R&S®Unified Firewall

Migrationsanleitung

Migrationsanleitung

ROHDE&SCHWARZ
Cybersecurity

Die in diesem Produkt enthaltene Software verwendet mehrere wichtige Open-Source-Softwarepakete. Informationen finden Sie im separat erhältlichen Dokument "Open Source Acknowledgement".
Die Open-Source-Software wird kostenfrei zur Verfügung gestellt. Sie sind berechtigt, die Softwarepakete entsprechend der zugehörigen Lizenzbedingungen zu verwenden.
Rohde & Schwarz dankt der Open-Source-Community für ihren wertvollen Beitrag zum Embedded Computing.

© 2019 Rohde & Schwarz Cybersecurity GmbH
Mühldorfstraße 15, 81671 München, Deutschland
Telefon: +49 (0) 89 41 29 - 0
E-Mail: cybersecurity@rohde-schwarz.com
Internet: https://rohde-schwarz.com/cybersecurity
Änderungen vorbehalten – Daten ohne Genauigkeitsangabe sind unverbindlich.
R&S® ist ein eingetragenes Warenzeichen der Firma Rohde & Schwarz GmbH & Co. KG.
Eigennamen sind Warenzeichen der jeweiligen Eigentümer.

R&S®Unified Firewall

Im gesamten Dokument werden die Produktnamen von Rohde & Schwarz ohne das Markenzeichen ® gekennzeichnet. R&S®Unified Firewall hat die Kurzbezeichnung R&S Unified Firewall.

1 Inhalt dieses Dokuments

Diese R&S Unified Firewall Migrationsanleitung beschreibt, wie Sie die Software Ihrer R&S Unified Firewall auf Version 10.2.2 aktualisieren können.

Bild 1-1: Beispiel: R&S Unified Firewall UF-500

1.1 Zielgruppe

Dieses Dokument richtet sich an Netzwerk- und Computertechniker, die für die Installation und Konfiguration der Systeme der R&S Unified Firewall zuständig sind.

1.2 Kapitelübersicht

Die Inhalte dieses Dokuments unterstützen Sie beim Upgrade Ihrer R&S Unified Firewall und bei den nach dem Upgrade erforderlichen Schritten.

Dieses Dokument enthält die folgenden Kapitel:

- Kapitel 2, "Vor dem Upgrade zu beachten", auf Seite 5
  Schritte, die vor dem Upgrade zu berücksichtigen sind
- Kapitel 2.1, "Unterstützte Geräte", auf Seite 5
  Hardware, die von Version 10.2.2 unterstützt wird
- Kapitel 2.2, "Entfernte Funktionen", auf Seite 6
  Eine Liste der Funktionen, die die R&S Unified Firewall in Version 10.2.2 und darüber nicht weiterführt
- Kapitel 2.3, "Manuelle Einstellungen", auf Seite 6
  Einstellungen, die Sie nach dem Upgrade manuell neu konfigurieren müssen
- Kapitel 3.1, "Upgrade der R&S Unified Firewall für die Versionen 9.6 und 9.8", auf Seite 7
  Upgrade-Informationen für die Versionen 9.6 und 9.8 der R&S Unified Firewall
- Kapitel 3.2, "Upgrade der R&S Unified Firewall für die Versionen 9.4 und 9.5", auf Seite 8
  Upgrade-Informationen für die Versionen 9.4 und 9.5 der R&S Unified Firewall
- Kapitel 3.3, "Upgrade der R&S Unified Firewall vor Version 9.4", auf Seite 10

Upgrade-Informationen für Versionen der R&S Unified Firewall vor 9.4

- Kapitel 4, "Erste Schritte", auf Seite 13
  Erste Schritte für den Gebrauch Ihrer R&S Unified Firewall Version 10.2.2 nach dem Upgrade
- Kapitel 5, "Kontakt, Service und Support", auf Seite 15
  Anlaufstellen bei Schwierigkeiten während des Upgrades

2 Vor dem Upgrade zu beachten

Bevor Sie die R&S Unified Firewall auf die neueste Version aktualisieren, beachten Sie bitte Folgendes:

- Stellen Sie sicher, dass Ihre Hardware unterstützt wird. Eine Liste der unterstützten Geräte finden Sie in Kapitel 2.1, "Unterstützte Geräte", auf Seite 5.
- Auf Geräten mit weniger als 4 GB Arbeitsspeicher können nicht alle UTM-Einstellungen gleichzeitig aktiv sein.
- Falls Sie zwei R&S Unified Firewalls im Hochverfügbarkeitsmodus verwenden, beachten Sie Folgendes:
  - Deaktivieren Sie den Hochverfügbarkeitsmodus, bevor Sie die R&S Unified Firewall auf Version 10.2.2 aktualisieren.
  - Sie müssen die Upgrade-Anweisungen für beide Geräte separat befolgen.
  - Konfigurieren Sie die Hochverfügbarkeitseinstellungen beider Geräte nach dem Upgrade, wie im R&S Unified Firewall Bedienhandbuch beschrieben.
- Ab Version 10.2 ist eine zentralisierte Verwaltung der R&S Unified Firewall nur noch über das R&S Unified Firewall Command Center möglich.
- Stellen Sie sicher, dass Ihre Konfiguration keine der Einstellungen aus Kapitel 2.2, "Entfernte Funktionen", auf Seite 6 zwingend benötigt.
- Einige Einstellungen werden nicht automatisch auf Version 10.2.2 der R&S Unified Firewall übertragen. Siehe hierzu Kapitel 2.3, "Manuelle Einstellungen", auf Seite 6.

2.1 Unterstützte Geräte

Version 10.2.2 wird von folgenden Geräten unterstützt:

- GPO150
- GPA300/500
- GPX850
- GPZ1000/2500/5000
- UTM+100/200/300/500/800/1000/2000/2500/5000
- NP+200/500/800/1000/2000/2500/5000
- GP-U 50/100/200/300/400/500
- GP-E 800/900/1000/1100/1200
- GP-S 1600/1700/1800/1900/2000
- GP-T 10
- UF-50/100/200/300/500/900/1000/1200/2000
- UF-T10

2.2 Entfernte Funktionen

Die folgenden Funktionen sind in Version 10.2.2 nicht verfügbar:

- VPN-Verbindungen über PPTP
- E-Mail-Reporting
- LAN-Accounting
- VPN-SSL-Bridges
- Desktopnotizen
- Dynamisches Routing
- Verbindungsspezifische DNS-Server
- Zentralisierte Verwaltung der R&S Unified Firewall. Nutzen Sie stattdessen das R&S Unified Firewall Command Center.

2.3 Manuelle Einstellungen

Die folgenden Einstellungen werden beim Upgrade auf Version 10.2.2 nicht automatisch aktualisiert. Konfigurieren Sie diese Einstellungen nach dem Upgrade nach Ihren Anforderungen erneut. Weiterführende Informationen zu den einzelnen Einstellungen entnehmen Sie entsprechenden Kapiteln im Anhang:

- Hochverfügbarkeit: Kapitel A, "High Availability", auf Seite 17
- Monitoring: Kapitel B, "Statistics", auf Seite 23
- Traffic-Shaping und QoS: Kapitel C, "Quality of Service (QoS)", auf Seite 27
- Anwendungsfilter - gilt für Version 9.6: Kapitel D, "Application Filter", auf Seite 29
- Mailproxy-Zertifikate - gilt für Version 9.8: Kapitel E, "Email Security", auf Seite 31
- IDS/IPS: Kapitel F, "IDS/IPS", auf Seite 35
- HTTPS-Proxy-Zertifikate: Kapitel G, "Proxy", auf Seite 37
- Reverse Proxy: Kapitel H, "Reverse Proxy", auf Seite 41

3 Vorgehensweise beim Upgrade

In den folgenden Kapiteln finden Sie Hinweise zum Upgrade Ihrer aktuellen Version der R&S Unified Firewall auf Version 10.2.2:

Installierte Version	Kapitel
≥10.0	Im R&S Unified Firewall Bedienhandbuch, Kapitel 3.4.1.8, "Update-Einstellungen", finden Sie weiterführende Informationen zum Upgrade Ihrer R&S Unified Firewall auf Version 10.2.2 mit Hilfe des Webclients.
9.8	Kapitel 3.1, "Upgrade der R&S Unified Firewall für die Versionen 9.6 und 9.8", auf Seite 7
9.7	**Hinweis:** Kontaktieren Sie unseren Vertrieb, falls Ihr Gerät nicht unter Unterstützte Geräte aufgelistet ist. **Hinweis:** Ein Upgrade der R&S Unified Firewall auf Version 10.2.2 wird von Version 9.7 nicht unterstützt. Stattdessen muss eine vollständige Neuinstallation erfolgen. In Kapitel 3.2.1, "Installieren der Version 10.2.2 mit einem USB-Stick", auf Seite 9 finden Sie Informationen zur manuellen Installation der Version 10.2.2.
9.6	Kapitel 3.1, "Upgrade der R&S Unified Firewall für die Versionen 9.6 und 9.8", auf Seite 7
9.4	Kapitel 3.2, "Upgrade der R&S Unified Firewall für die Versionen 9.4 und 9.5", auf Seite 8
9.5	
< 9.4	Kapitel 3.3, "Upgrade der R&S Unified Firewall vor Version 9.4", auf Seite 10

3.1 Upgrade der R&S Unified Firewall für die Versionen 9.6 und 9.8

ACHTUNG

Wird der Upgradevorgang unterbrochen, kann die R&S Unified Firewall beschädigt werden. Schalten Sie das Gerät während des Upgradevorgangs nicht aus. Starten Sie das Gerät nur dann neu, wenn Sie explizit dazu aufgefordert werden.

1. Falls Sie Version 9.8 der R&S Unified Firewall aktualisieren, konfigurieren Sie vorab den externen Zugang zum Webclient („Optionen > Firewall > Sicherheit > Zugriff“).
2. Wenn Sie ein Gerät mit weniger als 4 GB Arbeitsspeicher verwenden, deaktivieren Sie die UTM-Einstellungen, da das Upgrade ansonsten fehlschlagen könnte.
3. Öffnen Sie im gateprotect Administrationsclient den Update Manager („Einstellungen > Updates“).

4. Wählen Sie „Upgrade von v9.x auf 10.2.2“.

   Tipp: Falls sich das Upgrade nicht in der Liste befindet, klicken Sie auf „Aktualisieren“.

   Hinweis: Vor Installation des Upgrades müssen Sie alle Patches installieren. Zur Installation einiger Patches muss die R&S Unified Firewall gegebenenfalls neu gestartet werden. Ob ein Neustart notwendig ist, erfahren Sie in der Beschreibung der jeweiligen Patches.

5. Klicken Sie auf „Installieren“.

   - Das Upgrade wird automatisch heruntergeladen.
   - Die R&S Unified Firewall startet nach Abschluss des Downloads neu.
     Hinweis: Je nach Gerätetyp kann die Integritätsprüfung des Upgrades etwas Zeit in Anspruch nehmen.
   - Die R&S Unified Firewall installiert das Upgrade automatisch.
     Hinweis: Die Installation kann bis zu 30 Minuten in Anspruch nehmen.
   - Nach der Installation startet die R&S Unified Firewall automatisch neu.

6. Schließen Sie den gateprotect Administrationsclient.

Falls das Upgrade fehlschlägt oder das Gerät neu startet, und die alte Version weiterhin installiert ist, finden Sie in den Logdateien weiterführende Informationen.

Wie Sie auf den Webclient der R&S Unified Firewall zugreifen, erfahren Sie in Kapitel 4, "Erste Schritte", auf Seite 13.

Falls Sie ein Gerät mit weniger als 4 GB Arbeitsspeicher verwenden, aktivieren Sie die benötigten UTM-Einstellungen erneut.

Auf diesen Geräten können nicht alle UTM-Einstellungen gleichzeitig aktiv sein. Weiterführende Informationen entnehmen Sie Kapitel 3.4.5, "UTM", im R&S Unified Firewall Bedienhandbuch.

3.2 Upgrade der R&S Unified Firewall für die Versionen 9.4 und 9.5

Für das Upgrade der R&S Unified Firewall Versionen 9.4 und 9.5 stehen Ihnen folgende Optionen zur Verfügung:

- Option 1 (empfohlen): Installieren von Version 10.2.2 mit einem USB-Stick.
- Option 2 (nicht empfohlen): Upgrade der R&S Unified Firewall auf Version 9.6 mit anschließendem Upgrade auf Version 10.2.2.

3.2.1 Installieren der Version 10.2.2 mit einem USB-Stick

ACHTUNG

Wird der Upgradevorgang unterbrochen, kann die R&S Unified Firewall beschädigt werden. Schalten Sie das Gerät während des Upgradevorgangs nicht aus. Starten Sie das Gerät nur dann neu, wenn Sie explizit dazu aufgefordert werden.

1. Starten Sie den gateprotect Administrationsclient und erstellen Sie ein Backup Ihrer Konfiguration („Datei > Backup erstellen“).
2. Gehen Sie wie folgt vor, um einen bootfähigen USB-Stick zu erstellen:
   a) Stecken Sie den USB-Stick an Ihren Computer an.
   b) Geben Sie auf Ihrem Computer die folgende URL in die Adressleiste Ihres Browsers ein:
   https://www.mygateprotect.com
   Navigieren Sie zu „Downloads > Firewall (Vollversion)“.
   c) Laden Sie für Version 10.2 die folgenden Dateien herunter:
   - Das Systemabbild der R&S Unified Firewall (ISO-Datei)
   - Die USB-Installationsdatei (EXE-Datei)

   d) Führen Sie die USB-Installationsdatei aus.
   Der USB-Installationsassistent öffnet sich.
   e) Der Assistent begleitet Sie durch die Konfiguration. Beachten Sie hierbei:
   - Wählen Sie auf der Seite „Wählen Sie die R&S Cybersecurity ISO-Datei aus“ die ISO-Datei aus, die Sie in Schritt c heruntergeladen haben.
   - Wählen Sie auf der Seite „Wählen Sie eine Backup-Datei aus (optional)“ die Backup-Datei aus, die Sie in Schritt 1 erstellt haben.

   Wenn die Meldung „Konfiguration erfolgreich abgeschlossen.“ erscheint, haben Sie einen bootfähigen USB-Stick zur Installation des neuen Systemabbilds erstellt.
   f) Entfernen Sie den USB-Stick von ihrem Computer.
   ACHTUNG:
   Schließen Sie den USB-Stick niemals an einen Computer während des Startvorgangs an. Der USB-Stick löst in dem Fall eine unbeaufsichtigte Installation der R&S Unified Firewall aus. Während dieser Installation werden die Festplatten formatiert.
3. Gehen Sie wie folgt vor, um das Systemabbild mithilfe des bootfähigen USB-Sticks zu installieren:
   a) Schalten Sie das Gerät aus.
   b) Schließen Sie den USB-Stick mit dem neuen Systemabbild an einen beliebigen USB-Port des Geräts an.
   c) Schalten Sie das Gerät ein, um die unbeaufsichtigte Installation des Systemabbilds zu starten. Wenn der Installationsprozess erfolgreich beendet wurde, schaltet sich das Gerät automatisch aus.

d) Entfernen Sie den USB-Stick, nachdem sich das Gerät ausgeschaltet hat.
ACHTUNG:
Wir empfehlen Ihnen, den USB-Stick nach der vollständigen Installation der neuesten Softwareversion der R&S Unified Firewall neu zu formatieren. Dies verhindert eine versehentliche Installation des Systemabbilds, die eine Formatierung der Festplatten und Datenverlust zur Folge hat.

4. Konfigurieren Sie nach der Installation diejenigen Einstellungen neu, die nicht automatisch während des Upgrades übertragen wurden. Siehe hierzu Kapitel 2.3, "Manuelle Einstellungen", auf Seite 6.

Falls das Upgrade fehlschlägt oder das Gerät neu startet, und die alte Version weiterhin installiert ist, finden Sie in den Logdateien weiterführende Informationen.

Wie Sie auf den Webclient der R&S Unified Firewall zugreifen, erfahren Sie in Kapitel 4, "Erste Schritte", auf Seite 13.

3.2.2 Upgrade der R&S Unified Firewall auf Version 9.6 mit anschließendem Upgrade auf Version 10.2.2

1. Wiederholen Sie die Schritte unter Kapitel 3.3, "Upgrade der R&S Unified Firewall vor Version 9.4", auf Seite 10, bis Sie Version 9.6 erreichen.
2. Führen Sie das Upgrade der R&S Unified Firewall auf Version 10.2.2 durch, wie in Kapitel 3.1, "Upgrade der R&S Unified Firewall für die Versionen 9.6 und 9.8", auf Seite 7 beschrieben.

3.3 Upgrade der R&S Unified Firewall vor Version 9.4

Wenn Sie eine gateprotect-Firewall oder eine R&S Unified Firewall älter als Version 9.4 betreiben, müssen Sie Ihre Software zunächst auf Version 9.4 aktualisieren.

ACHTUNG

Wird der Upgradevorgang unterbrochen, kann die R&S Unified Firewall beschädigt werden. Schalten Sie das Gerät während des Upgradevorgangs nicht aus. Starten Sie das Gerät nur dann neu, wenn Sie explizit dazu aufgefordert werden.

1. Öffnen Sie im gateprotect Administrationsclient den Update-Manager („Einstellungen > Updates“).

   Tipp: Falls das Upgrade auf die nächsthöhere Version nicht aufgelistet ist, klicken Sie auf „Aktualisieren“.

Stellen Sie vor dem Upgrade sicher, dass alle Patches installiert sind. Um einen Patch zu installieren, befolgen Sie die nachfolgend beschriebenen Schritte.

2. Wählen Sie die nächsthöhere Version aus.
3. Klicken Sie auf „Installieren“.

   Das Upgrade wird heruntergeladen und automatisch installiert.
   Hinweis: Die Installation kann bis zu 30 Minuten in Anspruch nehmen.
4. Schließen Sie nach der Installation den gateprotect Administrationsclient. Klicken Sie im Logout-Fenster die Option „Neustart“.

   Tipp: Für einige Patches ist ein Neustart des Geräts erforderlich. Weitere Informationen entnehmen Sie bitte der entsprechenden Patch-Beschreibung.
5. Jede Softwareversion der R&S Unified Firewall erfordert eine bestimmte Version des gateprotect Administrationsclients. Diesen können Sie unter https://mygateprotect.com herunterladen.

   a) Gehen Sie zu „Downloads > Management Tools“
   b) Laden Sie den Installer für Ihre Version der R&S Unified Firewall herunter.
   c) Installieren Sie den gateprotect Administrationsclient.
   d) Starten Sie den gateprotect Administrationsclient.
6. Falls Ihre aktuelle Softwareversion weiterhin älter als Version 9.4 ist, wiederholen Sie die obigen Schritte ab Schritt 2.
   Sobald Sie Version 9.4 erreicht haben, können Sie mit den Schritten unter Kapitel 3.2, "Upgrade der R&S Unified Firewall für die Versionen 9.4 und 9.5",
   auf Seite 8 fortfahren.

Falls das Upgrade fehlschlägt oder das Gerät neu startet, und die alte Version weiterhin installiert ist, finden Sie in den Logdateien weiterführende Informationen.

4 Erste Schritte

Nach der Installation von Version 10.2.2 greifen Sie folgendermaßen auf die R&S Unified Firewall zu:

1. Öffnen Sie Ihren Browser.
2. Geben Sie in die Adressleiste des Browser `<IP-Adresse>:3438` ein.

   Ersetzen Sie hierbei `<IP-Adresse>` mit der IP-Adresse Ihrer R&S Unified Firewall.
3. Erstellen Sie eine Ausnahme für die Zertifikatswarnung.

   Die Anmeldeseite der R&S Unified Firewall erscheint.
4. Geben Sie die gleichen Anmeldedaten ein, die Sie zuvor im gateprotect Administrationsclient verwendet haben.
5. Klicken Sie auf „Login“.
6. Nach der Anmeldung werden Sie dazu aufgefordert, dem Endnutzer-Lizenzvertrag (EULA) zuzustimmen.
7. Um dem EULA zuzustimmen, klicken Sie auf „Akzeptieren & Anmelden“.

   Der Webclient wird geöffnet.

Informationen zu den ersten Schritten mit Version 10.2.2 der R&S Unified Firewall entnehmen Sie dem Bedienhandbuch. Das Bedienhandbuch finden Sie unter „Hilfe“ in der rechten oberen Ecke des Bildschirms. Sie erhalten darin eine allgemeine Einführung in die Software sowie detaillierte Beschreibungen der Konfigurationsdialoge.

5 Kontakt, Service und Support

Unterstützung erhalten Sie aus folgenden Quellen:

- R&S Unified Firewall Bedienhandbuch
- Service Desk unter myrscs.rohde-schwarz.com
- Unsere Vertriebspartner
- RSCS Support-Team (support.rscs@rohde-schwarz.com)

Anhang

A High Availability

The „High Availability" (HA) settings allow two independent R&S Unified Firewall 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 Firewall 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.

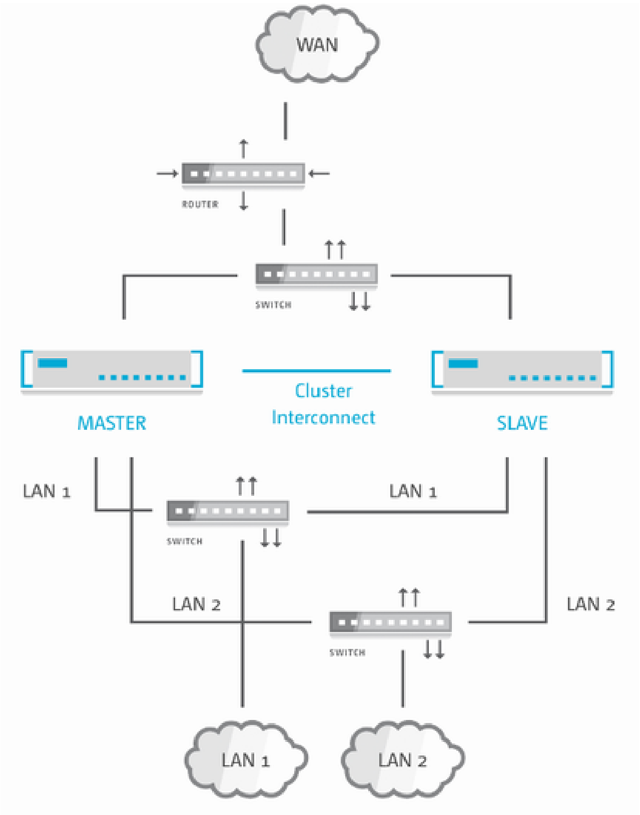


Bild A-1: Sample network setup for High Availability.

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

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

A.1 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 on configuring network interfaces and network connections, refer to the R&S Unified Firewall User Manual. 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 Firewall. 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 Firewall is to play in the HA cluster: ● „Master“ – R&S Unified Firewall is active and synchronizes its configuration to R&S Unified Firewall being the slave. ● „Slave“ – R&S Unified Firewall 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 Firewall systems for Cluster Interconnection.
„Local IP“	Enter the IP address which you want to assign to the HA interface on R&S Unified Firewall 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 Firewall can reach the other R&S Unified Firewall 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 Bild A-1).

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 Firewall. For further information, see Kapitel A.1.2, "Disabling High Availability Configurations", auf Seite 21.

A.1.1 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 Kapitel A.1.2, "Disabling High Availability Configurations", auf Seite 21.
2. Update both systems separately. For more information, see Kapitel 3, "Vorgehensweise beim Upgrade", auf Seite 7.
3. Enable High Availability. For more information, see Kapitel A.1, "High Availability Settings", auf Seite 18.

A.1.2 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.

   Hinweis: 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.

B 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, refer to the R&S Unified Firewall Bedienhandbuch.

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 Kapitel B.3, "Overview", auf Seite 25.

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 on table functionality, refer to the R&S Unified Firewall Bedienhandbuch.
- 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 on statistics settings, refer to the R&S Unified Firewall Bedienhandbuch.
- 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.

B.1 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 on IDS/IPS settings, refer to the R&S Unified Firewall Bedienhandbuch.

B.2 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

Statistics Element (Event Type)	Description
„Spam“ („Spam Alert“)	Number of spam emails detected
„Web Access“ („Web Content Blocked“)	Web access blocked by content filter
„Appfilter“ („Appfilter Alert“)	Number of alerts regarding blocked application-specific traffic

B.3 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 Firewall can detect.

The following special features apply only to this panel (diverging from the description of the individual statistics panels in "Working with statistics" auf Seite 23):

- 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`.

B.4 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 Firewall 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.

B.5 Top Domains Blocked

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

B.6 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 Firewall to collect this kind of data by enabling the „Connection Finished“ event type.

C 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 Firewall 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 Firewall 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.

C.1 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 on icons and buttons, refer to the R&S Unified Firewall Bedienhandbuch. **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.

C.2 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 Kapitel C.1, "QoS Settings", auf Seite 27.

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

C.2.1 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, refer to the R&S Unified Firewall Bedienhandbuch.

C.2.2 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.

D 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.

D.1 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 on license settings, refer to the R&S Unified Firewall Bedienhandbuch.

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.

D.2 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, refer to the R&S Unified Firewall Bedienhandbuch.

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 Firewall 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. For further information on firewall rule settings and desktop connection settings, refer to the R&S Unified Firewall Bedienhandbuch).

E Email Security

Under „UTM > Email Security“, you can manage your mail filter and antispam settings.

E.1 Antispam Settings

You can configure R&S Unified Firewall to protect your system from email spam.

The spam filter is included in the UTM license. When R&S Unified Firewall 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 refer to the R&S Unified Firewall Bedienhandbuch.

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.

Field	Description
„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 on icons and buttons, refer to the R&S Unified Firewall Bedienhandbuch. 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 Kapitel E.2, "Mail Filter Settings", auf Seite 32.

E.2 Mail Filter Settings

Under „UTM > Email Security > Mail Filter Settings“, you can activate the mail proxy on your R&S Unified Firewall. 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 on icons and buttons, refer to the R&S Unified Firewall Bedienhandbuch. 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, refer to the R&S Unified Firewall Bedienhandbuch.

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 Firewall and of your client machines.

F 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 Firewall, 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. If enabled, the IDS/IPS engine always scans traffic on *all* interfaces of your R&S Unified Firewall. For detailed information on the categories, see Emerging Threats FAQ.

IDS/IPS is included in the UTM license. When R&S Unified Firewall 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, refer to the R&S Unified Firewall Bedienhandbuch.

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 on icons and buttons, refer to the R&S Unified Firewall Bedienhandbuch.
„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 Firewall 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 on system logs, refer to the R&S Unified Firewall Bedienhandbuch.

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 on icons and buttons, refer to the R&S Unified Firewall Bedienhandbuch.

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.

G Proxy

Under „UTM > Proxy“, you can manage your HTTP(S), mail and VoIP proxy settings.

G.1 HTTP Proxy Settings

R&S Unified Firewall uses the Squid proxy. This proxy serves as an interface to the content filter and the antivirus scanner. For further information on the content filter and antivirus settings, refer to the R&S Unified Firewall Bedienhandbuch.

Under „UTM > Proxy > HTTP Proxy Settings“, you can configure the HTTP(S) proxy for your R&S Unified Firewall.

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 Firewall is able to correctly resolve the domains to be accessed.

Import the HTTPS Proxy CA of your R&S Unified Firewall 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 Firewall automatically forwards all requests which arrive on port 80 (HTTP) through the proxy (default setting). • „Intransparent“ The HTTP proxy of R&S Unified Firewall must explicitly be addressed on port 10080.

Field	Description
„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 Firewall forwards all requests which arrive on port 443 (HTTPS) automatically through the proxy (default setting). ● „Intransparent“ The HTTPS proxy of R&S Unified Firewall 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 Firewall 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 Firewall 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 on icons and buttons, refer to the R&S Unified Firewall Bedienhandbuch. **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.

G.2 Mail Proxy Settings

With the Mail proxy, you can use R&S Unified Firewall as a proxy for your emails.

Under „UTM > Proxy > Mail Proxy“, you can configure the mail proxy for your R&S Unified Firewall:

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 Firewall 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 Firewall dynamically creates certificates for each mail server. ● „Select certificate“ R&S Unified Firewall 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.

G.3 VoIP Proxy Settings

With the VoIP proxy, you can use R&S Unified Firewall as proxy for VoIP connections.

Under „UTM > Proxy > VoIP Proxy Settings“, you can configure the VoIP proxy for your R&S Unified Firewall:

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 Firewall uses to forward the VoIP connections.
„Activate SIP Proxy“	Select this checkbox if you want R&S Unified Firewall 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.
„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 Firewall 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.

H Reverse Proxy

Under „UTM > Reverse Proxy“ you can manage your backends, frontends and reverse proxy settings.

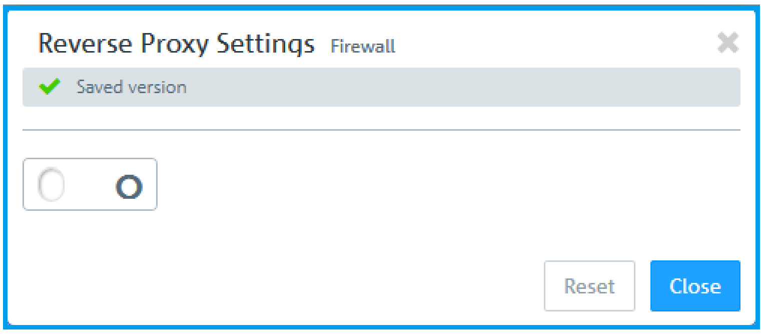
A reverse proxy is useful when a public website is hosted on your own network.

When the reverse proxy is active, the R&S Unified Firewall 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 Firewall 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.

H.1 Reverse Proxy Settings

The „UTM > Reverse Proxy > Reverse Proxy Settings“ allow you to activate and deactivate the reverse proxy in general.



Reverse Proxy Settings Firewall

✓ Saved version

Bild H-1: 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.

H.2 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.

H.3 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.
„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.

Field	Description
„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.