the "Name" of the bond interface. The "Status" column shows one of the following status indicators:

- Green – The bond interface is up.
- Gray – The bond interface is disabled.

Furthermore, the "Ports" (i.e. the Ethernet interfaces) that are assigned to the bond interface are displayed. The buttons in the last column allow you to view and adjust the settings for an existing bond interface or delete a bond interface from the system.

For further information, see Chapter 3.2, "Icons and Buttons", on page 23.

Bond Interfaces Settings

Use the "Bond Interfaces" settings to configure custom bond interfaces.

Under "Network > Interfaces > Bond Interfaces", you can add a new or edit an existing bond interface.

The "Bond Interface" panel displays the following information and allows you to configure the following elements:

Field	Description
I/◯	A slider switch indicates whether the bond interface is active (I) or inactive (◯). By clicking the slider switch, you can toggle the state of the bond interface. A new bond interface is enabled by default.
"Name"	Displays the name of the bond interface. The name is generated automatically. Bond interfaces are numbered in the order they are created, starting with `bond0`.
"Hardware Address"	Displays the hardware address (MAC address) of the bond interface.
"Used by"	Displays the network components (e.g. connections, other interfaces, etc.) that use the bond interface.

Field	Description
"Mode"	From the drop-down list, select the mode of operation for the bond interface, specifying how the multiple Ethernet interfaces are to be aggregated. The option is set to `IEEE 802.1AX (LACP, Direct Connection)` by default, but you can adjust the settings to the other values as neccessary: ● `Balance - Round-Robin (Trunk, Direct Connection)` – This mode provides load balancing and high availability. Packets are transmitted in sequential order from the first available aggregated Ethernet interface through the last, then continuing with the first aggregated Ethernet interface again. ● `Active-Backup (Bridge)` – This mode provides high availability only. Data is transmitted and received by the active Ethernet interface (i.e. the first Ethernet interface in the list) only as long as it is not faulty. When the first Ethernet interface fails, the next Ethernet interface in the list is used to transmit and receive data. ● `Balance - XOR (Trunk, Direct Connection)` – This mode provides load balancing and high availability. Packets are transmitted on all Ethernet interfaces. A simple algorithm (layer2+3 XOR) is applied to decide which Ethernet interface is used to transmit the data. ● `Broadcast (Trunk, Direct Connection)` – This mode provides high availability only. Data is transmitted and received on all Ethernet interfaces simultaneously. ● `IEEE 802.1AX (LACP, Direct Connection)` – This mode provides load balancing and high availability by using the LACP (Link Aggregation Control Protocol) standard. Packets are transmitted on all Ethernet interfaces. A simple algorithm (layer2+3 XOR) is applied to decide which Ethernet interface is used to transmit the data. ● `Balance - TLB (Bridge)` – This mode provides load balancing and high availability. In addition to the simple selection algorithm (layer 2+3 XOR), the current load of the Ethernet interface is taken into account when deciding which Ethernet interface is to be used to transmit the data. ● `Balance - ALB (Bridge)` – This mode provides load balancing and high availability. Data is received using ARP negotiation. In addition to the simple selection algorithm (layer2+3 XOR), the current load of the Ethernet interface is taken into account when deciding which Ethernet interface is to be used to transmit the data.
"Ports"	Add the Ethernet interfaces that you want to aggregate into one logical link by clicking the input field. You can select any number of the available Ethernet interfaces. **Note:** You can select only Ethernet interfaces that are not used by other interfaces or in any network connections. The selected Ethernet interfaces are displayed in a table at the bottom of the panel. To delete an element from the input field, click ✖ to the left of the entry.
"MTU"	Set the maximum size of each packet (in bytes). The Maximum Transmission Unit can be any integer from `64` to `16384`.

The buttons at the bottom right of the editor panel depend on whether you add a new bond interface or edit an existing interface. For a newly configured bond interface, click "Create" to add the interface to the list of available bond interfaces or "Cancel" to discard your changes. To edit an existing bond interface, click "Save" to store the reconfigured interface or "Reset" to discard your changes. You can click "Close" to shut the editor panel as long as no changes have been made on it.

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

Bridge Interfaces

Use the "Bridge Interfaces" settings to connect two interfaces and their networks on Layer 2, forming a common broadcast domain.

For more detailed information on bridge interfaces, see the following sections.

Bridge Interfaces Overview

Navigate to "Network > Interfaces > Bridge Interfaces" to display the list of bridge interfaces that are currently defined on the system in the item list bar.

In the expanded view, the first column of the table displays the "Name" of the bridge interface. The "Status" column shows one of the following status indicators:

- Green – The bridge interface is enabled.
- Orange – The bridge interface is disabled.

Furthermore, the "Ports" that are assigned to the bridge interface are displayed. The buttons in the last column allow you to view and adjust the settings for an existing bridge interface, create a new bridge interface based on a copy of an existing bridge interface or delete a bridge interface from the system.

For further information, see Chapter 3.2, "Icons and Buttons", on page 23.

Bridge Interfaces Settings

Use the "Bridge Interfaces" settings to configure custom bridge interfaces.

Under "Network > Interfaces > Bridge Interfaces", you can add a new or edit an existing bridge interface.

The "Bridge Interface" panel displays the following information and allows you to configure the following elements:

Field	Description
I/○	A slider switch indicates whether the bridge interface is active (I) or inactive (○). By clicking the slider switch, you can toggle the state of the bridge interface. A new bridge interface is enabled by default.
"Name"	Displays the name of the bridge interface. The name is generated automatically. Bridges are numbered in the order they are created, starting with `br0`.
"Hardware Address"	Displays the hardware address (MAC address) of the bridge interface.
"Used by"	Displays the network components (e.g. connections, other interfaces, etc.) that use the bridge interface.
"Ports"	Add the ports that the interface will bridge by clicking the input field. You can select any number of VLAN interfaces or other bridge interfaces. To delete an element from the input field, click ✖ to the left of the entry. The selected ports are displayed in a table at the bottom of the panel. **Note:** Bridges cannot be created using interfaces which are already used in another bridge.
"MTU"	Set the maximum size of each packet (in bytes). The Maximum Transmission Unit can be any integer from `64` to `16384`.

Field	Description
"Spanning Tree Protocol"	Optional: Select this checkbox to enable the Spanning Tree Protocol. It is disabled by default.
"Priority"	Only available if "Spanning Tree Protocol" is enabled: Set the bridge priority. Enter a multiple of `4096` in the range of `4096` to `61440`.
"Hello Interval"	Only available if "Spanning Tree Protocol" is enabled: Set the hello interval (in seconds). Enter any integer from `1` to `10`.
"Ports"	This table displays the ports selected in the bridge interface. If "Spanning Tree Protocol" is enabled, the buttons on the right of each entry allow you to configure the "Priority" and the "Cost" for the respective port, and to remove the port from the bridge interface.

The buttons at the bottom right of the editor panel depend on whether you add a new bridge interface or edit an existing bridge. For a newly configured bridge interface, click "Create" to add the bridge to the list of available bridge interfaces or "Cancel" to discard your changes. To edit an existing bridge interface, click "Save" to store the reconfigured bridge or "Reset" to discard your changes. You can click "Close" to shut the editor panel as long as no changes have been made on it.

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

Ethernet Interfaces

The physical "Ethernet Interfaces" receive the following default IP addresses: `192.168.X.254/24` (`X` being the number of the interface, i.e. the IP address of eth0 is `192.168.0.254`).

For more detailed information on Ethernet interfaces, see the following sections.

Ethernet Interfaces Overview

Navigate to "Network > Interfaces > Ethernet Interfaces" to display the list of Ethernet interfaces that are currently defined on the system in the item list bar.

In the expanded view, the first column of the table displays the "Name" of the Ethernet interface. The "Status" column shows one of the following status indicators:

- Green – The Ethernet interface is up.
- Gray – The Ethernet interface is disabled.

Furthermore, the "Speed" of the Ethernet interface is displayed. The button in the last column allows you to view and adjust the settings for an existing Ethernet interface.

For further information, see Chapter 3.2, "Icons and Buttons", on page 23.

Ethernet Interfaces Settings

Under "Network > Interfaces > Ethernet Interfaces", you can display more detailed information on the available Ethernet interfaces and adjust the settings.

The "Ethernet Interface" panel displays the following information and allows you to configure the following elements:

Field	Description
"Name"	Displays the name of the Ethernet interface, e.g. `eth0`.
"Description"	Displays a short description of the Ethernet interface.
"Hardware Address"	Displays the hardware address (Ethernet MAC address) of the Ethernet interface.
"Used by"	Displays the connection that is currently using the Ethernet interface.
"Status"	Displays the status of the Ethernet interface. The status can be one of the following: ● `up` – The Ethernet interface is enabled. ● `disabled` – The Ethernet interface is disabled.
"Speed"	Displays the speed (e.g. in Gbit/s) of the Ethernet interface.
"Duplex"	Displays the duplex mode of the interface, e.g. `full`.
"Type"	Displays the type of wiring connected to the interface, e.g. `twisted pair`.
I/○	A slider switch indicates whether the Ethernet interface link is active (I) or inactive (○). By clicking the slider switch, you can toggle the state of the Ethernet interface link.
"MTU"	Set the maximum size of each packet (in bytes). The Maximum Transmission Unit can be any integer from `64` to `16384`.

If you modify the settings, click "Save" to store your changes or "Reset" to discard them. Otherwise, click "Close" to shut the editor panel.

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

PPP Interfaces

Use the "PPP Interfaces" settings to create interfaces using the Point-to-Point Protocol.

For more detailed information on PPP interfaces, see the following sections.

PPP Interfaces Overview

Navigate to "Network > Interfaces > PPP Interfaces" to display the list of PPP interfaces that are currently defined on the system in the item list bar.

In the expanded view, the first column of the table displays the "Name" of the PPP interface. The "Status" column shows one of the following status indicators:

- Green – The PPP interface is enabled.
- Orange – The PPP interface is disabled.

Furthermore, the "Master Interface" that the PPP interface is associated with is displayed. The buttons in the last column allow you to view and adjust the settings for an existing PPP interface, create a new PPP interface based on a copy of an existing PPP interface or delete a PPP interface from the system.

For further information, see Chapter 3.2, "Icons and Buttons", on page 23.

PPP Interfaces Settings

Use the "PPP Interfaces" settings to configure custom PPP interfaces.

Under "Network > Interfaces > PPP Interfaces", you can add a new or edit an existing PPP interface.

The "PPP Interfaces" panel allows you to configure the following elements:

Field	Description
I/○	A slider switch indicates whether the PPP interface is active (I) or inactive (○). By clicking the slider switch, you can toggle the state of the PPP interface. A new PPP interface is enabled by default.
"Master Interface"	From the drop-down list, select the Ethernet, VLAN or bridge interface that the PPP interface is associated with.
"LCP Echo Interval"	Specify at which interval (in seconds) R&S Unified Firewalls sends an echo request to the peer by entering an integer value from `1` to `1800`.
"LCP Echo Failure"	Specify the number of LCP echo failures after which the peer is considered dead by entering an integer value from `0` to `64`. If you enter `0`, failures are ignored.
"MTU"	Set the maximum size of each packet (in bytes). The Maximum Transmission Unit can be any integer from `64` to `16384`.
"MRU"	Specify the Maximum Receive Unit by entering an integer value from `128` to `16384`.

The buttons at the bottom right of the editor panel depend on whether you add a new PPP interface or edit an existing interface. For a newly configured PPP interface, click "Create" to add it to the list of available PPP interfaces or "Cancel" to discard your changes. To edit an existing PPP interface, click "Save" to store the reconfigured interface or "Reset" to discard your changes. You can click "Close" to shut the editor panel as long as no changes have been made on it.

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

VLAN Interfaces

Use the "VLAN Interfaces" settings to add custom Virtual Local Area Network tags to all traffic on a given interface.

This method can be used to create »virtual interfaces« that allow you to put several logical network zones on one physical interface. When a VLAN tag is associated with a network interface, the tag is added to all outgoing packets that are sent via this virtual interface and stripped from the incoming packets that are received on this VLAN. Several VLANs may be associated with each network interface. Packets with different tags can be processed and associated with the corresponding interface.

For more detailed information on VLAN interfaces, see the following sections.

VLAN Interfaces Overview

Navigate to "Network > Interfaces > VLAN Interfaces" to display the list of VLAN interfaces that are currently defined on the system in the item list bar.

In the expanded view, the first column of the table displays the "Name" of the VLAN interface. The "Status" column shows one of the following status indicators:

- Green – The VLAN interface is enabled.
- Orange – The VLAN interface is disabled.

Furthermore, the "Master Interface" that the virtual local area network is associated with and the "VLAN Tag" are displayed. The buttons in the last column allow you to view and adjust the settings for an existing virtual local area network, create a new VLAN interface based on a copy of an existing virtual local area network or delete a VLAN interface from the system.

For further information, see Chapter 3.2, "Icons and Buttons", on page 23.

VLAN Interfaces Settings

Use the "VLAN Interfaces" settings to configure custom Virtual Local Area Network tags to be added to all traffic on a given interface.

Under "Network > Interfaces > VLAN Interfaces", you can add a new or edit an existing virtual local area network.

The "VLAN Interface" panel displays the following information and allows you to configure the following elements:

Field	Description
I/○	A slider switch indicates whether the VLAN interface is active (I) or inactive (○). By clicking the slider switch, you can toggle the state of the VLAN interface. A new VLAN interface is enabled by default.
"Name"	Displays the name of the VLAN interface. The name is generated automatically and contains the "VLAN Tag" and the underlying "Master Interface".
"Hardware Address"	For edited VLAN interfaces only: Displays the hardware address (MAC address) of the underlying "Master Interface".
"Used by"	Displays the network components (e.g. connections, other interfaces etc.) that use the VLAN interface.
"Master Interface"	For newly added VLAN interfaces only: From the drop-down list, select the Ethernet or Bridge interface that the virtual local area network is associated with. For edited VLAN interfaces only: Displays the Ethernet or Bridge interface that the virtual local area network is associated with.
"VLAN Tag"	Enter the text content of the VLAN tag. The tag may contain any integer from `1` to `4094`.
"MTU"	Set the maximum size of each packet (in bytes). The Maximum Transmission Unit is limited to the MTU value of the underlying master interface. **Note:** Due to a kernel restriction, the maximum MTU value is limited by the Maximum Transmission Unit value of the underlying interface.

The buttons at the bottom right of the editor panel depend on whether you add a new VLAN interface or edit an existing virtual local area network. For a newly configured VLAN interface, click "Create" to add the VLAN to the list of available virtual local area network interfaces or "Cancel" to discard your changes. To edit an existing VLAN interface, click "Save" to store the reconfigured VLAN or "Reset" to discard your changes. You can click "Close" to shut the editor panel as long as no changes have been made on it.

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

WLAN (Wireless LAN) Interfaces

All R&S Unified Firewalls models can be enhanced with a wireless USB flash drive to create a wireless access point in your network (see also Chapter 3.4.3.8, "WLAN Settings", on page 98).

Use the "WLAN Interfaces" settings to configure interfaces that can be used in WLAN connections.

For more detailed information on WLAN interfaces, see the following sections.

WLAN Interfaces Overview

Navigate to "Network > Interfaces > WLAN Interfaces" to display the list of WLAN interfaces that are currently defined on the system in the item list bar.

In the expanded view, the first column of the table displays the "Name" of the WLAN interface. The "Status" column shows one of the following status indicators:

- Green – The WLAN interface is enabled.
- Orange – The WLAN interface is disabled.

The button in the last column allows you to view and adjust the settings for an existing WLAN interface.

For further information, see Chapter 3.2, "Icons and Buttons", on page 23.

WLAN Interfaces Settings

Use the "WLAN Interfaces" settings to configure an interface that can be used in a WLAN connection.

Under "Network > Interfaces > WLAN Interfaces", you can view and edit an existing WLAN interface.

The "WLAN Interface" panel displays the following information and allows you to configure the following elements:

Field	Description
I/○	A slider switch indicates whether the WLAN interface is active (I) or inactive (○). By clicking the slider switch, you can toggle the state of the WLAN interface.
"Name"	Displays the name of the WLAN interface: `wlan0`. The name is automatically generated.

Field	Description
"Device Status"	Displays the status of the device. The status can be one of the following: ● Plugged – A wireless USB flash drive is connected to R&S Unified Firewalls. ● Unplugged – No wireless USB flash drive has been connected to your firewall yet, or a previously connected wireless USB flash drive has been disconnected from R&S Unified Firewalls.
"Hardware Address"	Displays the hardware address (Ethernet MAC address) of the physical interface that the wireless USB flash drive is connected to.
"Used by"	Displays the connection that uses the WLAN interface.
"MTU"	Set the maximum size of each packet (in bytes). The Maximum Transmission Unit can be any integer from 64 to 16384. **Note:** Due to a kernel restriction, the maximum MTU value is limited by the Maximum Transmission Unit value of the underlying interface.

The buttons at the bottom right of the editor panel allow you to shut ("Close") the editor panel as long as no changes have been made and to store ("Save") or to discard ("Reset") your changes.

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

3.4.3.6 Quality of Service (QoS)

Under "Network > QoS" you can set up Quality of Service for your Internet connections, in other words, for the network and PPP connections for which you configured a default gateway.

Quality of Service (QoS) prioritizes the processing of queued network packets in R&S Unified Firewalls based on Type of Service (ToS) flags. This way, performance-critical applications like Voice over IP (RTP) can be prioritized.

A precondition for Quality of Service is that applications or devices (such as VoIP telephone systems) set the ToS field in IP data packets. R&S Unified Firewalls then sorts the packets based on the value of the ToS field and assigns them to several queues with different priorities. Data packets from the queue with the highest priority are forwarded immediately. Data packets from queues with lower priority are only forwarded when all the queues with higher priority have been emptied.

QoS Settings

Navigate to "Network > QoS > QoS Settings" to open en editor panel to view, activate and adjust the Quality of Service settings.

The "QoS Settings" panel allows you to configure the following elements:

Field	Description
I/○	A slider switch indicates whether Quality of Service is active (I) or inactive (○). By clicking the slider switch, you can toggle the state of QoS.
"QoS Services"	Enter a "Service" for which you want to activate QoS. Specify the hexadecimal "Value" of the ToS field which defines the application or the device for the service. Click ⊕ to add the service to the list. You can edit or delete single entries in the list by clicking the corresponding button next to an entry. For further information, see Chapter 3.2, "Icons and Buttons", on page 23. **Note:** If you edit an entry, a check mark appears on the right of the entry. Click the check mark to apply your changes. Click ▲/▼ or drag and drop an entry to change the priority of the services. The service which is listed first in the list has the highest priority.

The buttons at the bottom right of the editor panel allow you to shut ("Close") the editor panel as long as no changes have been made and to store ("Save") or to discard ("Reset") your changes.

QoS Connections

The "Connections" settings allow you to configure Quality of Service connections.

The QoS connections configured here take effect only if Quality of Service has been activated for Internet connections. For more information, see "QoS Settings" on page 93.

For more detailed information on QoS connections, see the following sections.

QoS Connections Overview

Navigate to "Network > QoS > Connections" to display the list of QoS connections that are currently defined on the system in the item list bar.

In the expanded view, the columns of the table display the "Name" of the connection as well as the configured "Download" and "Upload" bandwidth thresholds. The buttons in the last column allow you to view and adjust the settings for an existing QoS connection or delete a connection from the system.

For further information, see Chapter 3.2, "Icons and Buttons", on page 23.

QoS Connections Settings

The "QoS Connection" settings allow you to configure the following elements for a Quality of Service connection:

Field	Description
"Internet Connection"	From the drop-down list, select the Internet connection for which you want to set up Quality of Service.
"Download Rate"/"Upload Rate"	To ensure Quality of Service, enter the bandwidth thresholds to be reserved for QoS services using this QoS connection. The two input fields determine the maximum bandwidth (in kilobits per second) for download and upload. If you set both fields to `0`, Quality of Service is not applied for this QoS connection.

The buttons at the bottom right of the editor panel depend on whether you add a new QoS connection or edit an existing connection. For a newly configured QoS connection, click "Create" to add the connection to the list of available QoS connections or "Cancel" to reject the creation of a new QoS connection. To edit an existing QoS connection, click "Save" to store the reconfigured connection or "Reset" to discard your changes. You can click "Close" to shut the editor panel as log as no changes have been made on it.

3.4.3.7 Routing

Use the "Routing" settings to configure routing tables and routing rules.

The routing settings allow you to define custom routes that are used to reach devices on a given destination network.

Routes between network objects are created automatically and hidden. You should not normally need to create routes unless you have an upstream router that requires special routes. To influence traffic between network objects, create a firewall rule as described under Chapter 3.3, "Firewall Rule Settings", on page 25.

Routing Rules

Routing rules specify which packets are managed by which routing table. This allows for more differentiated routing as routing rules include more fields of the IP header in the routing decision, whereas routing tables only consider the destination IP address.

Routing Rules Overview

Navigate to "Network > Routing Rules" to display the list of routing rules that are currently defined on the system.

The plus button ⊕ above the filter settings allows you to add new routing rules.

The "Filter Settings" allow you to narrow down the list of results in the table to display only entries that include a certain search string. You can filter the contents by selecting the required options from the drop-down list and/or entering search strings in the respective input fields. Click "Apply" to apply the selected filter options. The list of routing rules is adjusted to reflect your filter results. Click "Reset" to delete the selected filter options and display an unfiltered view of the list of routing rules.

The table columns of the routing rules list display the priority of the routing rule, the selectors that can be used to define which traffic should be routed where and whether it is a system rule or not. The buttons in the last column allow you to view and adjust the settings of a routing rule or delete a rule from the system.

For further information, see Chapter 3.2, "Icons and Buttons", on page 23.

System routing rules cannot be modified or deleted.

To close the "Routing Rules" panel, click ✖ in the upper right corner of the panel.

Routing Rules Settings

Under "Network > Routing Rules", you can add a new or edit an existing routing rule.

The "Routing Rule" settings allow you to configure the following elements:

Field	Description
"Priority"	Set the priority of the routing rule by entering an integer value from `64` to `32767` for custom rules. The rules are sorted by priority in ascending order. This means the system runs through the rules list starting with the system rule with priority `0` until all selectors in a rule match the packet. The action of this rule is then carried out.
"Source Subnet"	Optional: Enter the IP address of the source subnet in CIDR notation (IP address followed by a slash »/« and the number of bits set in the subnet mask, for example `192.168.50.0/24`).
"Destination Subnet"	Optional: Enter the IP address of the destination subnet in CIDR notation (IP address followed by a slash »/« and the number of bits set in the subnet mask, for example `192.168.50.0/24`).
"Input Interface"	Optional: Select one of the interfaces defined on R&S Unified Firewalls as the input interface.
"Output Interface"	Optional: Select one of the interfaces defined on R&S Unified Firewalls as the output interface.
"TOS"	Optional: Specify the Type of Service value by entering a hexadecimal number from `0` to `FF`.
"Action"	Specify the rule action: ● "Goto" – Enter the "Priority" of another routing rule. If a packet matches the selectors in the rule, it goes to the rule with the specified goto priority. ● "Table" – Enter the number of a routing table. If a packet matches the selectors in the rule, it runs through the specified routing table. If one of the routes in the table matches the packet, it is routed accordingly. Otherwise, the packet continues to run through the routing rules list. The parameter entered here, is displayed in the "Action Parameter" table column of the routing rules list (for more information, see "Routing Rules Overview" on page 95).

If you specify none of the selectors, the entire traffic matches the rule.

The buttons at the bottom right of the editor panel depend on whether you add a new routing rule or edit an existing rule. For a newly configured routing rule, click "Create" to add the rule to the list of available routing rules or "Cancel" to reject the creation of the new rule. To edit an existing rule, click "Save" to store the reconfigured rule or "Reset" to discard your changes. You can click "Close" to shut the editor panel as long as no changes have been made on it.

Routing Tables

Routing tables route packets through the network based on the destination IP address.

For more detailed information on routing tables, see the following sections.

Routing Tables Overview

Navigate to "Network > Routing > Routing Tables" to display the list of routing tables that are currently defined on the system in the item list bar.

Deselect the "Show configurable tables only" checkbox to display all tables on the system. Otherwise, only tables that can be edited are displayed.

The following tables are preset on the system:

- Table 254 is the main routing table. You can add custom routes to this table. The entries are then adopted for all existing routing tables.
- Table 255 contains local routes for all configured interfaces.
- Tables 1 to 63 are reserved for the management of the Internet connections.
- Tables 64 to 250 are reserved for routes with a source address and appear with a source IP address during the set-up of routes.
- Table 293 is reserved for the transparent proxy.

In the expanded view, the columns of the table display the name of the routing table. The buttons in the last column allow you to view and adjust the settings for an existing routing table or delete a table from the system.

For further information, see Chapter 3.2, "Icons and Buttons", on page 23.

Routing Tables Settings

The "Routing Tables" settings allow you to add a new or edit existing routing tables.

The "Routing Table" settings allow you to configure the following elements:

Field	Description
"Table Number"	Enter an ID for the routing table. Custom routing tables receive the ID `512` or higher. You must configure routing rules pointing to custom routing tables, otherwise those tables are not used (see "Routing Rules" on page 95).
"Routes"	This table displays the custom routes that are specified in the routing table. Click "Add" to open the "Edit Route" panel and define a new route. You can edit or delete single entries in the list by clicking the corresponding button next to an entry.

The "Edit Route" panel allows you to configure the following elements:

Field	Description
"Destination"	Enter the IP address of the destination network in CIDR notation (IP address followed by a slash »/« and the number of bits set in the subnet mask, for example 192.168.50.0/24).
"Interface"	Select an interface for the route.
"Gateway"	Enter an IP address as the gateway for this route. Traffic from the source zone to the destination network will be routed using this gateway (rather than the standard gateway).
"Type"	Select the address type from the drop-down list.
"Preferred Source"	Only packets with the selected sender address will be routed.
"Metric"	Define the costs for the route. The value entered here concerns routing protocols. A higher metric means the route is considered costly and is less likely to be chosen.

Click "OK" to save the route settings and return to the "Routing Table" panel.

The buttons at the bottom right of the editor panel depend on whether you add a new routing table or edit an existing table. For a newly configured routing table, click "Create" to add the table to the list of available routing tables or "Cancel" to discard your changes. To edit an existing routing table, click "Save" to store the reconfigured table or "Reset" to discard your changes. You can click "Close" to shut the editor panel as long as no changes have been made on it.

3.4.3.8 WLAN Settings

All R&S Unified Firewalls models can be enhanced with a wireless USB flash drive to create a wireless access point in your network.

Connect a compatible wireless USB adapter to the USB port of your R&S Unified Firewalls to configure a wireless access point. A successful configuration allows wireless clients to connect to this access point to join the wireless local area network (WLAN).

Navigate to "Network > WLAN Settings" to display and edit the WLAN settings of your R&S Unified Firewalls.

The "WLAN Settings" panel allows you to configure the following elements:

Field	Description
I/○	A slider switch indicates whether the WLAN is active (I) or inactive (○). By clicking the slider switch, you can toggle the state.
"Device Status"	Displays the status of the device. The status can be one of the following: ● `Plugged` – A wireless USB flash drive is connected to R&S Unified Firewalls. ● `Unplugged` – A previously connected wireless USB flash drive has been disconnected from R&S Unified Firewalls.
"License"	Displays your license information.

Field	Description
"Mode"	From the drop-down list, select the communication specifications according to IEEE 802.11. The mode can be one of the following: ● a – up to 54 Mbit/s 5 GHz ● an – up to 300 Mbit/s 5 GHz ● b – up to 11 Mbit/s 2.4 GHz ● g – up to 54 Mibt/s 2.4 GHz (default setting) ● gn – up to 300 Mbit/s 2.4 GHz
"Country Code"	From the drop-down list, select the correct two-letter code for your country. The set default value is the standard country code 00 which is compatible with all countries.
"SSID"	Enter an identifier for the WLAN.
"Show SSID"	Optional: Select this checkbox if you want the SSID to be visible to the public.
"Encryption Mode"	From the drop-down list, select the desired encryption mode. The mode can be one of the following: ● WPA ● WPA2 ● WPA+WPA2 (default setting)
"Encryption Protocol"	From the drop-down list, select one of the following encryption protocols to be used: ● TKIP – Temporal Key Integrity Protocol ● CCMP – Counter-Code/CBC-MAC Protocol ● TKIP+CCMP – a combination of the two methods above
"Preshard Key"	Enter the pre-shared key to be used for encryption. Clients need to supply this password in order to establish a secured connection to R&S Unified Firewalls.

On the "Advanced" tab:

Field	Description
"HT Mode"	If you selected an or gn as the communication mode, you can now select the channel width from the drop-down list: ● Disabled ● [HT-40] - 40MHz below the selected channel for the channels 5 to 13 in mode g ● [HT40+] - 40MHz above the selected channel for the channels 1 to 9 in mode g For the remaining communication modes, this field is disabled and set to 20 by default.
"Channel Number/ Frequency"	From the drop-down list, select the channel number (frequency). The options available for selection depend on the chosen communication mode and on the selected country code.
"Transmit Power"	Specify the transmit power (in decibel-milliwatts) to be used. The value can be any integer from 1 to the maximum transmit power. It is set to 20 dBm by default.
"Access Point Station Isolation"	Optional: Select this checkbox to prevent the clients from communicating directly with each other.
"Log Level"	Define the log level from level 0 to 4.

On the "MAC Filter" tab:

Field	Description
"MAC Filter Mode"	Use the MAC filter to determine whether a wireless device is to be granted access to the WLAN. The default setting is "Disabled" which means that no filtering is performed, but you can adjust the settings to one of the following values as necessary: ● "Blacklist" – The specified MAC addresses and, therefore, clients are blocked. ● "Whitelist" – The specified MAC addresses and, therefore, clients are granted access to the network.
"MAC Addresses"	Enter MAC addresses to be applied when filtering and click "Add" after each entry. You can edit or delete single entries in the list by clicking the corresponding button next to an entry.

The buttons at the bottom right of the editor panel allow you to shut ("Close") the editor panel as long as no changes have been made and to store ("Save") or to discard ("Reset") your changes.

3.4.4 Desktop

The " Desktop" settings display a list of all available services and the firewall rules defined in the system.

3.4.4.1 Desktop Connections

Navigate to "Desktop > Desktop Connections" to display and edit the connections between various desktop objects that are defined on the system.

Desktop Connections Overview

In the expanded view, the columns of the table display the nodes of the desktop connection. The buttons in the last column allow you to view and adjust the settings for an existing desktop connection, create a connection based on a copy of an existing desktop connection or delete a connection from the system.

For further information, see Chapter 3.2, "Icons and Buttons", on page 23.

Copied desktop connections are always set up between the same nodes as the original.

Desktop Connections Settings

When you edit a desktop connection, the "Connection" panel opens. Under "Description", you can enter additional information regarding the desktop connection for internal use.

On the "Rules" tab, you can modify the rule set for this connection. For further information on creating firewall rules, see Chapter 3.3, "Firewall Rule Settings", on page 25.

The "URL / Content Filter" tab allows you to configure the URL and content filter for this connection:

Field	Description
"Block all by default"	Select this checkbox to add all URL filters that are currently defined on the system to the blacklist and to select all content filters.
"Name"	Displays the name of the URL and content filter.
"URL Filter Black"/"White"	Add the URLs in the respective filters to the blacklist or whitelist by clicking the corresponding checkboxes.
"Content Filter"	Select the content filters by clicking the corresponding checkboxes.
"Schedule"	Displays whether the filter is always active, always inactive or active on a customized time schedule. Click the entry to modify the schedule.

If you have created application filter profiles as described in Chapter 3.4.5.2, "Application Filter", on page 121, you can enable or disable the application filter for this desktop connection. On the "Application Filter" tab, you can set the "Mode" of the application filter to "Blacklist" or "Whitelist" or disable the application filter for each selected profile by selecting the respective radio button.

The buttons at the bottom right of the editor panel allow you to shut ("Close") the editor panel as long as no changes have been made and to store ("Save") or to discard ("Reset") your changes.

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

For further information on URL and content filters and the application filter, see Chapter 3.4.5.7, "URL/Content Filter", on page 133 and Chapter 3.4.5.2, "Application Filter", on page 121.

3.4.4.2 Desktop Objects

Use the "Desktop Objects" settings to organize your network by setting up single and group objects for hosts, users, networks, VPN and IP ranges. The created objects are displayed as nodes on the desktop and can be used as sources and/or destinations in connections to apply firewall rules.

The item list bar displays an overview of all desktop objects, subdivided into types of desktop objects, that are currently defined on the system. When you click an entry in the item list bar, the system highlights the respective desktop object and all connections which use this object on the desktop.

To create a desktop object, click the ⊕ button at the top of the respective section in the item list bar. Alternatively, click the respective desktop object icon in the toolbar at the top of the desktop.

For further information, see Chapter 3.2, "Icons and Buttons", on page 23.

The sections below provide further information on the various types of desktop objects.

Host/Network Groups

Create desktop objects for host and network groups that can be used to create connections between multiple hosts or networks and other desktop objects (such as VPN objects, etc.). Host and network groups can be used as sources and/or destinations to apply firewall rules and web filters to multiple computers.

Host/Network Groups Overview

Navigate to "Desktop > Desktop Objects > Host/Network Groups" to display the list of host and network group objects that are currently defined on the system in the item list bar.

In the expanded view, the table displays the "Name" of the host or network group object. The buttons in the last column allow you to view and adjust the settings for an existing host or network group object, create a group object based on a copy of an existing host or network group object or delete a group object from the system.

For further information, see Chapter 3.2, "Icons and Buttons", on page 23.

Host/Network Groups Settings

The "Host/Network Group" settings allow you to configure the following elements:

Field	Description
"Name"	Specify a name for the host or network group object.
"Description"	Optional: Enter additional information on the host or network group object for internal use.
"Tags"	Optional: From the drop-down list, select the desktop tags that you want to assign to the host or network group object. For further information, see Chapter 3.4.4.4, "Desktop Tags", on page 114.
"Color"	Select the color to be used for this object on the desktop.
"Hosts/Networks"	Specify the hosts or networks that you want to add to the host or network group object. Define the "Name", whether login is allowed, the "Interface", and the IP address of the host or network. Click "Add" to add a host or network to the list. You can edit or delete single entries in the list by clicking the corresponding button next to an entry. For further information, see Chapter 3.2, "Icons and Buttons", on page 23. **Note:** If you edit an entry, a check mark appears on the right of the entry. Click the check mark to apply your changes.

The buttons at the bottom right of the editor panel depend on whether you add a new host or network group object or edit an existing object. For a newly configured object, click "Create" to add the object to the list of available host and network groups or "Cancel" to discard your changes. To edit an existing object, click "Save" to store the reconfigured object or "Reset" to discard your changes. You can click "Close" to shut the editor panel as long as no changes have been made on it.

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

Hosts

Create a host object that can be used to create connections between the host and other desktop objects (such as VPN objects etc.). A host (for example a printer or a VoIP phone) can be assigned a dedicated IP address so that firewall rules can be specifically applied to it. For further information on creating firewall rules, see Chapter 3.3, "Firewall Rule Settings", on page 25.

Hosts Overview

Navigate to "Desktop > Desktop Objects > Hosts" to display the list of host objects that are currently defined on the system in the item list bar.

In the expanded view, the columns of the table display the "Name" and the "IP" of the host object as well as the interface it is connected to. The buttons in the last column allow you to view and adjust the settings for an existing host object, create an object based on a copy of an existing host object or delete an object from the system.

For further information, see Chapter 3.2, "Icons and Buttons", on page 23.

Hosts Settings

The "Host" settings allow you to configure the following elements:

Field	Description
"Name"	Specify a name for the host object.
"Description"	Optional: Enter additional information on the host object for internal use.
"Tags"	Optional: From the drop-down list, select the desktop tags that you want to assign to the host object. For further information, see Chapter 3.4.4.4, "Desktop Tags", on page 114.
"Color"	Select the color to be used for this object on the desktop.
"Allow login"	Select this checkbox to allow the user to log on to R&S Unified Firewalls using the IP address of this host object. This allows your R&S Unified Firewalls to apply user-specific firewall rules to the user currently logged on.
"Icon"	Select an icon to represent the host on the desktop.
"Connected to"	Select an interface that the host is connected to.
"IP Address"	Enter the IP address of the host object.

The buttons at the bottom right of the editor panel depend on whether you add a new host object or edit an existing object. For a newly configured object, click "Create" to add the object to the list of available host objects or "Cancel" to discard your changes. To edit an existing object, click "Save" to store the reconfigured object or "Reset" to discard your changes. You can click "Close" to shut the editor panel as long as no changes have been made on it.

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

Internet Objects

Create Internet objects for your Internet connections. Internet objects are used to create connections between other desktop objects (such as VPN objects) and the Internet.

Internet Objects Overview

Navigate to "Desktop > Desktop Objects > Internet Objects" to display the list of Internet objects that are currently defined on the system in the item list bar.

In the expanded view, the table displays the "Object Name" of the Internet object. The buttons in the last column allow you to view and adjust the settings for an existing Internet object, create an object based on a copy of an existing Internet object or delete an object from the system.

For further information, see Chapter 3.2, "Icons and Buttons", on page 23.

Internet Objects Settings

The "Internet Object" settings allow you to configure the following elements:

Field	Description
"Object Name"	Specify a name for the Internet object.
"Description"	Optional: Enter additional information on the Internet object for internal use.
"Tags"	Optional: From the drop-down list, select the desktop tags that you want to assign to the Internet object. For further information, see Chapter 3.4.4.4, "Desktop Tags", on page 114.
"Color"	Select the color to be used for this object on the desktop.
"Connections"	Select the Internet connection(s) that this object is part of. For further information, see "Network Connections Settings" on page 73.

The buttons at the bottom right of the editor panel depend on whether you add a new Internet object or edit an existing object. For a newly configured object, click "Create" to add the object to the list of available Internet objects or "Cancel" to discard your changes. To edit an existing object, click "Save" to store the reconfigured object or "Reset" to discard your changes. You can click "Close" to shut the editor panel as long as no changes have been made on it.

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

For information on how to create an Internet object, see "Creating an Internet Object" on page 15.

IP Ranges

Create an IP address range object to group hosts by indicating a start and end IP address. If a DHCP server is configured for the selected interface, you can also use the address range of the DHCP server.

IP Ranges Overview

Navigate to "Desktop > Desktop Objects > IP Ranges" to display the list of IP range objects that are currently defined on the system in the item list bar.

In the expanded view, the columns of the table display the "Object Name" of the IP range object, the "Interface" it is connected to, as well as its "Start IP" and "End IP". The buttons in the last column allow you to view and adjust the settings for an existing IP range object, create an object based on a copy of an existing IP range object or delete an object from the system.

For further information, see Chapter 3.2, "Icons and Buttons", on page 23.

IP Ranges Settings

The "IP Range" settings allow you to configure the following elements:

Field	Description
"Name"	Specify a name for the IP range object.
"Description"	Optional: Enter additional information on the IP range object for internal use.
"Tags"	Optional: From the drop-down list, select the desktop tags that you want to assign to the IP range object. For further information, see Chapter 3.4.4.4, "Desktop Tags", on page 114.
"Color"	Select the color to be used for this object on the desktop.
"Allow login"	Select this checkbox to allow the user to log on to R&S Unified Firewalls using the IP range of this object. This allows your R&S Unified Firewalls to apply user-specific firewall rules to the user currently logged on.
"Interface"	Select an interface to assign it to the IP range object. Select `any` if you do not want to assign this object to a certain interface. This way, all interfaces will accept packets from the IP range of this object.
"Start IP"	Specify the start IP address of the IP range.
"End IP"	Specify the end IP address of the IP range.

If you want to use the IP address range of the DHCP server of the selected interface, click the "Use DHCP IP range" button at the bottom left of the editor panel.

The buttons at the bottom right of the editor panel depend on whether you add a new IP range object or edit an existing object. For a newly configured object, click "Create" to add the object to the list of available IP range objects or "Cancel" to discard your changes. To edit an existing object, click "Save" to store the reconfigured object or "Reset" to discard your changes. You can click "Close" to shut the editor panel as long as no changes have been made on it.

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

Networks

Create a network object that can be used to create connections between the network and other desktop objects (such as VPN objects, etc.).

Networks Overview

Navigate to "Desktop > Desktop Objects > Networks" to display the list of network objects that are currently defined on the system in the item list bar.

In the expanded view, the columns of the table display the "Name" and the "IP" of the network object as well as the "Interface" it is connected to. The buttons in the last column allow you to view and adjust the settings for an existing network object, create an object based on a copy of an existing network object or delete an object from the system.

For further information, see Chapter 3.2, "Icons and Buttons", on page 23.

Networks Settings

The "Network" settings allow you to configure the following elements:

Field	Description
"Name"	Specify a name for the network object.
"Description"	Optional: Enter additional information on the network object for internal use.
"Tags"	Optional: From the drop-down list, select the desktop tags that you want to assign to the network object. For further information, see Chapter 3.4.4.4, "Desktop Tags", on page 114.
"Color"	Select the color to be used for this object on the desktop.
"Allow login"	Select this checkbox to allow the user to log on to R&S Unified Firewalls using the IP address of this network object. This allows your R&S Unified Firewalls to apply user-specific firewall rules to the user currently logged on.
"Interface"	Select the interface that the network is connected to.
"Network IP"	Enter the IP address of the network in CIDR notation (IP address followed by a slash »/« and the number of bits set in the subnet mask, for example `192.168.50.0/24`).

The buttons at the bottom right of the editor panel depend on whether you add a new network or edit an existing network. For a newly configured network, click "Create" to add the network to the list of available networks or "Cancel" to discard your changes. To edit an existing network, click "Save" to store the reconfigured network or "Reset" to discard your changes. You can click "Close" to shut the editor panel as long as no changes have been made on it.

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

User Groups

Create desktop objects for user groups that can be used to create connections between multiple users and other desktop objects (such as VPN objects etc.) applying a common rule set to multiple users.

User Groups Overview

Navigate to "Desktop > Desktop Objects > User Groups" to display the list of user group objects that are currently defined on the system in the item list bar.

In the expanded view, the table displays the "Name" of the user group object. The buttons in the last column allow you to view and adjust the settings for an existing user group object, create an object based on a copy of an existing user group or delete an object from the system.

For further information, see Chapter 3.2, "Icons and Buttons", on page 23.

User Groups Settings

The "User Group" settings allow you to configure the following elements:

Field	Description
"Name"	Specify a name for the user group object.
"Description"	Optional: Enter additional information on the user group object for internal use.
"Tags"	Optional: From the drop-down list, select the desktop tags that you want to assign to the user group object. For further information, see Chapter 3.4.4.4, "Desktop Tags", on page 114.
"Color"	Select the color to be used for this object on the desktop.
"User"	Select the users you want to add to the group. The left-hand list displays the users in the group. The right-hand list displays the users available in the system that are not part of the group. To add a user to the group, click ‹. Click « to add all available users at once. To remove a user from the group, click ›. Click » to remove all users at once. Use the "Filter" field to narrow down the list of users to display only entries that include a certain search string. Click ⊗ to display an unfiltered view of the list of users. **Note:** Users may be part of multiple user groups.

The buttons at the bottom right of the editor panel depend on whether you add a new user group or edit an existing group. For a newly configured group, click "Create" to add the group to the list of available user groups or "Cancel" to discard your changes. To edit an existing group, click "Save" to store the reconfigured group or "Reset" to discard your changes. You can click "Close" to shut the editor panel as long as no changes have been made on it.

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

Users

Create desktop objects for users that can be used to display the users on the desktop and to create connections between the users and other desktop objects (such as VPN objects etc.).

The menu "Desktop > Desktop Objects > Users" only serves to create desktop objects for users that already exist in the system. For information on how to add and manage users, see Chapter 3.4.1.9, "User Authentication", on page 47.

Users Overview

Navigate to "Desktop > Desktop Objects > Users" to display the list of user objects that are currently defined on the system in the item list bar.

In the expanded view, the columns of the table display the "Name" of the user object and the "User Name" associated with it. The buttons in the last column allow you to view and adjust the settings for an existing user object, create an object based on a copy of an existing user object or delete an object from the system.

For further information, see Chapter 3.2, "Icons and Buttons", on page 23.

Users Settings

The "User" settings allow you to configure the following elements:

Field	Description
"Object Name"	Specify a name for the user object.
"Description"	Optional: Enter additional information on the user object for internal use.
"Tags"	Optional: From the drop-down list, select the desktop tags that you want to assign to the user object. For further information, see Chapter 3.4.4.4, "Desktop Tags", on page 114.
"Color"	Select the color to be used for this object on the desktop.
"User Name"	Select the user to be used for the object. **Note:** Users may belong to multiple user objects.

The buttons at the bottom right of the editor panel depend on whether you add a new user object or edit an existing object. For a newly configured object, click "Create" to add the object to the list of available user objects or "Cancel" to discard your changes. To edit an existing object, click "Save" to store the reconfigured object or "Reset" to discard your changes. You can click "Close" to shut the editor panel as long as no changes have been made on it.

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

VPN Groups

Create a VPN group object that can be used to create connections between multiple VPN connections and other desktop objects applying a common rule set to multiple VPN connections.

VPN Groups Overview

Navigate to "Desktop > Desktop Objects > VPN Groups" to display the list of VPN group objects that are currently defined on the system in the item list bar.

In the expanded view, the table displays the "Name" of the VPN group object. The buttons in the last column allow you to view and adjust the settings for an existing VPN group object, create an object based on a copy of an existing VPN group object or delete an object from the system.

For further information, see Chapter 3.2, "Icons and Buttons", on page 23.

VPN Groups Settings

The "VPN Group" settings allow you to configure the following elements:

Field	Description
"Name"	Specify a name for the VPN group object.
"Description"	Optional: Enter additional information on the VPN group object for internal use.
"Tags"	Optional: From the drop-down list, select the desktop tags that you want to assign to the VPN group object. For further information, see Chapter 3.4.4.4, "Desktop Tags", on page 114.
"Color"	Select the color to be used for this object on the desktop.
"VPN Connections"	Select the VPN connections you want to add to the VPN group object. Select the "Type" of VPN connection that you want to add from the drop-down list. Under "Name", select the desired connection from the drop-down list. Click "Add" to add the connection to the list. You can edit or delete single entries in the list by clicking the corresponding button next to an entry. For further information, see Chapter 3.2, "Icons and Buttons", on page 23. **Note:** If you edit an entry, a check mark appears on the right of the entry. Click the check mark to apply your changes. **Note:** VPN connections may belong to multiple VPN groups.

The buttons at the bottom right of the editor panel depend on whether you add a new VPN group object or edit an existing object. For a newly configured object, click "Create" to add the object to the list of available VPN group objects or "Cancel" to discard your changes. To edit an existing object, click "Save" to store the reconfigured object or "Reset" to discard your changes. You can click "Close" to shut the editor panel as long as no changes have been made on it.

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

VPN Hosts

Create a VPN host object that can be used to configure firewall rules for VPN Client-to-Site connections.

VPN Hosts Overview

Navigate to "Desktop > Desktop Objects > VPN Hosts" to display the list of VPN host objects that are currently defined on the system in the item list bar.

In the expanded view, the columns of the table display the "Name" of the VPN host object, the "Type" of VPN connection and the VPN connection that the VPN host belongs to. The buttons in the last column allow you to view and adjust the settings for an existing VPN host object, create an object based on a copy of an existing VPN host object or delete an object from the system.

For further information, see Chapter 3.2, "Icons and Buttons", on page 23.

VPN Hosts Settings

The "VPN Host" settings allow you to configure the following elements:

Field	Description
"Name"	Specify a name for the VPN host object.
"Description"	Optional: Enter additional information on the VPN host object for internal use.
"Tags"	Optional: From the drop-down list, select the desktop tags that you want to assign to the VPN host object. For further information, see Chapter 3.4.4.4, "Desktop Tags", on page 114.
"Color"	Select the color to be used for this object on the desktop.
"Icon"	Select an icon to represent the VPN host object on the desktop.
"VPN Connection Type"	Select the type of the VPN connection by clicking the respective radio button.
"IPsec Connection"/"VPN-SSL Connection"	This field depends on the selected VPN connection type. Select the connection you want to associate to the VPN host object from the drop-down list.

The buttons at the bottom right of the editor panel depend on whether you add a new VPN host object or edit an existing object. For a newly configured object, click "Create" to add the object to the list of available VPN host objects or "Cancel" to discard your changes. To edit an existing object, click "Save" to store the reconfigured object or "Reset" to discard your changes. You can click "Close" to shut the editor panel as long as no changes have been made on it.

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

VPN Networks

Create a VPN network object that can be used to configure firewall rules for VPN Site-to-Site connections.

VPN Networks Overview

Navigate to "Desktop > Desktop Objects > VPN Networks" to display the list of VPN network objects that are currently defined on the system in the item list bar.

In the expanded view, the columns of the table display the "Name" of the VPN network object, the "Type" of VPN connection and the VPN connection that the VPN network belongs to. The buttons in the last column allow you to view and adjust the settings for an existing VPN network object, create an object based on a copy of an existing VPN network object or delete an object from the system.

For further information, see Chapter 3.2, "Icons and Buttons", on page 23.

VPN Networks Settings

The "VPN Network" settings allow you to configure the following elements:

Field	Description
"Name"	Specify a name for the VPN network object.
"Description"	Optional: Enter additional information on the VPN network object for internal use.
"Tags"	Optional: From the drop-down list, select the desktop tags that you want to assign to the VPN network object. For further information, see Chapter 3.4.4.4, "Desktop Tags", on page 114.
"Color"	Select the color to be used for this object on the desktop.
"VPN Connection Type"	Select the type of VPN connection by clicking the respective radio button.
"IPsec Connection"/"VPN-SSL Connection"	This field depends on the selected connection type. Select the VPN connection you want to associate to the VPN network object from the drop-down list.

The buttons at the bottom right of the editor panel depend on whether you add a new VPN network object or edit an existing object. For a newly configured object, click "Create" to add the object to the list of available VPN network objects or "Cancel" to discard your changes. To edit an existing object, click "Save" to store the reconfigured object or "Reset" to discard your changes. You can click "Close" to shut the editor panel as long as no changes have been made on it.

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

VPN User Groups

Create desktop objects for VPN user groups that can be used to create connections between multiple users and other desktop objects applying a common rule set to multiple VPN users. VPN user groups are displayed at the VPN node on the desktop.

VPN User Groups Overview

Navigate to "Desktop > Desktop Objects > VPN User Groups" to display the list of VPN user group objects that are currently defined on the system in the item list bar.

In the expanded view, the table displays the "Name" of the VPN user group object. The buttons in the last column allow you to view and adjust the settings for an existing VPN user group object, create an object based on a copy of an existing VPN user group or delete an object from the system.

For further information, see Chapter 3.2, "Icons and Buttons", on page 23.

VPN User Groups Settings

The "VPN User Group" settings allow you to configure the following elements:

Field	Description
"Name"	Specify a name for the VPN user group.
"Description"	Optional: Enter additional information on the VPN user group object for internal use.
"Tags"	Optional: From the drop-down list, select the desktop tags that you want to assign to the VPN user group object. For further information, see Chapter 3.4.4.4, "Desktop Tags", on page 114.
"Color"	Select the color to be used for this object on the desktop.
"User"	Select the users you want to add to the VPN user group. The left-hand list displays the users in the group. The right-hand list displays the users available in the system that are not part of the group. To add a user to the group, click ‹. Click « to add all available users at once. To remove a user from the group, click ›. Click » to remove all users at once. Use the "Filter" field to narrow down the list of users to display only entries that include a certain search string. Click ⊗ to display an unfiltered view of the list of users. **Note:** Users may be part of multiple VPN user groups.

The buttons at the bottom right of the editor panel depend on whether you add a new VPN user group or edit an existing group. For a newly configured group, click "Create" to add the group to the list of available VPN user groups or "Cancel" to discard your changes. To edit an existing group, click "Save" to store the reconfigured group or "Reset" to discard your changes. You can click "Close" to shut the editor panel as long as no changes have been made on it.

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

VPN Users

Create desktop objects for users that can be used in VPN connections. VPN users are displayed at the VPN node on the desktop.

The menu "Desktop > Desktop Objects > VPN Users" only serves to create desktop objects for users that already exist in the system. For information on how to add and manage users, see Chapter 3.4.1.9, "User Authentication", on page 47.

VPN Users Overview

Navigate to "Desktop > Desktop Objects > VPN Users" to display the list of VPN user objects that are currently defined on the system in the item list bar.

In the expanded view, the columns of the table display the "Object Name" of the VPN user object and the "User Name". The buttons in the last column allow you to view and adjust the settings for an existing VPN user object, create an object based on a copy of an existing VPN user object or delete an object from the system.

For further information, see Chapter 3.2, "Icons and Buttons", on page 23.

VPN Users Settings

The "VPN User" settings allow you to configure the following elements:

Field	Description
"Object Name"	Specify a name for the VPN user object.
"Description"	Optional: Enter additional information on the VPN user object for internal use.
"Tags"	Optional: From the drop-down list, select the desktop tags that you want to assign to the VPN user object. For further information, see Chapter 3.4.4.4, "Desktop Tags", on page 114.
"Color"	Select the color to be used for this object on the desktop.
"User Name"	Select the user to be used for the VPN user object. **Note:** Users may belong to multiple user objects.

The buttons at the bottom right of the editor panel depend on whether you add a new VPN user object or edit an existing object. For a newly configured object, click "Create" to add the object to the list of available VPN user objects or "Cancel" to discard your changes. To edit an existing object, click "Save" to store the reconfigured object or "Reset" to discard your changes. You can click "Close" to shut the editor panel as long as no changes have been made on it.

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

3.4.4.3 Desktop Rules

Use the "Desktop Rules" settings to display and modify the rules which are used to manage network traffic. For more detailed information on firewall rules, see Chapter 3.3, "Firewall Rule Settings", on page 25.

Navigate to "Desktop > Desktop Rules" to display the list of rules that are currently defined on the system.

The "Filter Settings" allow you to narrow down the list of rules to display only rules that include a certain search string. You can filter the contents by selecting the required options from the drop-down lists and/or entering search strings in the respective input fields. Click "Apply" to make use of the selected filter options. The list of firewall rules is adjusted to reflect your filter results. Click "Reset" to delete your selected filter options and display an unfiltered view of the list of rules.

The table columns of the rules list display the following information:

Column	Description
"Object A"	This column indicates the source object in the connection.
"Direction"	This column displays the direction in which the rule is applied.
"Object B"	This column indicates the destination object in the connection.
"Service"	This column displays the name of the service of the rule.

The buttons in the last column allow you to view and adjust the settings for an existing rule. Click ✎ and the "Connection" dialog opens. For more detailed information on how to create firewall rules and editing connections, see Chapter 3.3, "Firewall Rule Settings", on page 25 and Chapter 3.4.4.1, "Desktop Connections", on page 100.

To close the "Desktop Rules" panel and return to the desktop, click ✖ in the upper right corner of the panel.

3.4.4.4 Desktop Tags

Under "Desktop Tags" you can create a list of tags that you can assign to any of the desktop objects, except to the "Firewall" root node and the main nodes (for example "Intranet"). You can use these tags to display a filtered desktop for a customized overview of your configured network. For further information, see Chapter 3.1.3, "Desktop", on page 21.

When restoring a backup from a software version prior to v10.0, the layers and regions that were defined in the desktop configuration are converted to tags. All desktop objects which lie on a layer or region are tagged with the converted tags.

Desktop Tags Overview

Navigate to "Desktop > Desktop Tags" to display the list of desktop tags that are currently defined on the system in the item list bar.

In the expanded view, the first column of the table displays the "Name" of the desktop tag. The buttons in the last column allow you to view and adjust the settings for an existing desktop tag, create a tag based on a copy of an existing desktop tag or delete a tag from the system.

For further information, see Chapter 3.2, "Icons and Buttons", on page 23.

When you click an entry in the item list bar, the nodes of all desktop objects that this desktop tag is assigned to are highlighted on the desktop. When you click a desktop object node on the desktop with the "Desktop Tags" item list bar being open, the desktop tags that are assigned to this desktop object are highlighted in the item list bar.

Desktop Tags Settings

Under "Desktop > Desktop Tags", you can add a new or edit an existing desktop tag.

The "Desktop Tag" settings allow you to configure the following element:

Field	Description
"Name"	Enter a "Name" for the desktop tag.

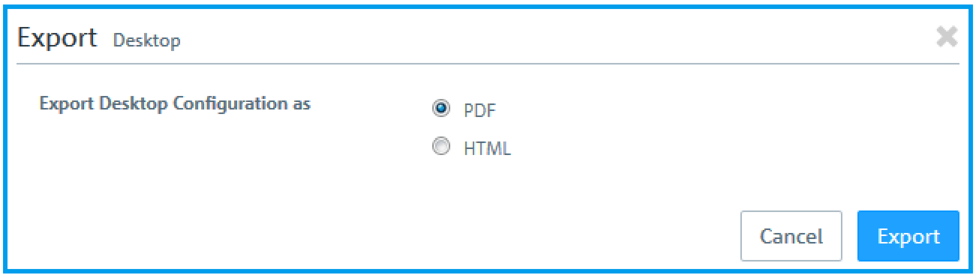
The buttons at the bottom right of the editor panel depend on whether you add a new desktop tag or edit an existing tag. For a newly configured desktop tag, click "Create" to add the tag to the list of available desktop tags or "Cancel" to discard your changes. To edit an existing desktop tag, click "Save" to store the reconfigured tag or "Reset" to discard your changes. You can click "Close" to shut the editor panel as long as no changes have been made on it.

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

3.4.4.5 Desktop Export

Navigate to "Desktop > Export" to create a report of the current desktop configuration and to transfer the report to your computer.

The "Export" panel allows you to choose between the PDF and the HTML file format by selecting the respective radio button.

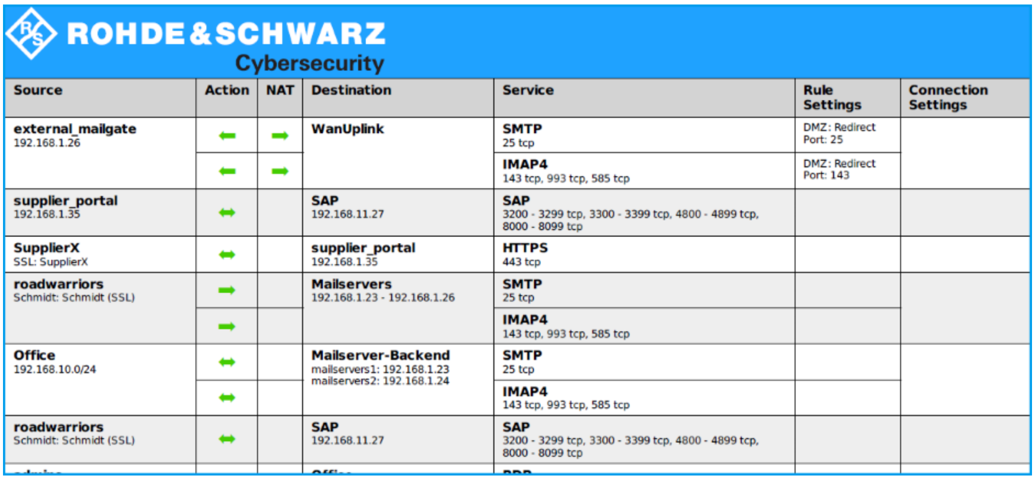


Export Desktop

Export Desktop Configuration as ● PDF ○ HTML

Figure 3-12: Desktop export — Selecting the file format for the report.

The export file contains a reproduction of the current desktop and a table containing all configured firewall rules, including additional information such as NAT, DMZ, IP addresses of host objects and the content of the description fields of the configured desktop objects and desktop connections.



Source	Action	NAT	Destination	Service	Rule Settings	Connection Settings
external_mailgate 192.168.1.26	⬅	➡	**WanUplink**	**SMTP** 25 tcp	DMZ: Redirect Port: 25	
	⬅	➡		**IMAP4** 143 tcp, 993 tcp, 585 tcp	DMZ: Redirect Port: 143	
supplier_portal 192.168.1.35	↔		**SAP** 192.168.11.27	**SAP** 3200 - 3299 tcp, 3300 - 3399 tcp, 4800 - 4899 tcp, 8000 - 8099 tcp		
SupplierX SSL: SupplierX	↔		**supplier_portal** 192.168.1.35	**HTTPS** 443 tcp		
roadwarriors Schmidt: Schmidt (SSL)	➡		**Mailservers** 192.168.1.23 - 192.168.1.26	**SMTP** 25 tcp		
	➡			**IMAP4** 143 tcp, 993 tcp, 585 tcp		
Office 192.168.10.0/24	↔		**Mailserver-Backend** mailservers1: 192.168.1.23 mailservers2: 192.168.1.24	**SMTP** 25 tcp		
	↔			**IMAP4** 143 tcp, 993 tcp, 585 tcp		
roadwarriors Schmidt: Schmidt (SSL)	↔		**SAP** 192.168.11.27	**SAP** 3200 - 3299 tcp, 3300 - 3399 tcp, 4800 - 4899 tcp, 8000 - 8099 tcp		

Figure 3-13: Desktop export — Sample report output.

Desktop objects will only be included if they are connected to other desktop objects.

If you want to create and transfer the export file, click "Export". Otherwise, click "Cancel" to shut the editor panel.

3.4.4.6 Services

Navigate to "Desktop > Services" to display the list of services and service groups that are currently defined on the system in the item list bar. Services are protocols or combinations of protocols and ports (if protocols use ports, such as TCP and UDP). When you click an entry in the item list bar, the system highlights the desktop objects and connections which use this service on the desktop. When you click an object on the desktop, the system highlights the services it uses in the list of services.

To create a user-defined service or a service group, click the ⊕ button at the top of the respective section in the item list bar.

For further information, see Chapter 3.2, "Icons and Buttons", on page 23.

The sections below provide further information on the various types of services and on service groups.

Predefined Services

Navigate to "Desktop > Services > Predefined Services" to display the list of predefined services that are currently defined on the system in the item list bar.

In the expanded view, the columns of the table display the "Name" of the service, indicate whether the service is used in a connection (green) or not (orange), and show the "Ports" (if applicable) and protocols that the service uses.

The predefined services are available for use in custom firewall rules (see "Setting Up a Firewall Rule" on page 26).

Service Groups

Use the "Service Groups" settings to group predefined and user-defined services in a service group. This way, you can assign a similar set of rules to different connections without having to add each service individually.

Service Groups Overview

Navigate to "Desktop > Services > Service Groups" to display the list of service groups that are currently defined on the system in the item list bar.

In the expanded view, the table columns display the "Name" of the service group and the number of "Services" belonging to this group. The buttons in the last column allow you to view and adjust the settings for an existing service group, create a new group based on a copy of an existing service group or delete a service group from the system.

For further information, see Chapter 3.2, "Icons and Buttons", on page 23.

Service Groups Settings

Use the "Service Groups" settings to configure service groups.

Under "Desktop > Services > Service Groups", you can add a new or edit an existing service group.

The "Service Group" panel displays the following information and allows you to configure the following elements:

Field	Description
"Name"	Enter a name for the service group.
"Services"	Along with the "Service Group" panel, a service selection list bar with all services that are currently defined on the system opens on the right side of the browser window. The list bar is subdivided into categories of services which serve a similar purpose. The categories can be collapsed and expanded by clicking the corresponding icon. For further information, see Chapter 3.2, "Icons and Buttons", on page 23. The "Filter" input field at the top of the service selection list bar helps you quickly find a particular service. As you type in the input field, R&S Unified Firewalls reduces the list to show only the services that contain the characters you are typing. Click ⊗ in the input field to delete the search string and display an unfiltered view of the list. To add an individual service to the service group, click ⊕ in front of the service in the service selection list bar. Click the ⊕ (Add filtered services) button directly below the header of a category to add all services belonging to that category at once. The services appear along with the ports and/or protocols assigned to them as entries in the list. To remove a service from the service group, click 🗑 next to the entry. The "Clear services" button at the bottom left of the panel allows you to delete all services from the group at once.

The buttons at the bottom right of the editor panel depend on whether you add a new service group or edit an existing group. For a newly configured service group, click "Create" to add the group to the list of available service groups or "Cancel" to reject the creation of a new service group. To edit an existing service group, click "Save" to store the reconfigured group or "Reset" to discard your changes. You can click "Close" to shut the editor panel as long as no changes have been made on it.

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

The service groups defined here are available for use in custom firewall rules (see "Setting Up a Firewall Rule" on page 26 for further information).

User-defined Services

If you require a port or protocol that is not covered by any of the predefined services (see "Predefined Services" on page 116), you can create a custom service to be applied to a connection.

Navigate to "Desktop > Services > User-defined Services" to display the list of user-defined services that are currently defined on the system in the item list bar.

User-defined Services Overview

In the expanded view, the columns of the table display the "Name" of the service, indicate whether the service is used in a connection (green) or not (orange), and show the

"Ports" used by the service. The buttons in the last column allow you to view and adjust the settings of a user-defined service, create a service based on a copy of an existing user-defined service or delete a user-defined service from the system.

For further information, see Chapter 3.2, "Icons and Buttons", on page 23.

User-defined Services Settings

Under "Desktop > Services > User-defined Services", you can add a new or edit an existing user-defined service.

The "User-defined Services " panel allows you to configure the following elements:

Field	Description
"Name"	Enter a name for the user-defined service.
"Ports/Protocols"	To extend the user-defined service to apply to traffic to certain ports/port ranges and/or protocols, click "Add" to open the "Edit Service" panel. On this panel, you can define the ports and protocols to be used: ● For TCP and UDP, specify individual ports or ranges to extend the service to apply to traffic being transmitted to a certain destination port. Use the "Port From" and "To" input fields to enter a value. The value can be any integer from `1` to `65535`. "Port From" and "To" form a port range. To enter an individual port, use the same value for both fields or leave "To" blank. ● Specify a protocol to apply the service to by selecting the corresponding checkbox. The buttons at the bottom right of the editor panel allow you to confirm your changes ("OK") and to discard your changes ("Cancel"). The "Edit Service" panel shuts automatically. The specified ports/port ranges and/or the protocol appear as a list entry. You can edit or delete single entries in the list by clicking the corresponding button next to an entry. For further information, see Chapter 3.2, "Icons and Buttons", on page 23.

The buttons at the bottom right of the editor panel depend on whether you add a new or edit an existing user-defined service. For a newly configured user-defined service, click "Create" to add it to the list of available services or "Cancel" to discard your changes. To edit an existing user-defined service, click "Save" to store the reconfigured service or "Reset" to discard your changes. You can click "Close" to shut the editor panel as long as no changes have been made on it.

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

The user-defined services defined here are available for use in custom firewall rules (see "Setting Up a Firewall Rule" on page 26).

3.4.5 UTM

The " 🛡 UTM" settings allow you to create and edit application filter profiles, define URL/content filters and to configure antivirus, email security settings, and proxies to protect your network.

3.4.5.1 Antivirus Settings

R&S Unified Firewalls protects your internal network from computer viruses using the integrated virus scanner provided by Avira.

The virus scanner is included in the UTM license. When you start R&S Unified Firewalls for the first time, the virus scanner runs as a test version for 30 days. When this period has expired, the virus scanner is deactivated automatically. For information about licensing, see Chapter 3.4.1.5, "License", on page 38.

Navigate to "UTM > Antivirus Settings" to open an editor panel to display, activate and adjust the virus scanner settings for your web and mail proxy.

The "Antivirus Settings" panel displays the following information and allows you to configure the following elements:

Field	Description
"License"	This field displays your license information for the virus scanner.
"Updates"	This field displays the date of the last attempt to update the virus scanner. Click the "Update now" link, to manually update the virus scanner.
"Last Successful Update"	This field displays the date and time of the last successful virus scanner update.

Scanner

On the "Scanner" tab, you can activate and deactivate the virus scanner for mail and HTTP(s)/FTP and adjust virus scanner settings.

Field	Description
I/◯	A slider switch indicates whether the virus scanner for emails, HTTP(s) and FTP is active (I) or inactive (◯). By clicking the slider switch, you can toggle the state of the respective service. This option is activated by default for all services.
"Enable Cloud Scan"	This checkbox is cleared by default. Select this checkbox to allow scanning of files in the Avira Protection Cloud. If the file is not identified as threat but classified as a risk by the local antivirus engine, the hash of the file will be sent to the Avira Protection Cloud. If the hash is known, the result will be passed back. If the hash is unknown, the file will be uploaded to the Avira Protection Cloud and scanned. **Note:** This will only work if the local antivirus engine classified the file's risk as high enough.
"Scan archived files"	This checkbox is pre-selected by default. Clear the checkbox if you do not want the virus scanner to check archived files for viruses.

Field	Description
"Block files if scan fails"	Optional: Select this checkbox to block emails and to cancel file downloads in HTTP(S) and FTP if the virus scanner did not successfully complete the scan. If an error occurs during the scan, the email is blocked and the recipient receives a notification. If this checkbox is cleared, the recipient receives a replacement email that contains the original email as an encrypted attachment along with the password required to decrypt it.
"Heuristic analysis"	Set the depth of the heuristic analysis by selecting an option from the drop-down list. Binary data are checked for code with similar characteristics to those of a virus or that could cause other damage. This method enables the recognition of subvariations of viruses which may have no signature of their own.
"Max. size of files to be scanned"	Define the maximum size (in megabyte) for an attachment to be scanned. Files exceeding the limit are not scanned. The default maximum file size is set to `15` megabytes.

Whitelist

On the "Whitelist" tab, you can add trusted hosts, servers and email addresses to a whitelist. Data transmitted from these hosts (via HTTP or FTP) and email addresses are excluded from virus scanning.

In the "Trusted HTTP/FTP Sources" input field, enter the IP address or the domain name of a trusted host or server.

You can use wildcards (* for whole words, ? for single characters) to include subdomains.

Click "Add" to add the host or server to the list.

You can edit or delete single entries in the list by clicking the corresponding button next to an entry. For further information, see Chapter 3.2, "Icons and Buttons", on page 23. If you edit an entry, a checkmark will appear on the right of the entry. Click the checkmark to apply your changes.

Click "↦ Export" to export your whitelist to the file system. Click "⇥ Import" to import a whitelist.

To set trusted email addresses, choose between the following options under "Trusted Mail Addresses":

- "Sender"
  All emails sent from this email address are excluded from virus scanning.
- "Recipient"
  All emails sent to this email address are excluded from virus scanning.
- "Sender/Recipient"
  All emails sent from OR sent to this email address are excluded from virus scanning.

Click "Add" to add the email address to the list.

You can edit or delete single entries in the list by clicking the corresponding button next to an entry. For further information, see Chapter 3.2, "Icons and Buttons", on page 23. If you edit an entry, a checkmark will appear on the right of the entry. Click the checkmark to apply your changes.

Updates

On the "Updates" tab, you can set up automatic updates for the antivirus scanner:

Field	Description
"Update Servers"	The default update server is preconfigured as: http://cybersecurity.rohde-schwarz.com/updateserver/av. You can add as many update servers as you like. To add an update server to the list, enter the IP address or the domain name of the update server and click "Add". You can edit or delete single entries in the list by clicking the corresponding button next to an entry. For further information, see Chapter 3.2, "Icons and Buttons", on page 23. If you edit an entry, a checkmark will appear on the right of the entry. Click the checkmark to apply your changes. **Note:** Update servers you added to the list are only contacted if the default update server is not available.
"Automatic Updates"	Enter the date and time for the first automatic update of the antivirus scanner. You can enter a date in the `MM/DD/YYYY` format or use the date picker to set a date. Set a time using the `hh:mm:ss` format. Specify the "Interval" for updating the antivirus scanner in hours. If you enter `0 h`, the update is performed immediately. Click "Add" to add the update schedule to the list. You can edit or delete single entries in the list by clicking the corresponding button next to an entry. For further information, see Chapter 3.2, "Icons and Buttons", on page 23. If you edit an entry, a checkmark will appear on the right of the entry. Click the checkmark to apply your changes.

If you modify these settings, click "Save" to store your changes or "Reset" to discard them. Otherwise, click "Close" to shut the editor panel.

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

ⓘ The antivirus settings for a certain protocol (HTTP, FTP, mail) are only applied to traffic which matches a rule with an active proxy for that protocol. Additionally, for HTTP and mail, the proxy must be activated as described in "HTTP Proxy Settings" on page 128 and Chapter 3.4.5.3, "Email Security", on page 123.

3.4.5.2 Application Filter

Application filters provide a way of filtering the network traffic based on the behavior of the data stream. This way, parts of an application, e.g. the Skype chat function, can be systematically filtered out, even if they are encrypted.

In some cases, for example with Skype, the application filter can only classify applications after a certain number of packets has been exchanged. This means that a first contact cannot be prevented. However, any subsequent packets are blocked.

Application Filter Settings

The "Application Filter Settings" allow you to activate and deactivate the application filter in general.

Field	Description
I/○	A slider switch indicates whether the application filter is active (I) or inactive (○). By clicking the slider switch, you can toggle the state of the application filter. The application filter is disabled by default.
"License"	Displays the license information for your application filter. For further information, see Chapter 3.4.1.5, "License", on page 38.

The buttons at the bottom right of the editor panel allow you to shut ("Close") the editor panel as long as no changes have been made and to store ("Save") or to discard ("Reset") your changes.

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

Application Filter Profiles

Navigate to "UTM > Application Filter > Profiles" to display the list of application filter profiles that are currently defined on the system in the item list bar.

In the expanded view, the columns of the table display the "Name" of the profile and the number of selected protocols and applications. The buttons in the last column allow you to view and adjust the settings for an existing application filter profile, create a profile based on a copy of an existing profile or delete a profile from the system.

For further information, see Chapter 3.2, "Icons and Buttons", on page 23.

The "Application Filter Profile" settings allow you to configure the following options:

Field	Description
"Profile Name"	Specify a name for the application filter profile.
"SSL Interception"	Select this checkbox to enable SSL interception. With SSL interception, R&S Unified Firewalls can evaluate the incoming traffic routed through SSL encrypted connections and apply the configured application filter profile to it.
"Rules"	Select the protocols and applications to be added to the profile. The table groups the protocols and applications by "Category". Use the "Filter" input field to narrow down the list of protocols and applications to display only entries that include a certain search string. Click ⊗ to display an unfiltered view of the list of protocols and applications. Click the › button next to a category to display the protocols and applications it contains along with a short description for each of them. Choose entire categories or single protocols or applications by selecting the corresponding checkboxes. Clear the checkbox next to a category or a protocol or an application to remove it from the application filter profile. To hide the protocols and applications, click the ⌄ button next to the category.

The buttons at the bottom right of the editor panel depend on whether you add a new application filter profile or edit an existing profile. For a newly configured application filter profile, click "Create" to add it to the list of available profiles or "Cancel" to discard your changes. To edit an existing application filter profile, click "Save" to store the reconfigured profile or "Reset" to discard your changes. You can click "Close" to shut the editor panel as long as no changes have been made on it.

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

The application filter profiles defined here are available for use in custom firewall rules where the selected protocols and applications are blacklisted or whitelisted (see Chapter 3.3, "Firewall Rule Settings", on page 25 and "Desktop Connections Settings" on page 100 for further information).

3.4.5.3 Email Security

Under "UTM > Email Security", you can manage your mail filter and antispam settings.

Antispam Settings

You can configure R&S Unified Firewalls to protect your system from email spam.

The spam filter is included in the UTM license. When R&S Unified Firewalls is started for the first time, the spam filter runs as a test version for 30 days. When this period has expired, the spam filter is deactivated automatically. For further information on licensing, see Chapter 3.4.1.5, "License", on page 38.

Navigate to "UTM > Email Security > Antispam Settings" to open an editor panel to display, activate and adjust the spam filter settings.

The "Antispam Settings" panel displays the following information and allows you to configure the following elements:

Field	Description
I/○	A slider switch indicates whether antispam is active (I) or inactive (○). By clicking the slider switch, you can toggle the state of this service. This option is activated by default.
"License"	This field displays your license information for the commercial spam filter.
"Spam Detection"	Select one of the following options by clicking the corresponding button: • "Confirmed" – Emails containing known and verified spam patterns are classified as spam. • "Bulk" – Additionally to `Confirmed`, emails from accounts known to send bulk emails (mass mailing) are classified as spam (default setting). • "Suspect" – Additionally to `Confirmed` and `Bulk`, emails from accounts sending suspicious amounts of emails are classified as spam.
"Spam Tag"	Specify how spam is tagged by selecting one of the following options: • "Header" – The original email is marked as spam in the header. • "Subject" – The original email is marked as spam in the header and the subject is changed according to the subject formatting (default setting). • "Attachment" – An email detected as spam is attached to a new email that is marked as spam both in the subject (according to the subject formatting) and in the header.
"Subject Tag format"	Specify how emails that are identified as spam are tagged. The subject tag can be any text and contain the variables %SUBJECT% (original subject of the spam email), %SPAMCLASS%, and %SPAMCLASSNUM% (spam category). By clicking ↺, the subject tag format is set to the default `*****SPAM***** [%SUBJECT%]`.
"Mail Lists"	You can specify a blacklist and/or a whitelist by adding as many email addresses as you like into the respective list. Both mail lists can be applied at the same time. There are two options to add email addresses to either list: • Email addresses can be manually added by entering an email address in the input field under the corresponding list and clicking "Add". • Email addresses can be imported from a text file by clicking "⇥ Import" on the right under the corresponding list and opening the file. The default maximum file size for imports is 1 megabyte. Each non-empty line of the selected text file adds an entry to the corresponding list. If a sender's email address matches both lists, the email is treated as a whitelisted item. You can edit or delete single entries in the lists by clicking the corresponding button next to an entry. For further information, see Chapter 3.2, "Icons and Buttons", on page 23. You can export a complete mail list as a text file to the local disk by clicking "↦ Export" on the right under the corresponding list. **Tip:** The email addresses in either mail list can contain wildcards: * for whole words, ? for single characters.

The buttons at the bottom right of the editor panel allow you to shut ("Close") the editor panel as long as no changes have been made and to store ("Save") or to discard ("Reset") your changes.

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

The antispam settings for the Mail protocol defined here are only applied to traffic which matches a rule with an active proxy for that protocol. Additionally, for Mail the proxy must be activated as described under "Mail Filter Settings" on page 125.

Mail Filter Settings

Under "UTM > Email Security > Mail Filter Settings", you can activate the mail proxy on your R&S Unified Firewalls. Once the mail proxy is enabled, you can filter emails by their destination address. If filtered, these mails will not be forwarded to the recipient and/or the mail server.

The "Mail Filter Settings" settings allow you to configure the following elements:

Field	Description
I/○	A slider switch indicates whether the mail proxy is active (I) or inactive (○). By clicking the slider switch, you can toggle the state of this service. The mail proxy is deactivated by default.
"Filter Mode"	Select the button with the filter mode you desire. If "Blacklist" (default setting) is selected, emails of all addresses in the blacklist (see below) will never be forwarded to the mail server. Selecting "Whitelist" will forward only addresses in the whitelist (see below) to the mail server.
"Action"	Select the button with the action you wish to be applied to the filtered emails. While "Reject emails" (default setting) will reject unwanted emails with an RFC-compliant answer, "Delete emails" will drop unwanted emails, making it appear to the sender as if the email has reached the mail server. **Important:** The "Delete emails" option is NOT RFC-compliant. Misconfiguration can lead to the deletion of important emails.
"Blacklist"/"Whitelist"	Depending on the selected filter mode, you can add as many email addresses as you like to a blacklist or a whitelist. There are two possibilities to add email addresses to either list: ● Email addresses can be manually added by entering an email address in the input field and clicking "Add". ● Email addresses can be imported from a text file by clicking "⇥ Import" and opening the file. The default maximum file size for imports is 1 megabyte. Each non-empty line of the selected text file adds an entry to the list. You can edit or delete single entries in the list by clicking the corresponding button next to an entry. For further information, see Chapter 3.2, "Icons and Buttons", on page 23. You can export the complete mail filter list as a text file to the local disk by clicking "↦ Export". **Tip:** The email addresses in either mail filter list can contain wildcards: * for whole words, ? for single characters (for example `*@example.*`).

The buttons at the bottom right of the editor panel allow you to shut ("Close") the editor panel as long as no changes have been made and to store ("Save") or to discard ("Reset") your changes.

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

Only if the mail proxy has been activated, the other mail filter, antispam and antivirus settings will have an impact. For more information, see "Antispam Settings" on page 123 and Chapter 3.4.5.1, "Antivirus Settings", on page 119.

If you use SSL inspection both in the mail filter and in firewall rules, you need to add your CA to the truststore of your R&S Unified Firewalls and of your client machines.

3.4.5.4 IDS/IPS

The Intrusion Detection/Prevention System (»IDS/IPS«) maintains a database of known threats to protect the computers on your network from a wide range of hostile attack scenarios, generate alerts when any such threats are detected and terminate communication from hostile sources. The network threat detection and prevention system is based on Suricata.

The threat database consists of an extensive rule set provided by ProofPoint. The rule set includes blacklisted IPs, malware communication patterns, network scan patterns, brute force attack patterns and many more. In IDS mode, the IDS/IPS engine only generates alerts if the traffic matches one of the rules. In IPS mode, the IDS/IPS engine generates alerts and also blocks malicious traffic. Once you activate IDS/IPS on R&S Unified Firewalls, all rules are activated by default. If any of the services in the network are blocked by the IDS/IPS, you can configure the IDS/IPS engine to ignore the rule that caused the false-positive. For detailed information on the categories, see Emerging Threats FAQ.

IDS/IPS is included in the UTM license. When R&S Unified Firewalls is started for the first time, IDS/IPS runs as a test version for 30 days. When this period has expired, IDS/IPS is deactivated automatically. For further information on licensing, see Chapter 3.4.1.5, "License", on page 38.

Navigate to "UTM > IDS/IPS" to open an editor panel to display, activate and adjust the IDS/IPS settings.

The "IDS/IPS" panel allows you to configure the following elements:

Field	Description
I/○	A slider switch indicates whether IDS/IPS is active (I) or inactive (○). By clicking the slider switch, you can toggle the state of IDS/IPS. IDS/IPS is deactivated by default.
"IDS/IPS License"	This field displays your license information for IDS/IPS.
"Mode"	Select the desired IDS/IPS mode by clicking the respective radio button. The mode can be one of the following: ● "IDS (log events)" – This mode is used to simply log events, no other action is carried out. ● "IPS Drop (drop and log packets)" – When an event is triggered, the packets which are related to this event are dropped without any response to the sender. A log entry is created. ● "IPS Reject (reject and log packets)" – When an event is triggered, the packets which are related to this event are rejected with a response to the sender. A log entry is created.

On the "Rules" tab:

Field	Description
"SID"	Specify the IDS/IPS rules which you want to be ignored. You can add as many rules as you like. Enter the unique signature ID (SID) of a rule and click "Add" to put the rule on the list. You can edit or delete single entries in the list by clicking the corresponding button next to an entry. For further information, see Chapter 3.2, "Icons and Buttons", on page 23.
"Description"	Optional: Enter additional information regarding the IDS/IPS rule to be ignored in the input field. If you leave the text field blank, it will be automatically filled as soon as your R&S Unified Firewalls finds a rule matching the signature ID.

Alternatively, you can add IDS/IPS rules which you want to be ignored by selecting the respective rules in the system log. For further information, see "System Log" on page 66.

The "Clear Ignored Rules" button at the bottom left of the panel allows you to delete all ignored IDS/IPS rules from the tab at once.

On the "Updates" tab, you can set up profiles for automatic IDS/IPS updates:

Field	Description
"From"	Enter the date and time for the first automatic IDS/IPS update. You can enter a date in the `MM/DD/YYYY` format or use the date picker to set a date. Set a time using the `hh:mm:ss` format.
"Interval"	Specify the interval for updating IDS/IPS in hours. If you enter `0` hours, the update is performed immediately.

You can add as many automatic update profiles as you like. Click "Add" to put the profile on the list. You can edit or delete single entries in the list by clicking the corresponding button next to an entry. For further information, see Chapter 3.2, "Icons and Buttons", on page 23.

If you modify the settings, click "Save" to store your changes or "Reset" to discard them. Otherwise, click "Close" to shut the editor panel.

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

3.4.5.5 Proxy

Under "UTM > Proxy", you can manage your HTTP(S), mail and VoIP proxy settings.

HTTP Proxy Settings

R&S Unified Firewalls uses the Squid proxy. This proxy serves as an interface to the content filter and the antivirus scanner (see Chapter 3.4.5.7, "URL/Content Filter", on page 133 and Chapter 3.4.5.1, "Antivirus Settings", on page 119).

Under "UTM > Proxy > HTTP Proxy Settings", you can configure the HTTP(S) proxy for your R&S Unified Firewalls.

The HTTPS proxy serves as a man-in-the-middle. For this purpose, it establishes a connection to the web server, generates a fake certificate for the website using its own HTTPS Proxy CA, and uses this fake certificate to establish a connection to the browser. This way, the proxy can analyze the traffic, apply the URL/content filter and scan for viruses.

When the HTTPS proxy is active, make sure that the DNS server of R&S Unified Firewalls is able to correctly resolve the domains to be accessed.

Import the HTTPS Proxy CA of your R&S Unified Firewalls as a trusted CA into the browsers of all clients.

Field	Description
I/○	A slider switch indicates whether the HTTP(S) proxy is active (I) or inactive (○). By clicking the slider switch, you can toggle the state of this service regardless of the configured proxy modes. The HTTP(S) proxy is deactivated by default. **Note:** Activating or deactivating the HTTP(S) proxy will also activate or deactivate the FTP proxy.
"Plain HTTP Proxy"	Select the desired mode of operation for the plain HTTP proxy by clicking the respective radio button. You can choose from the following options: ● "Disable Proxy" Disables the HTTP proxy. ● "Transparent" R&S Unified Firewalls automatically forwards all requests which arrive on port 80 (HTTP) through the proxy (default setting). ● "Intransparent" The HTTP proxy of R&S Unified Firewalls must explicitly be addressed on port 10080.
"HTTPS Proxy"	Select the desired mode of operation or disable the HTTPS proxy by clicking the respective radio button. You can choose from the following options: ● "Disable Proxy" Disables the HTTPS proxy. ● "Transparent" R&S Unified Firewalls forwards all requests which arrive on port 443 (HTTPS) automatically through the proxy (default setting). ● "Intransparent" The HTTPS proxy of R&S Unified Firewalls must explicitly be addressed on port 10443.
"Proxy CA"	The CA is used by the HTTPS proxy to generate the fake certificates. Depending on the certificate type, the R&S Unified Firewalls will make a proposal on which certificates are useful and which are not. **Note:** The CA will only be shown if "HTTPS Proxy" is set to "Transparent" or "Intransparent".
"Client Authentication"	Only available if "Plain HTTP Proxy" or "HTTPS Proxy" are set to "Intransparent": Select this checkbox to enable HTTP(S) client authentication using the R&S Unified Firewalls user management. **Note:** When you enable "Client Authentication", the FTP proxy will be disabled. In that case, a warning will be displayed. **Note:** The proxy can only process HTTP data packets. If a program tries to transmit data packets of other protocols through this port, the packets are blocked.
"Whitelist"	You can specify a list of domains that you want to be excluded from SSL interception, antivirus scanning and URL filtering. Domains in the whitelist are accepted by the HTTPS proxy without analysis and become directly available to the users' browser. No certificates are created. This is necessary for services which employ strict Certificate Pinning, such as Windows Update (URL: `windowsupdate.com`). You can add as many domains as you like. Enter a domain in the input field and click ⊕ to put the domain on the list. You can edit or delete single entries in the list by clicking the corresponding button next to an entry. For further information, see Chapter 3.2, "Icons and Buttons", on page 23. **Tip:** The domains can contain wildcards: * and . for whole words, ? for single characters.

If you modify these settings, click "Save" to store your changes or "Reset" to discard them. Otherwise, click "Close" to shut the editor panel.

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

Mail Proxy Settings

With the Mail proxy, you can use R&S Unified Firewalls as a proxy for your emails.

Under "UTM > Proxy > Mail Proxy", you can configure the mail proxy for your R&S Unified Firewalls:

Field	Description
I/○	A slider switch indicates whether the mail proxy is active (I) or inactive (○). By clicking the slider switch, you can toggle the state of the proxy regardless of the configured settings. The mail proxy is activated by default.
"Verify Server Certificates"	Select this checkbox if you want the mail proxy of R&S Unified Firewalls to validate upstream server certificates.
"Use StartTLS (SMTP)"	Select this checkbox to allow StartTLS for SMTP proxy connections.
"Certificates"	You can select the type of certificate you want to use for the email proxy by clicking the respective radio button. You can choose from the following options: ● "Create certificates automatically" R&S Unified Firewalls dynamically creates certificates for each mail server. ● "Select certificate" R&S Unified Firewalls uses one certificate for all servers. From the "Proxy Certificate" drop-down list, select a certificate. **Note:** Only non-CA certificates with private key are allowed.

If you modify these settings, click "Save" to store your changes or "Reset" to discard them. Otherwise, click "Close" to shut the editor panel.

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

VoIP Proxy Settings

With the VoIP proxy, you can use R&S Unified Firewalls as proxy for VoIP connections.

Under "UTM > Proxy > VoIP Proxy Settings", you can configure the VoIP proxy for your R&S Unified Firewalls:

Field	Description
"Internal Net"	From the drop-down list, select your local network interface that is to be used to make phone calls.
"Internet Connection"	Select the Internet connection from the drop-down list which R&S Unified Firewalls uses to forward the VoIP connections.
"Activate SIP Proxy"	Select this checkbox if you want R&S Unified Firewalls to serve as VoIP proxy for the SIP. It can be reached on port 5060.
"Forward data to an External SIP Proxy"	Select this checkbox to forward VoIP data in the SIP to an external SIP proxy.

Field	Description
"Address of External Proxy"	Enter the IP address of the external SIP proxy.
"Port"	Enter the port of the external SIP proxy.

To use the VoIP proxy, you have to enter the IP address of your R&S Unified Firewalls with port 5060 in your VoIP devices. For further details, see the documentation of your VoIP terminal devices.

If you modify these settings, click "Save" to store your changes or "Reset" to discard them. Otherwise, click "Close" to shut the editor panel.

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

3.4.5.6 Reverse Proxy

Under "UTM > Reverse Proxy" you can manage your backends, frontends and reverse proxy settings.

A reverse proxy is useful when a public website is hosted on your own network.

When the reverse proxy is active, the R&S Unified Firewalls device accepts the website request from external networks (e.g. the Internet). Then, it will relay it according to your configuration to on or more of your internal webservers.

The R&S Unified Firewalls reverse proxy allows you to host multiple domains on one IP address. Additionally, it provides load balancing and failover when you use multiple internal servers.

Reverse Proxy Settings

The "UTM > Reverse Proxy > Reverse Proxy Settings" allow you to activate and deactivate the reverse proxy in general.

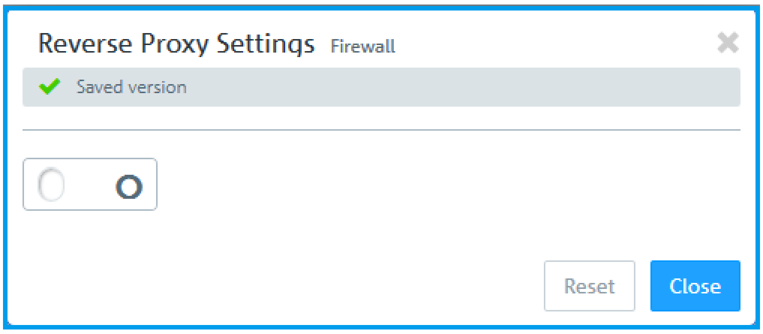


Figure 3-14: Reverse proxy settings — activate or deactivate the reverse proxy.

Field	Description
I/○	A slider switch indicates whether the reverse proxy settings are active (I) or inactive (○). By clicking the slider switch, you can toggle the state of the reverse proxy. The reverse proxy is disabled by default.

Backends

Navigate to "UTM > Reverse Proxy > Backends" to define at least one backend with one server. A backend consists of one or more internal webservers serving your website.

The "Reverse Proxy Backend" panel displays the following information and allows you to configure the following elements:

Field	Description
"Name"	Enter a name for the backend.
"SSL"	Select this checkbox to enable SSL. If SSL is enabled, the connection between the reverse proxy and the backend will be encrypted.
"Server"	Assign one or more servers to the backend. Enter a server address. Click ⊕ to add the IP address of the server to the list.

The buttons at the bottom right of the editor panel allow you to cancel ("Cancel") the process or to create ("Create") a new backend.

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

Frontends

Navigate to "UTM > Reverse Proxy > Frontends" to configure your frontends.

You have to define at least one backend with at least one server to realize the configuration.

After having created a backend, you can create a frontend in the "Reverse Proxy Frontend". Each configured frontend represents one website with its external IP address, port, domain and certificate (if SSL is enabled).

The "Reverse Proxy Frontend" panel displays the following information and allows you to configure the following elements:

Field	Description
I/○	A slider switch indicates whether the reverse proxy frontend is active (I) or inactive (○). By clicking the slider switch, you can toggle the state of the reverse proxy. The reverse proxy is enabled by default.
"Domain or IP address"	Enter the name of the domain or the IP address the frontend is assigned to.

Field	Description
"Connection"	Select a connection. You can choose a network connection as well as a PPP connection.
"Port"	Configure the external listen port for the reverse proxy, e.g. the port that is reachable from external networks.
"SSL"	Select this checkbox to enable SSL. If SSL is enabled, the reverse proxy will serve the website with SSL encryption, using the configured certificate for its authentication.
"Certificate"	Select a certificate with a private key. This option is only available if SSL is enabled.
"Proxy Paths"	Select a configured backend. Enter a URL path. The URL path has to be absolute, i.e. it has to start with `/`. You can now forward requests matching the URL parameters to the configured backend.
"Blocked Paths"	Block requests which match the URL parameter. Enter a URL path. The URL path has to be absolute, i.e. it has to start with `/`.

The buttons at the bottom right of the editor panel allow you to cancel ("Cancel") the process or to create ("Create") a new frontend.

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

3.4.5.7 URL/Content Filter

URL and content filters determine which websites are available to computers on the protected network.

The URL filter function of R&S Unified Firewalls checks Internet addresses (URL, Uniform Resource Locator consisting of server name, path and filenames) received in the HTTP traffic for allowed and/or not allowed terms according to their classification in the black- and whitelists.

A »blacklist« approach defines a list of sites to block and grants access to all sites that have not been explicitly forbidden. For example, if the URL of a website is on a blacklist, access to this site is blocked. Therefore, with the category "Ordering" being blacklisted, the URL `http://www.amazon.de` is blocked.

A »whitelist« approach can be used to limit access to a list of sites that have specifically been approved for usage and block all others. For example, if the subcategory "Shopping" is on the blocking list but you want to allow access to the URL `http://www.amazon.de`, this URL must be entered into a whitelist.

If websites do not contain any verifiable terms in their URLs, a URL filter alone is not sufficient. Therefore, R&S Unified Firewalls also filters the HTTP data communication by the content of the websites. Similar to a search engine, the content filter searches websites available on the Internet, analyzes and categorizes them and compiles the results in a database.

To use the URL and content filter, the HTTP proxy is essential. The HTTP data communication of a connection can only be filtered by URL lists and content if the HTTP proxy is activated for this connection in the rules editor.

The URL and content filters defined here are available for use in custom firewall rules (see Chapter 3.3, "Firewall Rule Settings", on page 25 for further information).

For more detailed information on URL/content filters, see the following sections.

URL/Content Filter Settings

Navigate to "UTM > URL/Content Filter > Settings" to configure the URL and content filter on your R&S Unified Firewalls.

Field	Description
"Content Filter License"	This field displays your license information for the content filter.
"URLs"	Select this checkbox to exclude sections behind a `?` (which serves to transfer variable values in PHP) from blacklists and whitelists.
"Safesearch"	Select this checkbox to automatically configure the setting `SafeSearch=strict` for searches using the search engines Google, Bing and Yahoo to hide any adult content in search requests. This setting cannot be changed by the users. **Note:** SafeSearch only works if the HTTPS proxy is active as most search engine providers use encrypted HTTPS connections on their websites.
"Duration of override by user"	When a website is blocked, you can override the blocking mechanisms of the content filter for a certain timespan. Enter the timespan in minutes for a content filter category of a profile to be deactivated. The default value is `5` minutes. **Note:** Only the current URL/content filter category of a profile is overridden to non-blocking for a defined period of time (see "URL/Content Filter Overview" on page 134 for further information).

The buttons at the bottom right of the editor panel allow you to shut ("Close") the editor panel as long as no changes have been made and to store ("Save") or to discard ("Reset") your changes.

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

URL/Content Filter Overview

Navigate to "UTM > URL/Content Filter > URL/Content Filter" to display the URL and content filters currently defined on the system.

In the expanded view, the columns of the table display the "Name" of the filter and the number of selected content filter, blacklist and whitelist entries. The buttons in the last column allow you to view and adjust the settings for an existing URL and content filter, create a filter based on a copy of an existing filter or delete a filter from the system.

For further information, see Chapter 3.2, "Icons and Buttons", on page 23.

URL/Content Filter Settings

The settings allow you to configure the following options:

Field	Description
"Name"	Specify a name for the URL and content filter.
"Override by user"	Select this checkbox to mark a content filter profile as overrideable. You can set the duration as described in "URL/Content Filter Settings" on page 134. **Note:** This option is only available for non-standard profiles.

Content Filter

In the "Content Filter" section, you can determine which websites should be available to users on the network and which should be blocked.

Click the › button next to a category to display its subcategories. Choose entire categories or single subcategories by selecting the corresponding checkboxes. Clear the checkbox next to a category or a subcategory to remove it from the blacklist or whitelist. To hide the subcategories, click the ⌄ button next to the category.

URL Filter

In the "URL Filter" section, you can blacklist and/or whitelist filters for URLs.

Field	Description
"Blacklist" /"Whitelist"	You can specify a blacklist and/or a whitelist by adding as many terms as you like to the respective list. If both lists are applied at the same time, the whitelist has the higher priority. There are two options to add terms to either list: ● Search terms can be manually added by entering a term in the input field under the corresponding list and clicking "Add". ● Search terms can be imported from a text file by clicking "⇥ Import" on the right under the corresponding list and opening the file. The default maximum file size for imports is 1 megabyte. Each non-empty line of the selected text file adds an entry to the corresponding list. You can edit or delete single entries in the lists by clicking the corresponding button next to an entry. For further information, see Chapter 3.2, "Icons and Buttons", on page 23. You can export a complete term list as a text file to the local disk by clicking "↦ Export" on the right under the corresponding list. **Tip:** The terms in either list can contain wildcards: * for whole words, ? for single characters.

To create the "Blacklist" or "Whitelist", you can enter the search terms directly or use regular expressions (RegEx):

RegEx	Description	Example
`.`	Placeholder for any single character.	`ho.me` - e.g. home, hole
`*`	Any number of repetitions of the character.	`hom*` - e.g. hom, homm
`.*`	Any number of characters.	`ho.*e` - e.g. home, house

RegEx	Description	Example
^	Start of a line.	`^home` - home only at the start of the line
$	End of a line.	`home$` - home only at the end of the line

The buttons at the bottom right of the editor panel depend on whether you add a new URL and content filter or edit an existing filter. For a newly configured URL and content filter, click "Create" to add it to the list of available filters or "Cancel" to discard your changes. To edit an existing URL and content filter, click "Save" to store the reconfigured filter or "Reset" to discard your changes. You can click "Close" to shut the editor panel as long as no changes have been made on it.

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

3.4.6 VPN

Use the "🔒 VPN" settings to configure R&S Unified Firewalls for use as a virtual private network server to provide *Client-to-Site* (C2S) VPN connections, enabling remote computers to securely access resources on the local network (using IPsec and VPN SSL); and as a *Site-to-Site* (S2S) VPN gateway that creates a secure communication channel between two remote networks via the Internet (using IPsec and VPN SSL).

Client-to-Site VPN Connections

With a Client-to-Site VPN connection, you can reach the corporate network from outside. Authentication is either effected with IPsec using issued certificates or a so-called PSK (preshared key) or with VPN SSL using certificates.

IPsec Client-to-Site and VPN SSL Client-to-Site connections can be operated in one of two modes, depending on the client settings:

- In *split tunnel mode*, only communication between the client and the internal network (for example, a corporate network) is routed through R&S Unified Firewalls. Clients are able to reach devices on the internal network through the tunnel. Packets intended for other destinations (such as the Internet) are not routed through R&S Unified Firewalls.
  For example, suppose a user utilizes a remote access VPN software client connecting to a corporate network using a hotel wireless network. The user with split tunneling is able to connect to file servers, database servers, mail servers and other services on the corporate network through the VPN connection. When the user connects to Internet resources (websites, FTP sites and so on), the connection request goes directly out the gateway provided by the hotel network.
- In *full tunnel mode*, all traffic is routed through R&S Unified Firewalls, including communication with sites on the Internet.
  For example, full tunneling will no longer allow the user to use hotel networks to access the Internet. All traffic which is sent out by the client while the VPN connection is active will be sent to the firewall.

IPsec C2S connections are established using a standard VPN client or the "R&S Cybersecurity VPN Client". For more information, see "IPsec Connections Settings" on page 140.

VPN SSL C2S connections are established using a standard VPN client or the "R&S Cybersecurity VPN Client". For more information, see "VPN SSL Connections Settings" on page 145.

Site-to-Site VPN Connections

With a Site-to-Site connection, two locations are connected using an encrypted tunnel to a virtual network and exchanging data through this tunnel. The two locations can have fixed IP addresses. Authentication is either effected with IPsec using issued certificates or a so-called PSK (preshared key) or with VPN SSL using certificates.

IPsec

IPsec (Internet Protocol Security) is a set of protocols which works at the network layer or the data link layer and secures the exchange of packets through untrusted networks (such as the Internet) by authenticating and encrypting each IP packet of a communication session. IPsec meets the highest security requirements.

VPN SSL

VPN over SSL offers a fast and secure opportunity to tie down a Road Warrior. The biggest advantage of VPN SSL is that all the data traffic runs over a TCP or UDP port and no further special protocols are required, contrary to IPsec.

Before setting up VPN connections, make sure that you have installed the necessary certificates as described under Chapter 3.4.7, "Certificate Management", on page 147.

3.4.6.1 IPsec Settings

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

You need two VPN IPsec capable servers for an IPsec Site-to-Site connection. For a Client-to-Site connection, you need separate client software.

Your R&S Unified Firewalls is able to create and use secured connections using the IPsec protocol suite. This is based on ESP in tunnel mode. The key exchange can be accomplished using version 1 of the IKE protocol or using the newer IKEv2, selectively using Preshared Keys or using X.509 compliant certificates. Using IKEv1, it is possible to authenticate using XAUTH. The firewall server is also capable of serving IPsec-secured L2TP.

Under "VPN > IPsec Settings", you can activate IPsec and configure the Layer 2 Tunneling Protocol (L2TP) settings on your R&S Unified Firewalls:

Field	Description
I/○	A slider switch indicates whether the IPsec is active (I) or inactive (○). By clicking the slider switch, you can toggle the state.
"Start IP"	Enter the start IP address of the address range from which IP addresses are assigned to clients. This address range must not overlap any of your local networks.
"End IP"	Enter the end IP address of the address range from which IP addresses are assigned to clients. This address range must not overlap any of your local networks.
"Local IP"	Enter the local IP address which R&S Unified Firewalls uses for communication with the clients.
"DNS IP"	Optional: Enter the DNS server address which is transmitted to the client when the connection is established.
"WINS IP"	Optional: Enter the WINS server address which is transmitted to the client when the connection is established.

The buttons at the bottom right of the editor panel allow you to shut ("Close") the editor panel as long as no changes have been made and to store ("Save") or to discard ("Reset") your changes.

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

3.4.6.2 VPN SSL Settings

VPN over SSL offers a fast and secure opportunity to tie down a Road Warrior. The biggest advantage of VPN SSL is the fact that all the data traffic runs over a TCP or UDP port and no further special protocols are required.

R&S Unified Firewalls allows you to provide VPN access to remote client computers (C2S, »Client-to-Site«) or to create a secure connection between two remote networks (S2S, »Site-to-Site«) via the VPN SSL protocol.

Under "VPN > VPN-SSL Settings", you can activate VPN SSL and configure its general settings on your R&S Unified Firewalls:

Field	Description
I/○	A slider switch indicates whether VPN SSL is active (I) or inactive (○). By clicking the slider switch, you can toggle the state.
"Host certificate"	Select a host certificate that R&S Unified Firewalls uses in all VPN SSL connections.
"DNS"	Optional: Enter the DNS server which is to be used by clients in a Client-to-Site connection for the time the connection is established.
"WINS"	Optional: Enter the WINS server which is to be used by clients in a Client-to-Site connection for the time the connection is established.
"Timeout"	Specify the timeout of in seconds. The tunnel is disconnected if there is no traffic until the timeout expires. The default setting is `0`, which means that the tunnel is maintained permanently.

Field	Description
"Log Level"	Define the log level. A log level of 5 is recommended for troubleshooting.
"Routes"	Enter routes for the VPN SSL tunnels that the clients or the remote end establishing the connection are to create. These routes then apply to all VPN SSL connections. Click "Add" to add the route to the list. You can edit or delete single entries in the list by clicking the corresponding button next to an entry. For further information, see Chapter 3.2, "Icons and Buttons", on page 23. **Note:** If you edit an entry, a check mark appears on the right of the entry. Click the check mark to apply your changes.

On the "Client-to-Site" tab:

Field	Description
"Protocol"	Select the protocol to be used by clicking the respective radio button.
"Port"	Specify the VPN SSL listening port number to be used for incoming connections. **Note:** The same port number must 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 any of your local networks.
"Encryption algorithm"	From the drop-down list, select the encryption algorithm to be used in VPN SSL C2S connections.
"Key renegotiation"	A VPN SSL connection renews the session key while the connection is established to increase security. Specify this rekeying interval (in seconds).
"Compression"	Optional: Clear this checkbox to deactivate LZO (Lempel-Ziv-Oberhumer, a lossless data compression algorithm) compression. This checkbox is selected by default.

On the "Site-to-Site" tab:

Field	Description
"Protocol"	Select the protocol to be used by clicking the respective radio button.
"Port"	Specify the VPN SSL listening port number to be used for incoming connections. **Note:** The same port number must be specified on the remote site.
"Address pool"	Specify the address range from which IP addresses are used in S2S connections. This address range must not overlap any of your local networks.
"Encryption algorithm"	From the drop-down list, select the encryption algorithm to be used in VPN SSL S2S connections.
"Key renegotiation"	A VPN SSL connection renews the session key while the connection is established to increase security. Specify this rekeying interval (in seconds).
"Compression"	Optional: Clear this checkbox to deactivate LZO (Lempel-Ziv-Oberhumer, a lossless data compression algorithm) compression. This checkbox is selected by default.

The buttons at the bottom right of the editor panel allow you to shut ("Close") the editor panel as long as no changes have been made and to store ("Save") or to discard ("Reset") your changes.

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

3.4.6.3 VPN Connections

Under "VPN Connections", you can create and manage VPN connections.

IPsec Connections

R&S Unified Firewalls allows you to provide VPN access to remote clients via IPsec (IPsec Client-to-Site) and to create a secure tunnel between two remote networks (IPsec Site-to-Site).

IPsec Connections Overview

Navigate to "VPN > VPN Connections > IPsec Connections" to display the list of IPsec connections that are currently defined on the system in the item list bar.

In the expanded view, the columns of the table display the "Name" and the "Type" of the IPsec connection. Furthermore, the columns display the authentication method selected for this connection. The buttons in the last column allow you to view and adjust the settings for an IPsec connection or to delete a connection from the system.

For further information, see Chapter 3.2, "Icons and Buttons", on page 23.

IPsec Connections Settings

Under "VPN > VPN Connections > IPsec Connections", you can add or edit an existing IPsec connection.

The "IPsec Connections" settings allow you to configure the following elements:

Field	Description
I/○	A slider switch indicates whether the IPsec connection is active (I) or inactive (○). By clicking the slider switch, you can toggle the state of the connection. A new connection is enabled by default.
"Name"	Enter a unique name for the connection. It must consist of 1 to 63 alphanumeric characters and underscores.
"Connection type"	Select the type of the connection by selecting the respective radio button. You can choose from the following three types: ● "R&S Cybersecurity VPN Client" – A C2S connection with the R&S Cybersecurity VPN Client is established. The easily configurable R&S Cybersecurity VPN Client can be used for Client-to-Site connections via the IPsec protocol. ● "Client-to-Site" – A C2S connection with a standard VPN client is established (e.g. for full tunneling). ● "Site-to-Site" – A S2S connection is established.
"Network Connection"	From the drop-down list, select the interface to be used to establish the tunnel.

The elements on the "Network" tab depend on the selected connection type:

Field	Description
"Local network"	Enter the IP address of the local network that is reachable from the outside through the VPN tunnel. It has to be in valid CIDR notation (IP address followed by a slash »/« and the number of bits set in the subnet mask, for example `192.168.1.0/24`). **Note:** For full tunneling, enter `0.0.0.0/0`.
"Client IP"	Optional and for R&S Cybersecurity VPN Client and Client-to-Site connections only: Enter the IP address under which the client is reachable.
"Use L2TP"	Optional and for Client-to-Site connections only: This checkbox is cleared by default. You can select the checkbox if you want to establish the IPsec connection on Layer 2. In this case, the "Local network" is set to `0.0.0.0/0`.
"Remote network"	For Site-to-Site connections only: Enter the IP address of the remote network that is reachable through the VPN tunnel. It has to be in valid CIDR notation (IP address followed by a slash »/« and the number of bits set in the subnet mask, for example `192.168.1.0/24`).
"Destination"	For Site-to-Site connections only: Enter the public IP address or hostname of the IPsec server.
"Dynamic destination"	For Site-to-Site connections only: This checkbox is cleared by default. If it is selected, incoming connections from any remote end are allowed for this connection. In this case, the "Destination" field is grayed out and it is not possible to initiate the connection from the local side.
"Establish connection"	For Site-to-Site connections only: Select whether the tunnel is established by the local site ("Initiate connection") or by the remote site "Wait for connection" by selecting the respective radio button.

On the "Authentication" tab, you can define the authentication settings for the IPsec connection:

Field	Description
"Authentication type"	Select the type of authentication for the IPsec connection by selecting the respective radio button. You can choose from the following five types: ● "PSK only (Preshared Key)" – Establishes an IPsec connection by using a password. This password has to registered on both sides of the VPN connection. ● "XAUTH (Client mode)" – Establishes an IPsec connection with IKEv1. R&S Unified Firewalls connects to the remote server with the given logon credentials. ● "XAUTH (Server mode)" – Establishes an IPsec connection with IKEv1. User accounts have to be created (see Chapter 3.4.1.9, "User Authentication", on page 47. ● "Certificate" – Establishes an IPsec connection by using certificates. The certificates selected on both devices must exactly match each other. ● "Certificate Authority" – Establishes an IPsec connection by using certificates. R&S Unified Firewalls accepts all remote certificates which are signed by the selected CA. **Note:** The remaining elements on this tab depend on the selected authentication type.
"Preshard Key"	Specify the password to use for the authentication of the IPsec connection. Clients need to supply this password to establish a VPN connection to R&S Unified Firewalls. **Note:** If you set up more than one VPN connection with a dynamic IP address (`%any`), the pre-shared key can no longer be clearly allocated to one VPN connection. The IPsec service then automatically uses the first VPN connection in the configuration.
"Local Identifier"	Optional: Enter a hostname or email address to clearly identify the local site. **Note:** If the hostname does not really exist, add an @ symbol in front of the hostname. Otherwise, R&S Unified Firewalls tries to resolve the hostname to an IP address.
"Remote Identifier"	Optional: Enter a hostname or email address to clearly identify the remote site. **Note:** If the hostname does not really exist, add an @ symbol in front of the hostname. Otherwise, R&S Unified Firewalls tries to resolve the hostname to an IP address.
"XAUTH Username"	Enter the username the firewall uses in XAUTH client mode to authenticate towards the remote end.
"XAUTH Password"	Enter the password the firewall uses in XAUTH client mode to authenticate towards the remote end.
"Show Password"	Optional: Select this checkbox to verify the password.
"Host certificate"	Select a certificate which R&S Unified Firewalls uses to authenticate towards the remote end. The private key for this certificate has to be available.

Field	Description
"Remote certificate"	Select an external certificate which the remote end uses for authentication. The remote end needs the private key for this connection to establish the tunnel.
"Identifier"	For "Certificate" and "Certificate Authority" only: Select identifiers to clearly identify the local and the remote end of the connection by clicking the respective radio button. The following options are available: ● The default setting is using the "Distinguished Name" of the certificates. This is recommended for connections between R&S Unified Firewalls systems. ● Using the first "Subject Alternative Name" (SAN) of the certificates. ● Using user-defined identifiers. Enter the identifiers manually under "Local Identifier" and/or "Remote Identifier". The data entered here has to be covered by the distinguished name or a subject alternative name of the certificates used to establish a tunnel. It is possible to use wildcards: * for whole words, ? for single characters.

On the "ISAKMP (IKE)" tab, you can define the encryption settings for the IPsec connection:

Field	Description
"IKE Version"	Select the Internet key exchange version to be used for the connection. IKEv2 is faster in establishing a tunnel and in rekeying. IKEv1 is maintained for compatibility reasons. **Note:** If you select the R&S Cybersecurity VPN Client as connection type or if you enable L2TP in a Client-to-Site connection, IKEv2 is not available.
"Encryption algorithm"	Select the cryptographic hash to verify the message.
"Authentication algorithm"	Select the algorithm to encrypt the message.
"DH group"	Select the Diffie-Hellman (DH) group to be used for IKE negotiation.
"Lifetime"	Specify the timeout (in seconds) after which the IKE connection expires and a new exchange is performed. **Note:** The value entered here only has an indirect influence on the renegotiation time. The precise point in time is determined randomly to avoid that all tunnels are re-established at the same time which would result in a heavy system load.
"Use mobile IKE (IKEv2 only)"	For IKEv2 only: Select this checkbox to allow one side to change its IP address without disconnecting the tunnel.

On the "IPsec" tab, you can select the encryption and authentication algorithms for the IPsec SA negotiation quick mode:

Field	Description
"Encryption algorithm"	Select the cryptographic hash to verify the message.
"Authentication algorithm"	Select the algorithm to encrypt the message.

Field	Description
"Lifetime"	Specify the timeout (in seconds) after which the IPsec SA expires and a new exchange is performed. **Note:** The value entered here only has an indirect influence on the renegotiation time. The precise point in time is determined randomly to avoid that all tunnels are re-established at the same time which would result in a heavy system load.
"Perfect Forward Secrecy (PFS)"	Select this checkbox to activate Perfect Forward Secrecy. Using PFS is recommended because it increases security. However, it has to be deactivated if the remote end does not support it (such as Windows XP). **Note:** If you select IKEv2, PFS is automatically used.
"PFS group"	Only if PFS is enabled: Select the Diffie-Hellman (DH group) to be used with PFS.

On the "Additional Settings" tab, you can set up port and protocol restrictions (for example for L2TP) for the IPsec connection. Only packets matching the settings are forwarded through the tunnel.

Field	Description
"Local Port"	Enter the local port you want to restrict traffic to.
"Remote Port"	Enter the remote port you want to restrict traffic to.
"Protocol number"	Enter the IANA protocol number for the protocol you want to restrict traffic to. **Note**: If you select "Client-to-Site" as the connection type and select the "Use L2TP" checkbox for this connection, the "Local Port" and the "Remote Port" are automatically set to `1701`, and the "Protocol number" is automatically set to `17` (UDP). If the "Use L2TP" checkbox is cleared, the "Local Port", the "Remote Port" and the "Protocol number" are automatically set to `0`.
"Data Compression"	Optional: Select this checkbox to activate data compression.

The buttons at the bottom right of the editor panel depend on whether you add a new VPN IPsec connection or edit an existing connection. For a newly configured connection, click "Create" to add the connection to the list of available IPsec connections or "Cancel" to discard your changes. To edit an existing connection, click "Close" as long as no changes have been made, "Save" to store the reconfigured connection or "Reset" to discard your changes.

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

VPN SSL Connections

R&S Unified Firewalls allows you to provide VPN access to remote clients via VPN SSL (Client-to-Site) and to create a secure tunnel between two remote networks (Site-to-Site).

VPN SSL Connections Overview

Navigate to "VPN > VPN Connections > VPN-SSL Connections" to display the list of VPN SSL connections that are currently defined on the system in the item list bar.

In the expanded view, the columns of the table display the "Name" of the VPN-SSL connection, the "Certificate"used in the connection, the "Status" and the "Type" of the connection. The buttons in the last column allow you to view and adjust the settings for a VPN SSL connection or to delete a connection from the system.

For further information, see Chapter 3.2, "Icons and Buttons", on page 23.

VPN SSL Connections Settings

Under "VPN > VPN Connections > VPN-SSL Connections", you can add or edit an existing VPN SSL connection.

The "VPN-SSL Connections" settings allow you to configure the following elements:

Field	Description
I/○	A slider switch indicates whether the VPN SSL connection is active (I) or inactive (○). By clicking the slider switch, you can toggle the state of the connection. A new connection is enabled by default.
"Name"	Enter a unique name for the connection. The name must consist of alphanumeric characters (allowed are letters of the English alphabet, integers and underscores).
"Certificate"	Select the server certificate for VPN SSL connections from the drop-down list. **Note:** The VPN certificate has to be signed by the same certificate authority (CA) on all sites. Therefore, it is advisable to manage the VPN CA and the VPN certificates on one site and then to export and import the VPN certificates from there to the other sites.
"Connection type"	Select the type of the connection and the role of your R&S Unified Firewalls by clicking the respective radio button. You can choose from the following three types: • "R&S Cybersecurity VPN Client" – A C2S connection with the R&S Cybersecurity VPN Client is established (e.g. for full tunneling). The easily configurable R&S Cybersecurity VPN Client can be used for Client-to-Site connections via the VPN SSL protocol. You can generate the configuration file on your R&S Unified Firewalls directly. For more information, see "VPN SSL Connections Settings" on page 145. **Note:** This connection type can also be used with the standard OpenVPN client to connect, in particular, mobile clients to your local network. • "Site-to-Site (Server)" – A S2S connection with your R&S Unified Firewalls serving as a server is established. • "Site-to-Site (Client)" – A S2S connection with your R&S Unified Firewalls serving as a client is established.

The elements in the settings section depend on the selected connection type.

For Client-to-Site (R&S Cybersecurity VPN Client) connections you can configure the following elements:

Field	Description
"Set default gateway"	Select this checkbox to use the VPN SSL tunnel as default route (i.e. for full tunneling).
"Client IP"	Optional: You can manually enter the IP address under which the client is reachable.
"Additional remote networks"	Indicate local networks to which the client is to create routes for this connection in valid CIDR notation (IP address followed by a slash »/« and the number of bits set in the subnet mask, for example `192.168.1.0/24`). Click "Add" to add a network to the list. You can edit or delete single entries in the list by clicking the corresponding button next to an entry. For further information, see Chapter 3.2, "Icons and Buttons", on page 23. **Note:** If you edit an entry, a check mark appears on the right of the entry. Click the check mark to apply your changes.

For Site-to-Site connections where R&S Unified Firewalls serves as server you can configure the following elements:

Field	Description
"Address pool"	Displays the address range from which IP addresses are used for this connection. The address range is specified in the VPN SSL settings. For more information, see Chapter 3.4.6.2, "VPN SSL Settings", on page 138.
"Remote IP"	Optional: Enter the IP address of the remote end.
"Remote Networks"	Indicate the networks which are available on the remote end. When the connection is established, the server sets up routes in these networks. Click "Add" to add a network to the list. You can edit or delete single entries in the list by clicking the corresponding button next to an entry. For further information, see Chapter 3.2, "Icons and Buttons", on page 23. **Note:** If you edit an entry, a check mark appears on the right of the entry. Click the check mark to apply your changes.
"Additional Local Networks"	Indicate additional local networks. When the connection is established, the server sets up routes in these networks. Click "Add" to add a network to the list. You can edit or delete single entries in the list by clicking the corresponding button next to an entry. For further information, see Chapter 3.2, "Icons and Buttons", on page 23. **Note:** If you edit an entry, a check mark appears on the right of the entry. Click the check mark to apply your changes.

For Site-to-Site connections where R&S Unified Firewalls serves as client you can configure the following elements:

Field	Description
"Address pool"	Displays the address range from which IP addresses are used for this connection. The address range is specified in the VPN SSL settings. For more information, see Chapter 3.4.6.2, "VPN SSL Settings", on page 138.
"Host"	Enter the network IP address under which the remote end is reachable. Click "Add" to add a network to the list. If you add more than one network, an automatic failover occurs in case the first network is not reachable. R&S Unified Firewalls then successively tries to reach the networks on the list until one network is reachable. You can edit or delete single entries in the list by clicking the corresponding button next to an entry. For further information, see Chapter 3.2, "Icons and Buttons", on page 23. **Note:** If you edit an entry, a check mark appears on the right of the entry. Click the check mark to apply your changes.
"Server Port"	Enter the port number used for this connection on the remote end.
"Try establishing connection for"	Define the timeout in minutes after which no more connection attempts are made. If this option is set to `0`, the connections attempts are continued without interruption.

The buttons at the bottom right of the editor panel depend on whether you add a new VPN SSL connection or edit an existing connection. For a newly configured connection, click "Create" to add the connection to the list of available VPN SSL connections or "Cancel" to discard your changes. To edit an existing connection, click "Close" as long as no changes have been made, "Save" to store the reconfigured connection or "Reset" to discard your changes.

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

3.4.7 Certificate Management

The "✹ Certificiate Management" settings allow you to control the certificates used by the R&S Unified Firewalls web client, the built-in SSL proxy and the OpenVPN server, to create templates to ease the creation of certificates and to enable OCSP/CRL services.

3.4.7.1 Certificate Signing Requests

R&S Unified Firewalls allows you to generate a certificate signing request and to export a certificate signing request to e.g. sign it on another firewall.

Certificate Signing Requests Overview

Navigate to "Certificate Management > Certificate Requests" to display the list of certificate signing requests that are currently defined on the system in the item list bar.

The buttons in the item list header allow you to generate a new certificate signing request and to sign a certificate signing request.

In the expanded view, the item list bar displays the "Common Name" of the certificate signing request. The button in the last column allows you to delete an existing certificate signing request from the system.

For further information, see Chapter 3.2, "Icons and Buttons", on page 23.

Certificate Signing Requests Settings

Under "Certificate Management > Certificate Requests", you can add a certificate signing request.

The "Generate Certificate Request" settings allow you to configure the following elements (some fields are only displayed for certain certificate types):

Field	Description
"Type"	From the drop-down list, select what kind of certificate you want to create the certificate signing request for. You can choose from the following three types: ● `Secondary CA` ● `VPN Certificate` ● `Webserver Certificate (R&S Cybersecurity UA Client)` For further information, see "Types of Certificates" on page 153.
"Private Key Encryption"	Decide whether to use the pre-selected `RSA` (Rivest-Shamir-Adleman) or the selectable `DSA` (Digital Signature Algorithm) as the encryption algorithm for the private key. (`DSA` is not available for VPN certificates due to limitations of OpenVPN.) **Note:** DSA with a private key size of 1024 bits or lower is not accepted by most clients.
"Private Key Size"	Decide whether to use the default value (`2048 Bit`) or to select a different bit length for the private key. Longer keys are more secure but they take longer to create.
"Private Key Password"	Enter a password to secure the private key.
"Show Private Key Password"	Optional: Select the checkbox to verify the private key password.
"Fill from Template"	From the drop-down list, select a template to fill in the input fields regarding the "Distinguished Name" (see Chapter 3.4.7.4, "Templates", on page 154). Alternatively, you can manually enter the information.
"Common Name (CN)"	Specify a name for the certificate.
"Country (C)"	Optional: Enter the two-letter code denoting the country.
"State (ST)"	Optional: Enter the name of the state.
"City (L)"	Optional: Enter the name of the city.
"Organization (O)"	Optional: Enter the name of the organization.
"Organizational Unit (OU)"	Optional: Enter the name of the unit within the organization.

Field	Description
"Subject Alternative Name (SAN)"	Optional: Enter as many custom subject alternative names as you like for the certificate for specific usage and select the corresponding types from the drop-down list. Available types are: `E-Mail`, `DNS`, `DirName`, `URI` and `IPv4`. Click the ⊕ button to put a subject alternative name on the list. You can edit or delete single entries in the list by clicking the corresponding button next to an entry. For further information, see Chapter 3.2, "Icons and Buttons", on page 23. **Note:** If you edit a subject alternative name, a check mark appears on the right of the entry. You have to click the check mark before being able to save the settings of the certificate.
"OCSP"	Optional and only available for secondary CAs: Select the checkbox to activate validation via OCSP (Online Certificate Status Protocol) for the secondary CA. For more information, see Chapter 3.4.7.3, "OCSP/CRL", on page 153.
"CRL"	Optional and only available for secondary CAs: Select the checkbox to activate validation via CRL (Certificate Revocation List) for the secondary CA. For more information, see Chapter 3.4.7.3, "OCSP/CRL", on page 153.
"Addresses for OCSP Responder/CRL Download"	Optional and only available for secondary CAs: Define base URLs for OCSP and CRL by entering a URL in the input field and clicking the ⊕ button. The actual URLs for the certificates are built from the base URL (protocol://hostname/) and are appended with `ocsp/<id-of-the-ca>` for OCSP URLs and with `/crls/<id-of-the-ca>.crl` for the CRL download URL. The base URL has to point to R&S Unified Firewalls or to any host providing the CRL (when the CRL is mirrored). You can edit or delete single entries in the list by clicking the corresponding button next to the entry. For further information, see Chapter 3.2, "Icons and Buttons", on page 23. **Note:** If you edit a URL, a check mark appears on the right of the entry. You have to click the check mark before being able to save the settings of the certificate. To activate the OCSP and CRL services, see Chapter 3.4.7.3, "OCSP/CRL", on page 153.

The buttons at the bottom right of the editor panel allow you to generate a new certificate signing request and to add it to the list of available certificate signing requests or to reject ("Cancel") the creation of the new certificate signing request.

After you have generated a certificate signing request, the system prompts you have to save the certificate signing request as a PEM file to the local machine.

Signing a Certificate Signing Request

To sign a certificate signing request, perform the following steps:

1. Navigate to "Certificate Management > Certificate Requests".

   The list of certificate signing requests which are currently defined on the system opens.

2. In the item list header, click the ⇥ (Sign certificate request) button.

   The "Sign Certificate Request" editor panel opens.

3. Click "Select File" behind the "Request File" input field.

   The local disk search opens.

4. Select a certificate signing request file in PEM format from the local disk.
5. Click "Open".

   The local disk search closes.
6. Under "Validity", define the initial period of time for which the new certificate should be considered valid. You can enter a date in the format `MM/DD/YYYY` (for example `04/20/2017`) or use the date picker to set the validity period of the certificate.

   Note: The validity period of the certificate must not exceed the validity period of the signing CA.
7. Under "Signing CA", select the certificate authority that is to be used to sign the new certificate from the drop-down list. This CA will be the parent CA that is used to verify or to revoke the certificate.
8. Under "CA Password", enter the password for the private key of the signing CA. The password is necessary as the signing of the public key of the new certificate is done with the private key of the signing certificate authority.
9. Optional: Select the "Show CA Password" checkbox to verify the signing CA's password.
10. Click "Sign" to sign the certificate signing request file.

    The certificate signing request is signed.

After signing the certificate signing request, the system prompts you to save the certificate to the local disc. It is also possible to export the certificate as described in Chapter 3.4.7.2, "Certificates", on page 150.

3.4.7.2 Certificates

The "Certificates" settings allow you control the certificates used by the R&S Unified Firewalls web client, the built-in SSL proxy and the OpenVPN server.

To secure encrypted connections, R&S Unified Firewalls uses digital certificates as described in the X.509 standard.

R&S Unified Firewalls itself acts as a certification authority. Therefore, a so-called CA certificate is required. To centralize the management of the certificates, it is advisable to create a CA certificate on a central firewall and use it to sign every certificate used for the application directly. This is called a single-staged certification chain.

All certificates for applications have to be signed by the central firewall. If a certificate is needed for another firewall, you have to create a request on it. This request has to be signed by the central firewall. The signed request which you created has to be imported by the other firewalls to use it.

If the other firewalls require the ability to create certificates for mostly local purposes which are however recognized as valid to your whole organization, you can use multi-staged certification chains. Therefore, you need a so-called root CA certificate on your central firewall with which you sign the secondary CA certificates. You need to create requests for these secondary CA certificates on your other firewalls. After you imported the signed CA certificates, the other firewalls themselves are able to sign certificates for applications. To display these hierarchies clearly, R&S Unified Firewalls shows them in a tree view.

Certificates Overview

Navigate to "Certificate Management > Certificates" to display the list of certificates that are currently defined on the system in a tree of authorities in the item list bar.

The buttons in the item list header allow you to create a new certificate and to import a certificate from a file.

Upon first boot and after a reinstallation, there are four certificates created by default:

Certificate Name	Definition
HTTPS Proxy CA	a certificate authority for the creation of subordinate certificates used by the HTTPS proxy
HTTPS Proxy Initialization	a preconfigured certificate for the HTTPS proxy
Mail Proxy CA	a certificate authority for the creation of subordinate certificates used by the mail proxy
Mail Proxy Initialization	a preconfigured certificate for the mail proxy

In the expanded view, the item list bar displays the name of the certificate and its dependency. The buttons behind the individual certificates show you the validity status and the type of each certificate, allow you to view the details of each certificate, replace a certificate by importing a new certificate, export and verify a certificate, temporarily suspend or renew the validity of a certificate, and permanently revoke the certificate.

For further information, see Chapter 3.2, "Icons and Buttons", on page 23.

Certificates Settings

The "Certificates" settings control the certificates used by R&S Unified Firewalls.

The plus button ⊕ in the element list header allows you to add new certificates.

The certificate settings allow you to configure the following elements (some fields are only displayed for certain certificate types):

Field	Description
"Type"	From the drop-down list, select what kind of certificate to create. For further information, see "Types of Certificates" on page 153.
"Signing CA"	If the certificate type was set to `VPN Certificate`, `Webserver Certificate`, `Secondary CA` or `HTTPS Proxy CA`, you can now select the certificate authority that is to be used to sign the new certificate. This CA will be the parent CA that is used to verify or to revoke the certificate.

Field	Description
"Private Key Encryption"	Decide whether to use the pre-selected `RSA` (Rivest-Shamir-Adleman) or the selectable `DSA` (Digital Signature Algorithm) as the encryption algorithm for the private key. (`DSA` is not available for VPN certificates due to limitations of OpenVPN.) **Note:** DSA with a private key size of 1,024 bits or lower is not accepted by most clients.
"Private Key Size"	Decide whether to use the default value (`2048 Bit`) or to select a different bit length for the private key. Longer keys are more secure but they take longer to create.
"Validity"	Define the initial period of time for which the certificate should be considered valid. The input fields are pre-filled with the current date as the date issued and the same day one year later as the date of expiry. To define a different period of time, enter the new date in the following format: MM/DD/YYYY (for example `04/20/2017`).
"CA Password"	Optional: Enter a password for the private key of the signing CA if the certificate type was set to `VPN Certificate`, `Webserver Certificate`, `Secondary CA` or `HTTPS Proxy CA`. The password is necessary as the signing of the public key of the new certificate is done with the private key of the signing certificate authority.
"Show CA Password"	Optional: Select this checkbox to verify the signing CA's password.
"Private Key Password"	Optional: Enter a password to secure the private key.
"Show Private Key Password"	Optional: Select the checkbox to verify the private key password.
"Fill from Template"	From the drop-down list, select a template to fill in the input fields regarding the "Distinguished Name" (see Chapter 3.4.7.4, "Templates", on page 154). Alternatively, you can manually enter the information.
"Common Name (CN)"	Specify a name for the certificate.
"Country (C)"	Optional: Enter the two-letter code denoting the country.
"State (ST)"	Optional: Enter the name of the state.
"City (L)"	Optional: Enter the name of the city.
"Organization (O)"	Optional: Enter the name of the organization.
"Organizational Unit (OU)"	Optional: Enter the name of the unit within the organization.
"Subject Alternative Name"	Optional: Enter as many custom subject alternative names as you like for the certificate for specific usage and select the corresponding types from the drop-down list. Available types are: `E-Mail`, `DNS`, `DirName`, `URI` and `IPv4`. Click the ⊕ button to put a subject alternative name on the list. You can edit or delete single entries in the list by clicking the corresponding button next to an entry. For further information, see Chapter 3.2, "Icons and Buttons", on page 23. **Note:** If you edit a subject alternative name, a check mark appears on the right of the entry. You have to click the check mark before being able to save the settings of the certificate.
"OCSP"	Optional and only available for CAs: Select the checkbox to activate validation via OCSP (Online Certificate Status Protocol) for the CA and its subcertificates. For more information, see Chapter 3.4.7.3, "OCSP/CRL", on page 153.

Field	Description
"CRL"	Optional and only available for CAs: Select the checkbox to activate validation via CRL (Certificate Revocation List) for the CA and its subcertificates. For more information, see Chapter 3.4.7.3, "OCSP/CRL", on page 153.
"Addresses for OCSP Responder/CRL Download"	Optional and only available for CAs: Define base URLs for OCSP and CRL by entering a URL in the input field and clicking the ⊕ button. The actual URLs for the certificates are built from the base URL (protocol://hostname/) and are appended with `ocsp/<id-of-the-ca>` for OCSP URLs and with `/crls/<id-of-the-ca>.crl` for the CRL download URL. The base URL has to point to the firewall or to any host providing the CRL (when the CRL is mirrored). You can edit or delete single entries in the list by clicking the corresponding button next to the entry. For further information, see Chapter 3.2, "Icons and Buttons", on page 23. **Note:** If you edit a URL, a check mark appears on the right of the entry. You have to click the check mark before being able to save the settings of the certificate. To activate the OCSP and CRL services, see Chapter 3.4.7.3, "OCSP/CRL", on page 153.

The buttons at the bottom right of the editor panel allow you to create a new certificate and to add it to the list of available certificates or to reject ("Cancel") the creation of the new certificate.

Types of Certificates

R&S Unified Firewalls offers various certificate types to choose from when creating a certificate.

Certificate type	Description
"VPN Certificate"	Creates a certificate that is used to identify VPN clients and servers. A suitable parent CA has to be selected.
"Webserver Certificate (UA client)"	Creates a certificate that is used for webservers. A suitable parent CA has to be selected.
"CA for VPN/Webserver Certificates"	Creates a certificate authority that can directly sign VPN and webserver certificates. No subordinate authorities can be attached. This CA can become a subordinate authority itself by exporting a signing request and reimporting the newly signed public certificate, thus signing it externally.
"CA with secondary CAs"	Creates a certificate authority that can sign subordinate CAs and client certificates for VPN and webservers.
"Secondary CA"	Creates a subordinate CA that can be used to sign VPN and webserver certificates. A parent CA of the kind `CA with secondary CAs` has to be selected.

3.4.7.3 OCSP/CRL

Enable the OCSP and/or CRL services to allow clients to verify the validity of certificates issued by the central firewall.

If co-workers quit their job or a private key gets lost, the corresponding certificate must be blocked to assure the company's security. This has to be done on the firewall which issued the certificate. The deletion of the certificate on the issuing firewall always includes the revocation of the certificate. To make the status of a certificate accessible to other firewalls, R&S Unified Firewalls offers two distinct services:

- OCSP (Online Certificate Status Protocol) – The remote firewall requests the status of the certificate from the issuing firewall at the moment the certificate is needed.
- CRL (Certificate Revocation List) – The firewall is able to provide static revocation lists in predefined intervals which can be downloaded by remote firewalls. Then the application only has to check whether the current CRL lists the certificate as blocked.

To use OCSP and/or CRL, the services in general have to be activated once with the necessary settings. While creating or renewing a CA, you have to declare whether OCSP and/or CRL requests should be sent and under which addresses (URLs) these services should be offered. These options are stored in the certificates themselves, so applications or remote firewalls know where to check the status of a certificate. For further information, see Chapter 3.4.7.2, "Certificates", on page 150.

The "OCSP/CRL" settings allow you to configure the following elements:

Field	Description
I/○	A slider switch indicates whether the corresponding service is active (I) or inactive (○). By clicking the slider switch, you can toggle the state of both services individually. Both options are deactivated by default.
"Allow access to OCSP/CRL service from Internet"	Select this checkbox to allow access to the respective service from the Internet.
"Port"	Specify the port that is reachable from the Internet.
"Validity Period"	Specify the cache time (in hours) which is sent in the HTTP header to requesting firewalls. After this period has elapsed, new requests will be answered. The default cache time is set to `168` hours.
"Update Interval"	Specify the update interval in hours, the default interval is set to `48` hours.

The buttons at the bottom right of the editor panel allow you to shut ("Close") the editor panel as long as no changes have been made and to store ("Save") or to discard ("Reset") your changes.

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

3.4.7.4 Templates

To ease the creation of new certificates, you can use templates to prepopulate the input fields regarding the "Distinguished Name" and the "Subject Alternative Names".

Templates Overview

Navigate to "Certificate Management > Templates" to display the list of templates that are currently defined on the system in the item list bar.

In the expanded view, the columns of the table display the name and the settings of the template. The buttons in the last column allow you to view and adjust the settings for an existing template, create a new template based on a copy of an existing template or delete a template from the system.

For further information, see Chapter 3.2, "Icons and Buttons", on page 23.

Templates Settings

The "Templates" settings allow you to configure the following elements:

Field	Description
"Name"	Specify a name for the template.
"Country (C)"	Optional: Enter the two-letter code denoting the country.
"State (ST)"	Optional: Enter the name of the state.
"Location (L)"	Optional: Enter the name of the city.
"Organization (O)"	Optional: Enter the name of the organization.
"Organizational Unit (OU)"	Optional: Enter the name of the unit within the organization.
"Subject Alternative Names"	Optional: Enter as many custom subject alternative names (SAN) as you like for the certificate for specific usage and select the corresponding types from the drop-down list. Available types are: `E-Mail`, `DNS`, `DirName`, `URI` and `IPv4`. Click "Add" to put a subject alternative name on the list. You can edit or delete single entries in the list by clicking the corresponding button next to an entry. For further information, see Chapter 3.2, "Icons and Buttons", on page 23. **Note:** If you edit a subject alternative name, a check mark appears on the right of the entry. You have to click the check mark before being able to save the settings of the certificate.

The buttons at the bottom right of the editor panel depend on whether you add a new template or edit an existing template. For a newly configured template, click "Create" to add the template to the list of available templates or "Cancel" to discard your changes. To edit an existing template, click "Close" as long as no changes have been made, "Save" to store the reconfigured template or "Reset" to discard your changes.

3.4.7.5 Trusted Proxy CAs

Navigate to "Certificate Management > Trusted Proxy CAs" to display the list of custom and system certificate authorities that are currently defined on the system in the item list bar and that the SSL proxy trusts for external connections.

In the expanded view, the first column of the table displays the "Name" of the CA certificate. The buttons in the last column allow you to view the settings for an existing CA certificate or delete a CA certificate from the system.

For further information, see Chapter 3.2, "Icons and Buttons", on page 23.

To send a custom CA to R&S Unified Firewalls, click the ⇥ (Import) button in the item list header, select and open the desired PEM file and click "Import". The imported custom certificate is added to the list of available trusted proxy CAs.

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

3.4.8 Diagnostic Tools

Navigate to the "🔧 Diagnostic Tools" menu to use diagnostic tools if problems in the communication between R&S Unified Firewalls and other devices occur.

Use the diagnostic tools to verify whether R&S Unified Firewalls can communicate with a computer or other device at a specific network address (`ping`) or to follow the path a message takes as it travels through the network (`traceroute`).

To allow diagnostic analysis between zones, a firewall rule with the ICMP protocol or the ICMP Ping application has to be active in the corresponding direction.

For more detailed information on network tools, see the following sections.

3.4.8.1 Ping

Navigate to "Diagnostic Tools > Ping" to use the `ping` command to check if R&S Unified Firewalls can communicate with a computer or other device at a specific network address.

Ping is a diagnostic tool that continuously sends ping signals to the target to check if it is able to receive data. Pinging can help you debug communication problems by verifying connectivity between R&S Unified Firewalls and the remote device.

The "Ping"settings allow you to configure the following "Parameters":

Field	Description
"Destination"	Enter the valid network address to ping.
"Request Count"	Select the number of ICMP echo request packets to be sent to the target. You can choose any integer from `1` to `10` from the drop-down list. The default number is set to `4`.

Click "Run" to start pinging. The "Output" area displays the output of the `ping` command. If the other device responds to the ping, R&S Unified Firewalls can reach the device.

The "Close" button at the bottom of the panel allows you to shut the panel and return to the complete overview of your entire configured network.

3.4.8.2 Traceroute

Navigate to "Diagnostic Tools > Traceroute" to use the `traceroute` command to track the path a message takes through the network.

Packets sent from R&S Unified Firewalls may pass through many other devices on the way to their final destination, which can make it difficult to figure out where problems are occurring if connectivity cannot be established. You can use the `traceroute` command to track the route that packets follow from R&S Unified Firewalls along the path to a certain host.

The "Traceroute" settings allow you to configure the following "Parameters":

Field	Description
"Destination"	Enter the IP address of the final destination.
"Max Hops"	Enter the maximum number of nodes (routers or other devices) to be traversed on the way to the destination. The default number is set to `30`, but you can enter any integer from `1` to `255`. If the destination is not reached before this threshold, probe packets are discarded.

Click "Run" to start tracerouting. The "Output" area displays the list of gateways traversed along the way.

The "Close" button at the bottom of the panel allows you to shut the panel and return to the complete overview of your entire configured network.

Index