LCOS FX 11.1

Benutzerhandbuch

12/2024

LANCOM SYSTEMS

Inhalt

Copyright

Alle Angaben in dieser Dokumentation sind nach sorgfältiger Prüfung zusammengestellt worden, gelten jedoch nicht als Zusicherung von Produkteigenschaften. LANCOM Systems haftet ausschließlich in dem Umfang, der in den Verkaufs- und Lieferbedingungen festgelegt ist.

Das Produkt enthält separate Komponenten, die als sogenannte Open Source Software eigenen Lizenzen, insbesondere der General Public License (GPL), unterliegen. Sofern die jeweilige Lizenz dies verlangt, werden Quelldateien zu den betroffenen Software-Komponenten auf Anfrage bereitgestellt. Bitte senden Sie eine E-Mail an *gpl@lancom.de*.

Produkte von LANCOM Systems enthalten Software, die vom „OpenSSL Project" für die Verwendung im „OpenSSL Toolkit" entwickelt wurde (*www.openssl.org*).

Produkte von LANCOM Systems enthalten kryptographische Software, die von Eric Young (*eay@cryptsoft.com*) geschrieben wurde.

Produkte von LANCOM Systems enthalten Software, die von der NetBSD Foundation, Inc. und ihren Mitarbeitern entwickelt wurde.

Produkte von LANCOM Systems enthalten das LZMA SDK, das von Igor Pavlov entwickelt wurde.

Bitdefender SDK © Bitdefender 1997-2024

LANCOM Systems GmbH

A Rohde & Schwarz Company

Adenauerstr. 20/B2

52146 Würselen

Deutschland

www.lancom-systems.de

1 Über dieses Handbuch

LCOS FX ist das Betriebssystem für LANCOM R&S®Unified Firewalls und Teil der LANCOM Betriebssystem-Familie.

Die LANCOM Betriebssysteme sind die vertrauenswürdige Grundlage für das gesamte LANCOM Produktportfolio. Jedes Betriebssystem verkörpert die LANCOM Werte **Sicherheit**, **Zuverlässigkeit** und **Zukunftsfähigkeit**.

- **Für höchste Sicherheit Ihrer Netzwerke**

  wird jedes LANCOM Betriebssystem in gewohnter Qualität von unseren Entwicklern sorgfältig gepflegt und weiterentwickelt. Garantiert Backdoor-frei.

- **Sie stehen für größtmögliche Zuverlässigkeit,**

  denn über die gesamte Lebenszeit eines Produktes werden regelmäßig Release Updates, Security Updates und Major Releases zur Verfügung gestellt.

- **Als Grundlage maximaler Zukunftsfähigkeit Ihrer Netzwerke**

  stehen sie im Zuge der LANCOM Lifecycle-Richtlinien für alle LANCOM Produkte kostenlos zur Verfügung, inklusive neuer Major Features.

Das LANCOM R&S®Unified Firewall Benutzerhandbuch beschreibt die Funktionalitäten von LANCOM R&S®Unified Firewalls.

LANCOM R&S®Unified Firewalls vereinen Firewall, Intrusion Prevention, Anwendungskontrolle, Web-Filter, Anti-Virus-Schutz und viele weitere Funktionen in einem einzigen System.

Abbildung 1: LANCOM R&S®Unified Firewalls

Dieses Dokument gilt für alle LANCOM R&S®Unified Firewall-Modelle.

Je nach vorliegender Lizenz kann das Produkt individuelle Funktionen aufweisen, die von anderen Modellen abweichen. Weitere Informationen zu Ihrem spezifischen Modell finden Sie im jeweiligen Datenblatt.

Im Folgenden erhalten Sie weitere Informationen zu diesem Dokument.

1.1 Zielgruppe

Dieses Handbuch ist für den Netzwerk- oder Computertechniker bestimmt, der für die Installation und Konfiguration der LANCOM R&S®Unified Firewalls zuständig ist sowie für Mitarbeiter, die über den Webclient Regeln für die Filterung des Datenverkehrs festlegen.

Um dieses Dokument effektiv nutzen zu können, sollten Sie, abhängig von Ihrer Zuständigkeit, über die folgenden Fähigkeiten verfügen:

- Für die Installation und Konfiguration der Hardware sollten Sie mit Telekommunikationsgeräten und Installationsverfahren vertraut sein. Sie sollten außerdem über ausreichende Erfahrung als Netzwerk- oder Systemadministrator verfügen.
- Zur Festlegung der Filterregeln müssen Sie grundlegende TCP/IP-Netzwerkkonzepte verstehen.

1.2 Inhalt dieses Benutzerhandbuchs

Der Inhalt dieses Benutzerhandbuchs soll Ihnen bei der Installation und Konfiguration von LANCOM R&S®Unified Firewalls behilflich sein.

Dieses Dokument enthält die folgenden Kapitel:

- *Inbetriebnahme* auf Seite 7

  Loggen Sie sich auf ihrer LANCOM R&S®Unified Firewall ein, um das System für Ihr Netzwerk einzurichten.
- *Benutzeroberfläche* auf Seite 20

  Die Abschnitte dieses Kapitels beschreiben die Elemente der Benutzeroberfläche von LANCOM R&S®Unified Firewalls.

Wir sind bestrebt, eine Dokumentation zur Verfügung zu stellen, die Ihren Bedürfnissen entspricht. Um die Dokumentation zu verbessern, senden Sie uns Fehler, Anregungen oder Kommentare an unser *Support-Portal*.

Wenn Sie Ihr Feedback senden, geben Sie den Titel und das Datum des Dokuments auf der Titelseite an.

1.3 Konventionen

In diesem Kapitel werden die typografischen Konventionen und andere Bezeichnungen erläutert, die zur Darstellung der Informationen in diesem Handbuch verwendet werden.

Elemente der webbasierten, grafischen Benutzeroberfläche (GUI, oder „Webinterface“) werden folgendermaßen angezeigt:

Konvention	Beschreibung
Grafische Elemente der Benutzeroberfläche	Alle Namen von Elementen der grafischen Benutzeroberfläche auf dem Bildschirm, wie z. B. Menüpunkte, Schaltflächen, Kontrollkästchen, Dialogfelder, Listennamen, sind fett gedruckt.
Übergeordneter Menüpunkt > **Untermenü-Element**	Eine Abfolge von Menübefehlen wird durch größer als Zeichen zwischen den Menüpunkten und die gesamte Abfolge in Fettschrift angezeigt. Wählen Sie das Untermenü-Element vom übergeordneten Menüpunkt.
[Keys]	Die Key-Namen sind in eckige Klammern gefasst.
`Listenoptionen`, `wörtlicher Text`, `Dateinamen`, `Befehle`, `Programmcode`	Listenoptionen, wörtlicher Text, Dateinamen, Befehle, Codierbeispiele und Bildschirmausgaben erscheinen in nichtproportionaler Schrift.
Links	Links, die Sie anklicken können (z. B. Verweise auf andere Teile in diesem Handbuch), werden in blauer Schrift angezeigt.
Referenzen	Referenzen zu Teilen der Gerätedokumentation werden in Kursiv dargestellt.
`<NAME>` `<Sitzungs-Timeout>`	Parameter und Platzhalter erscheinen in nichtproportionaler Schrift und in spitzen Klammern.
PDF-Datei ZIP-Archiv	Dateitypen erscheinen in Großbuchstaben.

Anmerkungen

Dieses Handbuch enthält die folgenden Formen von Hervorhebungen, um Sie auf bestimmte Informationen aufmerksam zu machen oder Ihnen zusätzliche Informationen zu geben:

Diese Hervorhebung enthält zusätzliche Informationen, die Ihnen die Arbeit erleichtern können.

Dies ist ein Hinweis. Dieser Hinweis enthält wichtige Zusatzinformationen zum Produkt oder dessen Verwendung.

Diese Hervorhebung markiert sicherheitsrelevante Informationen. Nichtbeachtung kann LANCOM R&S®Unified Firewalls gefährden, oder Ihre Netzwerksicherheit beeinträchtigen.

1.4 Weitere Quellen

Dieser Abschnitt enthält zusätzliche Dokumente und weitere Informationsquellen zu LANCOM R&S®Unified Firewalls.

Beachten Sie die folgenden Dokumente und Quellen:

- ***Datenblätter*** fassen die technischen Eigenschaften der verschiedenen LANCOM R&S®Unified Firewall-Modelle zusammen.
- ***Release Notes*** enthalten aktualisierte Informationen zu jedem neuen Release von LCOS FX.
- ***LANCOM Support Knowledge Base*** enthält Informationen und Schritt-für-Schritt-Anleitungen für viele Themen rund um LCOS FX.

Für zusätzliche Dokumente, wie z. B. technische Spezifikationen, besuchen Sie unsere *Produkt-Webseite*

2 Inbetriebnahme

In diesem Dokument finden Sie alle zur Einrichtung und Konfiguration Ihres LANCOM R&S®Unified Firewall-Geräts benötigten Informationen.

Befolgen Sie zur Inbetriebnahme die unten beschriebenen Schritte.

Beim ersten Start nach der Lieferung oder nach einer Neuinstallation läuft LANCOM R&S®Unified Firewall für 30 Tage als Testversion. Weitere Informationen finden Sie unter *Lizenz* auf Seite 47.

2.1 Ersteinrichtung

1. Nehmen Sie das vorinstallierte LANCOM R&S®Unified Firewall-Gerät aus der Verpackung.
2. Verbinden Sie ein Patchkabel mit dem Port mit der Beschriftung **eth1** auf der Frontseite Ihres LANCOM R&S®Unified Firewall-Geräts und mit dem Ethernet-Port Ihres Computers.
3. Verbinden Sie ein Patchkabel mit dem Port mit der Beschriftung **eth0** auf der Frontseite Ihres LANCOM R&S®Unified Firewall-Geräts und mit dem LAN-Port des Geräts (z. B. Ihrem Router, DSL- oder Kabelmodem), welches Sie von Ihrem Provider für den Zugang zum Internet bekommen haben. Stellen Sie sicher, das dieses Gerät eingeschaltet ist.
4. Stellen Sie sicher, dass der Netzwerkadapter Ihres Computer auf „IP-Adresse automatisch konfigurieren" eingestellt ist.
5. Schalten Sie Ihr LANCOM R&S®Unified Firewall-Gerät ein.
6. Starten Sie einen Webbrowser auf Ihrem Computer.
7. Geben Sie in der Adressleiste des Browsers *https://192.168.1.254:3438* ein.
8. Erstellen Sie eine Ausnahme für die Zertifikatwarnung.

   Die LANCOM R&S®Unified Firewall-Loginseite erscheint.
9. Geben Sie auf der Loginseite des LANCOM R&S®Unified Firewall-Webclients `admin` als **Benutzername** und das voreingestellte **Kennwort** `admin` ein.

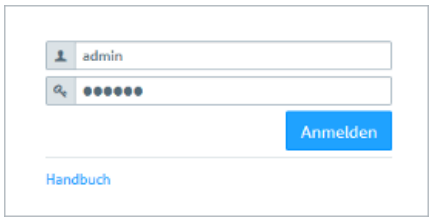


Abbildung 2: Loginseite des LANCOM R&S®Unified Firewall Webclients

10. Klicken Sie auf **Anmelden**.
11. Nach dem ersten Login mit den voreingestellten Anmeldedaten werden Sie vom System aufgefordert, die Endnutzer-Lizenzvereinbarung (EULA) zu akzeptieren und anschließend die folgenden beiden Passwörter zu ändern:

    › Das Passwort für den Benutzer *admin* – Sie benötigen dieses Passwort, um sich beim LANCOM R&S®Unified Firewall-Webclient anzumelden.

› Das Support-Passwort – Das Support-Passwort ist das Passwort, mit dem der technische Support sich auf Ihrer LANCOM R&S®Unified Firewall anmelden kann. Bewahren Sie es sicher und vor unbefugtem Zugriff geschützt auf.

Das neue Benutzerpasswort und das Support-Passwort dürfen aus nicht weniger als acht und nicht mehr als 255 Zeichen bestehen. Erlaubt sind lateinische Buchstaben inklusive deutsche Umlaute sowie Zahlen und Sonderzeichen. Kyrillisch oder andere Schriften nicht. Es müssen Zeichen aus mindestens drei der Kategorien Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen verwendet werden.

Erlaubter Zeichensatz:

```
[A-Za-z0-9]^_-`´~.,ß'!@#"§$%^&*()-=+\][{}|:/?>_<@äöüÄÖÜ*$
```

Dieser Schritt ist verpflichtend.

12. Klicken Sie auf **Akzeptieren & Anmelden**, um die neuen Passwörter und die EULA zu akzeptieren.

Der Setup-Assistent erscheint.

Mit Ausnahme der Sprachauswahl am Anfang des Setup-Assistenten können Sie den Assistenten jederzeit über die Schaltfläche **Assistent abbrechen** beenden. Nach einem Abbruch des Assistenten können Sie eine manuelle Einrichtung vornehmen, also mit den Schritten *Internetverbindung konfigurieren* auf Seite 14 und *Internetzugang aktivieren* auf Seite 16 fortfahren.

Bis auf wenige Ausnahmen können Sie innerhalb des Setup-Assistenten mit den Schaltflächen **Zurück** und **Weiter** navigieren.

13. Wählen Sie die Sprache für den Setup-Assistenten und den Webclient aus. Sie können die Sprache des Webclient später nach Bedarf jederzeit umschalten.

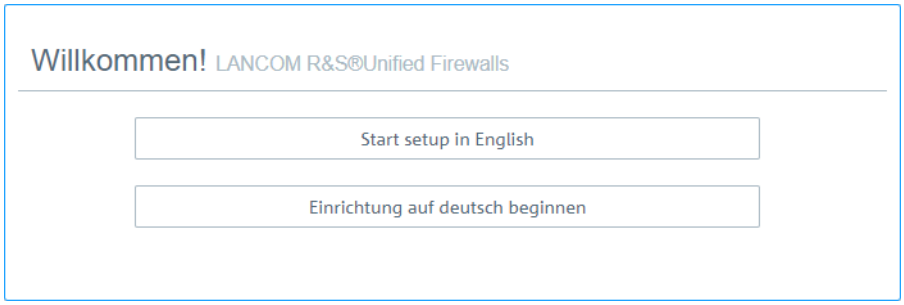


Abbildung 3: Willkommensseite des Setup-Assistenten

14. Wenn Sie die Konfiguration einer vorherigen Installation wiederherstellen wollen, dann klicken Sie auf **Auswählen**, um eine Backup-Datei auszuwählen. Geben Sie das zugehörige Backup-Passwort an. Klicken Sie danach auf **Backup wiederherstellen und neu starten**.

Anschließend wird der Setup-Assistent beendet, die Konfiguration aus dem Backup wiederhergestellt und die Firewall neu gestartet.

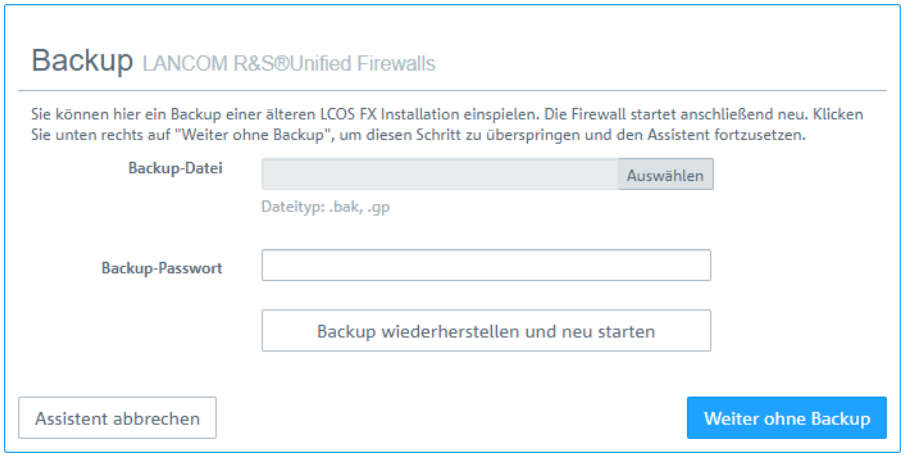


Abbildung 4: Optional eine vorhandene Konfiguration aus einem Backup wiederherstellen

Alternativ fahren Sie für eine Neuinstallation mit **Weiter ohne Backup** fort.

15. Konfigurieren Sie die folgenden allgemeinen Einstellungen der Firewall:

Firewall-Hostname

Geben Sie Ihrer Firewall einen Namen, der als Hostname verwendet wird.

Zeitzone

Die Zeitzone wird mit der momentan im Browser eingestellten Zeitzone vorbelegt. Ändern Sie diese Einstellung bei Bedarf.

Nutzungs-Statistiken senden

Erlauben Sie optional, dass Informationen über Auslastung und Zustand der Firewall aufgezeichnet und an die LANCOM Systems GmbH übermittelt werden. Es werden keine persönlichen Informationen und keine Bestandteile des über die Firewall erfolgten Datenverkehrs übertragen.

Sie können diese Einstellung später wieder ändern. Siehe auch *Allgemeine Einstellungen* auf Seite 35.

Absturzberichte senden

Erlauben Sie optional, dass im Fehlerfall allgemeine Informationen zum Sytemzustand, zur aktuellen Systemkonfiguration und zum aufgetretenen Fehler an die LANCOM Systems GmbH übertragen werden. Die Daten werden nur zur Fehleranalyse verwendet und anschließend wieder gelöscht. Es erfolgt keine Weitergabe irgendwelcher Daten an Dritte.

Sie können diese Einstellung später wieder ändern. Siehe auch *Allgemeine Einstellungen* auf Seite 35.

Abbildung 5: Allgemeine Einstellungen der Firewall

16. Selektieren Sie als **Internet-Interface** den Firewall-Port (Standard: **eth0**), mit dem dass Gerät verbunden ist, welches Sie von Ihrem Provider für den Zugang zum Internet bekommen haben. Geben Sie dann Ihre Option für den **Internetzugriff** an:

    Abhängig von Ihrer Auswahl können Sie für die Auswahl notwendige Daten konfigurieren.

    DHCP

    Die IP-Adresse für dieses Interface wird über DHCP bezogen.

    Statische Konfiguration

    Geben Sie die **IP-Adresse mit Präfix-Länge** (CIDR-Notation), den **Standard-Gateway** und den **DNS-Server** an.

    ADSL / SDSL

    Geben Sie den **Benutzernamen** und das **Passwort** an, die Sie von Ihrem Internet-Provider erhalten haben.

VDSL

Geben Sie die **VLAN-ID**, den **Benutzernamen** und das **Passwort** an, die Sie von Ihrem Internet-Provider erhalten haben.

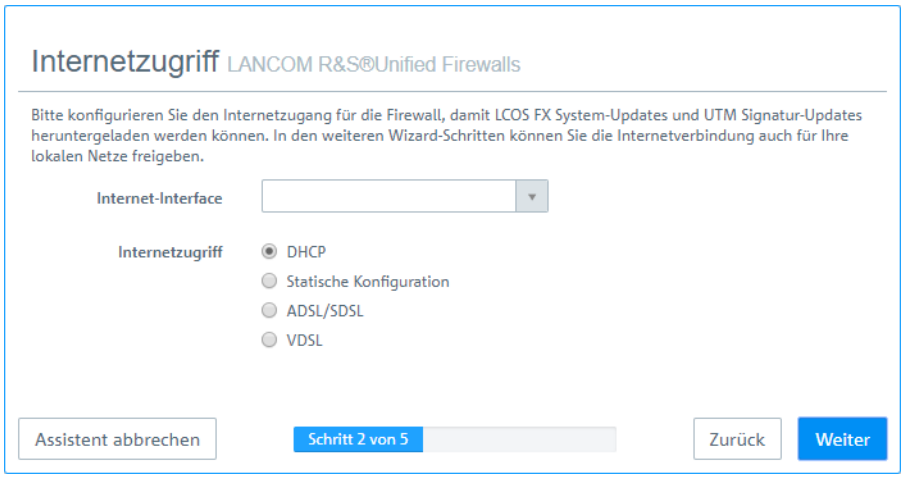


Abbildung 6: Internetzugang

17. Konfigurieren Sie hier das lokale Netzwerk, mit dem die Firewall verbunden ist oder später sein soll. Jede Zeile entspricht einer Netzwerkschnittstelle der Firewall (Spalte **Interface**).

Sie können eine Schnittstelle aktivieren / deaktivieren, je nachdem, ob Sie sie verwenden möchten oder nicht (Spalte **Aktiv**). Die Internet-Schnittstelle kann nicht deaktiviert werden.

Geben Sie im Feld **IP und Präfixlänge** die IP ein, die die Firewall auf dieser Schnittstelle verwenden soll, einschließlich der Präfixlänge (CIDR-Notation). Wenn Sie das Feld leer lassen, hat die Firewall keine IP-Verbindung auf dieser Schnittstelle. In diesem Fall können Sie nicht über diese Schnittstelle auf die Firewall zugreifen und können keinen DHCP-Server oder Web- oder Mail-Zugang für alle Clients zulassen, die über diese Schnittstelle verbunden sind. Jede Schnittstelle sollte ein eigenes Subnetz haben.

Um einen DHCP-Server auf einer Schnittstelle zu aktivieren, aktivieren Sie das Kontrollkästchen **DHCP-Server aktivieren** für eine Schnittstelle. Der DHCP-Bereich hängt von der dieser Schnittstelle zugeordneten Firewall-IP ab und wird auf den größten im Subnetz verfügbaren kontinuierlichen Bereich voreingestellt.

Sie können typischen Internetverkehr (**Web** und **E-Mail**) für Clients zulassen, die mit einer Schnittstelle verbunden sind, indem Sie das entsprechende Kontrollkästchen für eine Schnittstelle aktivieren. **Web** ermöglicht es Clients, sich

über HTTP mit dem Internet zu verbinden. **E-Mail** ermöglicht SMTP-, POP3- und IMAP-Verkehr. Dazu gehören auch die SSL / TLS-Versionen dieser Protokolle.

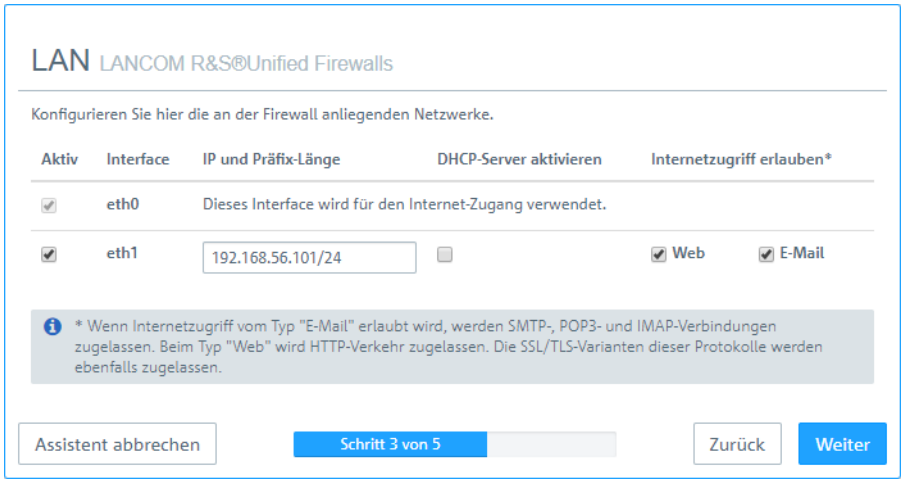


Abbildung 7: Lokale Netzwerke

18. Wählen Sie die Sicherheitsfeatures **Anti-Virus**, **IDS** und / oder **Contentfilter** aus, die aktivert werden sollen. Abhängig von Ihrem Gerät sind evtl. nicht alle Features verfügbar.

Beim ersten Start nach der Lieferung oder nach einer Neuinstallation läuft die LANCOM R&S®Unified Firewall für 30 Tage als Testversion. Während des Testzeitraums können Sie kein Backup erstellen. Nach Ablauf des Testzeitraums bleibt die Firewall weiterhin mit Ihrer Konfiguration erhalten. Die UTM-Features werden deaktiviert und Sie können keine Änderungen mehr speichern.

Mehr Information hierzu finden Sie unter *Lizenz* auf Seite 47.

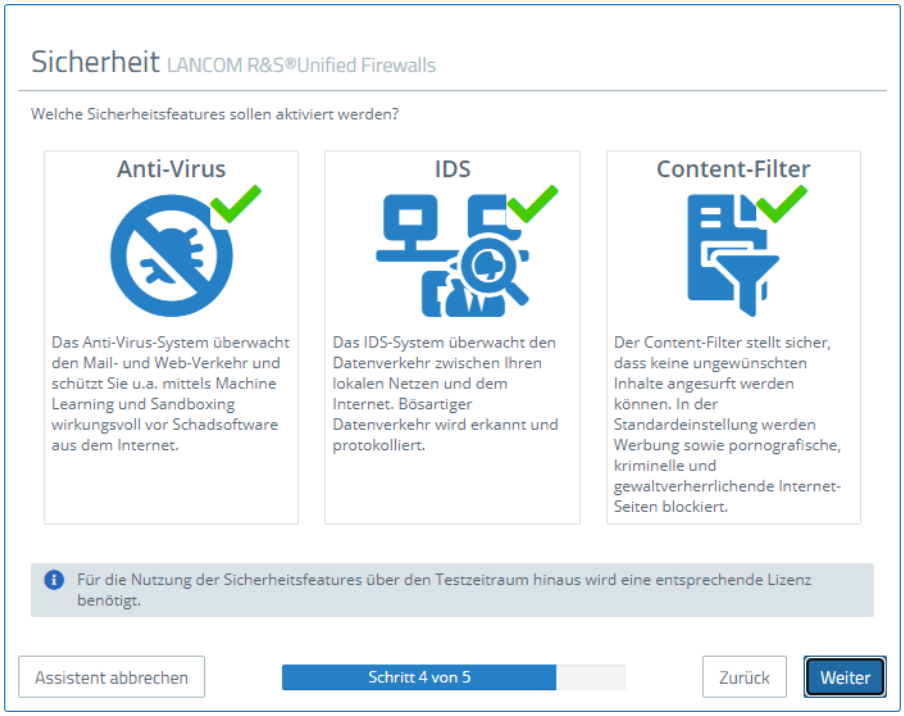


Abbildung 8: Sicherheitsfeatures

19. Hier sehen Sie eine Zusammenfassung der gemachten Einstellungen und können ggfs. zurückgehen, um diese anzupassen. Klicken Sie **Fertigstellen**, wenn alles in Ordnung ist.

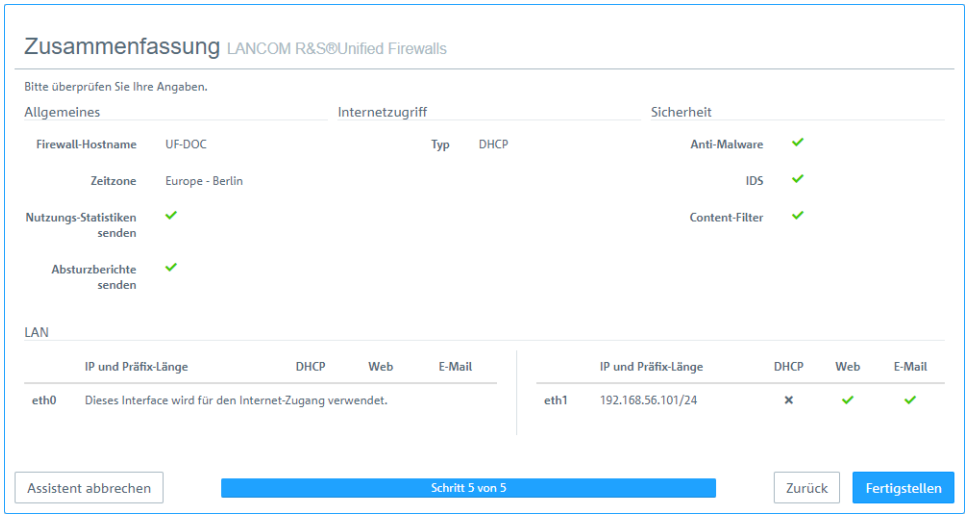


Abbildung 9: Zusammenfassung der gemachten Einstellungen

20. Warten Sie ab bis der Setup-Assistent fertig ist. Nun werden Ihnen die Links angezeigt, über die Sie den Webclient nach Ablauf des Setup-Assistenten erreichen können. Klicken Sie entweder auf einen dieser Links oder auf OK, um zum Webclient zu wechseln.

Wenn Sie das automatisch erzeugt Zertifikat für den Web-Proxy verwenden wollen, dann laden Sie es herunter und rollen es auf Ihre Clients aus.

Abbildung 10: Fertigstellung

Falls Sie den Setup-Assistenten erneut verwenden wollen, dann müssen Sie Ihre Firewall auf die Werkseinstellungen zurücksetzen. Siehe hierzu *Kopfzeile* auf Seite 21.

2.2 Internetverbindung konfigurieren

Dieses Kapitel beschreibt, wie Sie ihre Internetverbindung einrichten können.

1. Verbinden Sie ein Patchkabel mit dem **eth0**-Port auf der Frontseite Ihrer LANCOM R&S®Unified Firewall und mit dem LAN-Port des Geräts, das Sie von Ihrem Anbieter für den Internetzugang erhalten haben (z. B. ein Router oder ein DSL- oder Kabelmodem).
2. Navigieren Sie in der Navigationsleiste zu **Netzwerk** > **Verbindungen**.

   Rechts neben der Navigationsleiste öffnet sich die Objektleiste.
3. Um zu sehen, welche Netzwerkverbindung welchem Interface zugewiesen ist, klicken Sie in der rechten oberen Ecke der Objektleiste auf ».

   Die Objektleiste erweitert sich.
4. Löschen Sie die voreingestellte Verbindung auf eth0, indem Sie in der letzten Tabellenspalte in derselben Zeile auf 🗑 (Klicken zum Löschen) klicken.
5. Fahren Sie je nach Typ Ihrer Internetverbindung gemäß einem der folgenden drei Ansätze fort:
   - *Verbindung über Wählleitung*
   - *Kabel- oder Routerverbindung mit dynamischer IP-Adresse*
   - *Statische Internetverbindung mit statischer IP-Adresse*

2.2.1 Verbindung über Wählleitung

2.2.1.1 Netzwerkverbindung konfigurieren

Führen Sie diesen Schritt aus, wenn Sie eine PPTP-Verbindung konfigurieren möchten. Bei PPPoE-Verbindungen entfällt dieser Schritt.

1. Um eine neue Netzwerkverbindung anzulegen, klicken Sie in der Objektleiste auf ⊕ (Neuen Eintrag erstellen).

   Der Dialog **Netzwerk-Verbindung** öffnet sich. Damit können Sie eine Netzwerkverbindung konfigurieren.
2. Geben Sie im Eingabefeld **Name** einen Namen für Ihre Netzwerkverbindung ein.
3. Wählen Sie in der Drop-down-Liste **Interface** den Menüeintrag **eth0** aus.
4. Wählen Sie in der Drop-down-Liste **Typ** den Menüeintrag **Static** aus.
5. Geben Sie im Eingabefeld **IP-Adressen** die IP-Adresse und die Subnetzmaske für die Netzwerkverbindung ein.

   ⓘ Bei dieser IP-Adresse handelt es sich um die Client- / NIC-IP-Adresse, die Sie von Ihrem Provider erhalten.
6. Klicken Sie rechts auf ⊕, um Ihren Eintrag zur Liste der IP-Adressen hinzuzufügen.
7. Klicken Sie auf **Erstellen**.

   Der Dialog **Netzwerk-Verbindung** schließt sich. Das neue Interface wird zur Liste der verfügbaren Netzwerkverbindungen in der Objektleiste hinzugefügt.

2.2.1.2 PPP-Interface erstellen

1. Navigieren Sie zu **Netzwerk** > **Interfaces** > **PPP-Interfaces**.
2. Um ein neues PPP-Interface zu erstellen, klicken Sie in der Leiste mit der Objektliste auf ⊕ (Neuen Eintrag erstellen).

   Der Dialog **PPP-Interface** öffnet sich. Darin können Sie ein PPP-Interface konfigurieren.

3. Wählen Sie in der Drop-down-Liste **Haupt-Interface** den Menüeintrag **eth0** aus.
4. Sofern Ihr Provider es nicht anders vorgibt, belassen Sie die weiteren Einstellungen auf ihren Standardwerten.
5. Klicken Sie auf **Erstellen**.

   Der Dialog **PPP-Interface** schließt sich. Das neue Interface wird zur Liste der verfügbaren PPP-Interfaces in der Objektleiste hinzugefügt.

2.2.1.3 PPP-Verbindung erstellen

1. Navigieren Sie zu **Netzwerk** > **Verbindungen** > **PPP-Verbindungen**.
2. Um eine neue PPP-Verbindung anzulegen, klicken Sie in der Objektleiste auf ⊕ (Neuen Eintrag erstellen).

   Der Dialog **PPP-Verbindung** öffnet sich. Damit können Sie eine PPP-Verbindung konfigurieren.
3. Geben Sie im Eingabefeld **Name** einen Namen für Ihre PPP-Verbindung ein.
4. Wählen Sie aus der Drop-down-Liste **Interface** das PPP-Interface aus, das Sie unter *PPP-Interface erstellen* auf Seite 14 erstellt haben.
5. Wählen Sie aus der Drop-down-Liste **Typ** Ihren Verbindungstyp aus.
6. Geben Sie die Anmeldedaten ein, die Sie von Ihrem Provider erhalten haben.

   ⓘ Falls Sie eine PPTP-Verbindung erstellen, geben Sie im Eingabefeld **PPTP-Server-IP** die IP-Adresse des Modems ein, welches Sie von Ihrem Provider erhalten haben.
7. Sofern Ihr Provider es nicht anders vorgibt, belassen Sie die weiteren Einstellungen auf ihren Standardwerten.
8. Klicken Sie auf **Erstellen**.

   Der Dialog **PPP-Verbindung** schließt sich. Die neue Verbindung wird zur Liste der verfügbaren PPP-Verbindungen in der Objektleiste hinzugefügt.
9. Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

   Sie haben Ihre Internetverbindung konfiguriert.

2.2.2 Kabel- oder Routerverbindung mit dynamischer IP-Adresse

1. Navigieren Sie zu **Netzwerk** > **Verbindungen** > **Netzwerk-Verbindungen**.
2. Um eine neue Netzwerkverbindung anzulegen, klicken Sie in der Objektleiste auf ⊕ (Neuen Eintrag erstellen).

   Der Dialog **Netzwerk-Verbindung** öffnet sich. Damit können Sie eine Netzwerkverbindung konfigurieren.
3. Geben Sie im Eingabefeld **Name** einen Namen für Ihre Netzwerkverbindung ein.
4. Wählen Sie in der Drop-down-Liste **Interface** den Menüeintrag **eth0** aus.
5. Wählen Sie in der Drop-down-Liste **Typ** den Menüeintrag **DHCP** aus.
6. Setzen Sie den Haken im Kontrollkästchen **DNS-Server beziehen**
7. Setzen Sie den Haken im Kontrollkästchen **Domain beziehen**
8. Klicken Sie auf **Erstellen**.

   Der Dialog **Netzwerk-Verbindung** schließt sich. Die neue Verbindung wird zur Liste der verfügbaren Netzwerkverbindungen in der Objektleiste hinzugefügt.
9. Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

   Sie haben Ihre Internetverbindung konfiguriert.

2.2.3 Statische Verbindung mit statischer IP-Adresse

2.2.3.1 Netzwerkverbindung konfigurieren

1. Navigieren Sie zu **Netzwerk** > **Verbindungen** > **Netzwerk-Verbindungen**.
2. Um eine neue Netzwerkverbindung anzulegen, klicken Sie in der Objektleiste auf ⊕ (Neuen Eintrag erstellen).

   Der Dialog **Netzwerk-Verbindung** öffnet sich. Damit können Sie eine Netzwerkverbindung konfigurieren.
3. Geben Sie im Eingabefeld **Name** einen Namen für Ihre Netzwerkverbindung ein.
4. Wählen Sie in der Drop-down-Liste **Interface** den Menüeintrag **eth0** aus.
5. Wählen Sie in der Drop-down-Liste **Typ** den Menüeintrag **Static** aus.
6. Geben Sie im Eingabefeld **IP-Adressen** die IP-Adresse und die Subnetzmaske für Ihre Netzwerkverbindung ein.

   ⓘ Die IP-Adresse erhalten Sie von Ihrem Provider.
7. Klicken Sie rechts auf ⊕, um Ihren Eintrag zur Liste der IP-Adressen hinzuzufügen.

2.2.3.2 DNS-Einstellungen konfigurieren

1. Wechseln Sie im Fenster **Netzwerk-Verbindung** auf den Tab **WAN**.
2. Setzen Sie den Haken im Kontrollkästchen **Standard Gateway setzen**
3. Geben Sie im Eingabefeld **Standard-Gateway** die Standard-IP-Adresse Ihres Gateways ein.
4. Klicken Sie auf **Erstellen**.

   Der Dialog **Netzwerk-Verbindung** schließt sich. Die neue Verbindung wird zur Liste der verfügbaren Netzwerkverbindungen in der Objektleiste hinzugefügt.
5. Navigieren Sie zu **Netzwerk** > **DNS-Einstellungen**.

   Der Dialog **DNS-Einstellungen** öffnet sich. Damit können Sie die DNS-Einstellungen konfigurieren.
6. Entfernen Sie den Haken im Kontrollkästchen **Bezogenene Server**.

   Die Eingabefelder **1. Nameserver**/**2. Nameserver** können nun bearbeitet werden.
7. Geben Sie in den Eingabefeldern **1. Nameserver** und **2. Nameserver** die IP-Adressen der DNS-Server ein, die Sie von Ihrem Provider erhalten haben.
8. Um die Einstellungen zu speichern, klicken Sie auf **Speichern**.

   Der Dialog **DNS-Einstellungen** schließt sich.
9. Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

Sie haben Ihre Internetverbindung konfiguriert.

2.3 Internetzugang aktivieren

2.3.1 Internet-Objekt erstellen

1. Navigieren Sie zu **Desktop** > **Desktop-Objekte** > **Internet-Objekte**.
2. Klicken Sie in der Objektleiste auf ⊕ (Neuen Eintrag erstellen), um ein neues Internet-Objekt zu erstellen.

   Der Dialog **Internet-Objekt** öffnet sich. Damit können Sie ein Internet-Objekt konfigurieren.

3. Geben Sie unter **Objekt-Name** einen Namen für das Internet-Objekt an.
4. Wählen Sie aus der Drop-down-Liste **Verbindungen** Ihre Internetverbindung aus.

   Hinweise zur Erstellung einer Internetverbindung erhalten Sie unter *Internetverbindung konfigurieren* auf Seite 14.
5. Klicken Sie rechts auf ⊕, um Ihren Eintrag zur Liste der Verbindungen hinzuzufügen.
6. Klicken Sie auf **Erstellen**.

   Der Dialog **Internet-Objekt** schließt sich. Das neue Objekt wird zur Liste der verfügbaren Internet-Objekte in der Objektleiste hinzugefügt.

   Weitere Informationen finden Sie unter *Desktop-Objekte* auf Seite 116.

2.3.2 Lokale Netzwerkverbindung konfigurieren

1. Nutzen Sie ein Patchkabel, um einen der Ports mit der Beschriftung **ethX** (ausgenommen **eth0**, da dieser für die Internetverbindung verwendet wird) auf der Frontseite Ihres LANCOM R&S®Unified Firewall Geräts mit einem der Ethernet-Ports auf Ihrem Netzwerkverteiler zu verbinden.
2. Navigieren Sie zu **Netzwerk** > **Verbindungen** > **Netzwerk-Verbindungen**.
3. Klicken Sie in der Leiste mit der Objektliste auf ⊕ (Neuen Eintrag erstellen), um eine neue Netzwerkverbindung zu erstellen.

   Der Dialog **Netzwerk-Verbindung** öffnet sich. Damit können Sie eine Netzwerkverbindung konfigurieren.
4. Geben Sie im Eingabefeld **Name** einen Namen für Ihre Netzwerkverbindung ein.
5. Wählen Sie in der Drop-down-Liste **Interface** den Port aus, an den Sie Ihren Netzwerkverteiler angeschlossen haben.
6. Wählen Sie in der Drop-down-Liste **Typ** den Typ **Static** aus.
7. Geben Sie im Eingabefeld **IP-Adressen** die IP-Adresse dieser Verbindung passend zu ihrem lokalen Netzwerk in CIDR-Schreibweise ein (IP-Adresse gefolgt von einem Schrägstrich „/" und der Anzahl der in der Subnetzmaske festgelegten Bits, beispielsweise `192.168.50.1/24`).
8. Klicken Sie rechts auf ⊕, um Ihren Eintrag zur Liste der IP-Adressen hinzuzufügen.
9. Klicken Sie auf **Erstellen**.

   Der Dialog **Netzwerk-Verbindung** schließt sich.

2.3.3 Netzwerk-Objekt erstellen

1. Navigieren Sie zu **Desktop** > **Desktop-Objekte** > **Netzwerke**.
2. Klicken Sie in der Leiste mit der Objektliste auf ⊕ (Neuen Eintrag erstellen), um ein neues Netzwerk-Objekt zu erstellen.

   Der Dialog **Netzwerk** öffnet sich. Damit können Sie eine Netzwerkverbindung konfigurieren.
3. Geben Sie im Eingabefeld **Name** einen Namen für das Netzwerk-Objekt ein.
4. Wählen Sie in der Drop-down-Liste **Interface** die Netzwerkverbindung aus, die Sie unter *Lokale Netzwerkverbindung konfigurieren* auf Seite 17 erstellt haben.
5. Geben Sie unter **Netzwerk-IP** die IP-Adresse Ihres lokalen Netzwerks ein.
6. Klicken Sie auf **Erstellen**.

   Der Dialog **Netzwerk** schließt sich. Das neue Objekt wird zur Liste der verfügbaren Netzwerk-Objekte in der Objektleiste hinzugefügt.

   Weitere Informationen finden Sie unter *Desktop-Objekte* auf Seite 116.

2.3.4 Firewall-Regeln für den Internetzugang konfigurieren

1. Richten Sie eine Verbindung zwischen dem Netzwerk-Objekt (siehe *Netzwerk-Objekt erstellen* auf Seite 17) und dem Internet-Objekt (siehe *Internet-Objekt erstellen* auf Seite 16) ein, die Sie in den vorigen Schritten erstellt haben:

   a. Klicken Sie auf die Schaltfläche in der Symbolleiste oben auf dem Desktop. Die Desktop-Objekte, die für diese Verbindung und mögliche weitere Verbindungen zwischen Desktop-Objekten ausgewählt werden können, werden durch gepunktete Kreise und Linien hervorgehoben.

   b. Wählen Sie ein Netzwerk-Objekt als Quellobjekt für die Verbindung aus, indem Sie auf das entsprechende Desktop-Objekt klicken.

   c. Wählen Sie ein Internet-Objekt als Zielobjekt für die Verbindung aus, indem Sie auf das entsprechende Desktop-Objekt klicken.

   Sie werden automatisch zu **Desktop** > **Desktop-Verbindungen** weitergeleitet. Das Bearbeitungsfenster **Verbindung** öffnet sich.

   Alternativ können Sie auf die Schaltfläche im kreisförmigen Menü des Quellobjekts auf dem Desktop klicken und anschließend das Zielobjekt auswählen.

2. Richten Sie eine nach Ihren Bedürfnissen ausgerichtete Firewall-Regel mit HTTP und / oder HTTPS ein:

   a. Auf der rechten Seite des Browserfensters erscheint eine Liste der Dienste, auf welche die Firewall-Regel angewendet werden kann. Diese Liste ist in Kategorien unterteilt, die Dienste mit ähnlichen Funktionen zusammenfassen.

   Geben Sie in das Eingabefeld **Filter** `HTTP` oder `HTTPS` ein. Bereits während der Eingabe zeigt der Webclient diejenigen Dienste und Dienstgruppen an, die die eingegebenen Zeichen enthalten.

   Um **HTTP** und **HTTPS** aus der Kategorie **Internet** hinzuzufügen, klicken Sie jeweils auf ⊕.

   Die ausgewählten Dienste werden aus der Dienstauswahlliste entfernt und in der Tabelle **Regeln** angezeigt.

   b. Klicken Sie auf **Erstellen**.

   c. Der Dialog **Verbindung** schließt sich. Die neue Desktop-Verbindung wird zur Liste der verfügbaren Desktop-Verbindungen in der Objektleiste hinzugefügt.

   Weitere Informationen finden Sie unter *Einstellungen für Firewall-Regeln* auf Seite 30.

2.3.5 Desktopkonfiguration aktivieren

1. Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

Der Internetzugang ist aktiviert.

2.4 Firmware-Update

Es gibt zwei verschiedene Möglichkeiten ein Firmware-Update auf einer LANCOM R&S®Unified Firewall durchzuführen.

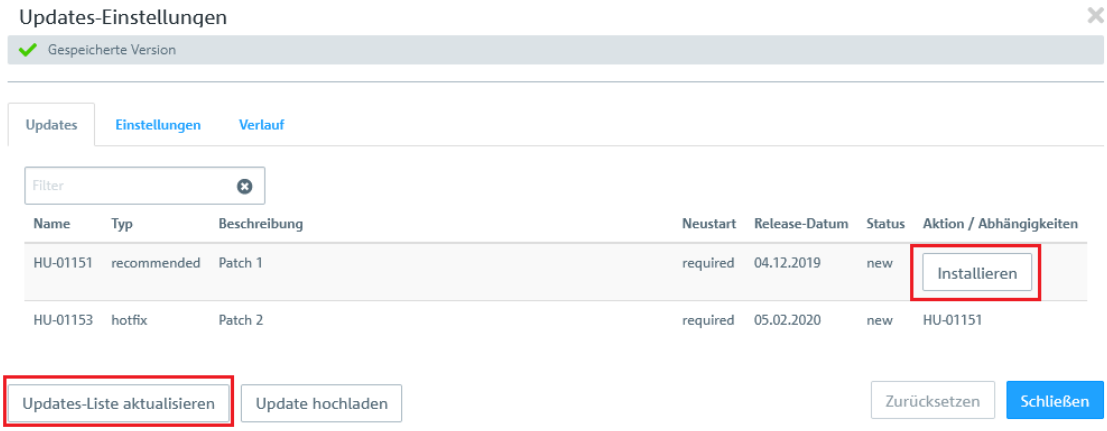
Zur erfolgreichen Durchführung eines Online Firmware-Update muss sichergestellt sein, dass die verwendete Internetverbindung mindestens eine Download-Bandbreite von 1MBit/s zur Verfügung stellt.

1. **Online Firmware-Update über die Web-Konfigurationsoberfläche:**

   › Öffnen Sie den Dialog **Firewall** > **Updates-Einst.**

› Hat die Unified Firewall ein neues Update bereits über ihren automatischen Suchmechanismus (siehe Registerkarte **Einstellungen**) gefunden, wird dieses in der Liste angezeigt und kann mit einem Klick auf die Schaltfläche **Installieren** durchgeführt werden.

Mit der Schaltfläche **Updates-Liste aktualisieren** können Sie die Suche nach einem Firmware-Update manuell anstoßen.



2. **Manuelles Firmware-Update per '*.iso'-Firmwaredatei:**

   Die Durchführung eines manuellen Firmware-Update per *.iso-Konfigurationsdatei ist in *diesem Knowledge Base Artikel* beschrieben.

   Beachten Sie, dass bei dieser Aktualisierungs-Variante die Lizenzierung Ihrer Unified Firewall nach der Übertragung von neuer Firmware und Backup-Datei zunächst gelöscht wird. Das Gerät befindet sich dann wieder im 30 Tage Testzeitraum!

   Um das Gerät wieder zu lizenzieren, müssen Sie die Lizenzdatei, welche Sie bei der Registrierung Ihrer Lizenz erhalten haben erneut in das Gerät einspielen. Siehe auch Abschnitt *Lizenz* auf Seite 47.

3 Benutzeroberfläche

Die Abschnitte dieses Kapitels beschreiben die Elemente der Benutzeroberfläche Ihrer LANCOM R&S®Unified Firewall.

Der LANCOM R&S®Unified Firewall-Webclient erfordert eine Bildschirmauflösung von mindestens 1024 × 786 Pixeln (XGA).

Wenn JavaScript aktiviert ist, werden die folgenden Browser ab der angegebenen Version unterstützt:

- Google Chrome 10
- Chromium 10
- Mozilla Firefox 12

Elemente des Webclients auf Seite 20 bietet eine Übersicht der Hauptkomponenten des Webclients.

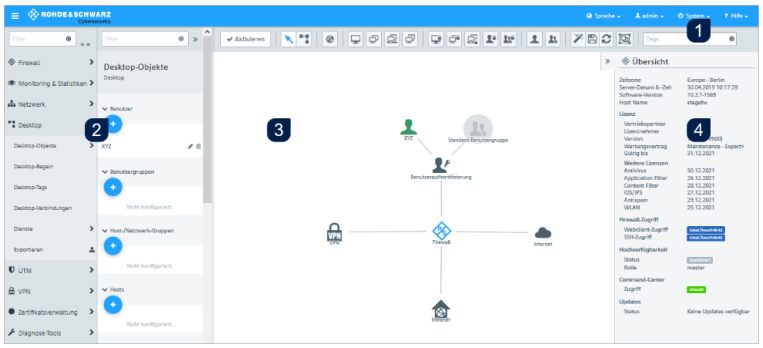
Symbole und Schaltflächen auf Seite 28 erklärt die Bedeutung der Symbole und Schaltflächen, die auf der Benutzeroberfläche und in diesem Handbuch häufig zur Anwendung kommen.

Einstellungen für Firewall-Regeln auf Seite 30 beschreibt, wie Sie eine Firewall-Regel für eine Verbindung zwischen zwei Desktopobjekten einrichten.

Menüreferenz auf Seite 33 gibt die Anordnung der Menüpunkte in der Navigationsleiste auf der linken Seite der Benutzeroberfläche wieder. Informationen zu den verfügbaren Optionen finden Sie im jeweiligen Abschnitt.

3.1 Elemente des Webclients

Der LANCOM R&S®Unified Firewall-Webclient hat ein standardmäßig in vier Bereiche unterteiltes Seitenlayout mit einer gemeinsamen Kopfzeile, einer Navigationsleiste links sowie einem Hauptinhaltsbereich (Desktop) und einem Infobereich rechts.



1. Kopfzeile
2. Navigationsbereich
3. Desktop
4. Infobereich

Abbildung 11: LANCOM R&S®Unified Firewall-Webclient

In den folgenden Abschnitten werden die in jedem Bereich angezeigten Informationen beschrieben.

3.1.1 Kopfzeile

Die Kopfzeile (1) enthält folgende Elemente (von links nach rechts):

Abbildung 12: Kopfzeile des LANCOM R&S®Unified Firewall-Webclients

1. ☰ Schaltfläche zum Ein- und Ausblenden der Navigationsleiste.
2. Rohde & Schwarz®Cybersecurity GmbH-Logo.
3. Sprachenmenü, mit dem Sie die Sprache des Webclients auswählen können.
4. Benutzermenü, mit dem Sie die aktuelle Sitzung beenden und zur Loginseite zurückkehren können.
5. Systemmenü, mit dem Sie LANCOM R&S®Unified Firewall herunterfahren, neu starten, auf die Werkseinstellungen zurücksetzen können oder einen Wiederherstellungspunkt auswählen.

   Wenn Sie Ihre LANCOM R&S®Unified Firewall auf die Werkseinstellungen zurücksetzen, dann können Sie optional auch alle Protokolldateien löschen lassen.

   Bei einer Aktualisierung der Firmware wird automatisch ein Wiederherstellungspunkt gesetzt. Falls nach einer bestimmten Zeit nach der Aktualisierung keine Anmeldung erfolgt, dann wird ein Fehler angenommen und abhängig von Ihren Einstellungen die vorherige Version wieder aktiviert. Siehe auch *Update-Einstellungen* auf Seite 54.
6. Ein Hilfemenü mit Links auf die PDF-Version des LANCOM R&S®Unified Firewall Benutzerhandbuchs, die *REST-API-Dokumentation* auf Seite 22, die *LANCOM Support Knowledge Base* und einige Tutorial Videos. Außerdem können sie den Support kontaktieren und auf Anfrage auch Debug-Daten senden. Dazu müssen Sie die Bearbeitungsnummer eines Support-Tickets mit einem dazugehörigen Passwort angeben. Danach erzeugt die LANCOM R&S®Unified Firewall eine Datei mit allen Konfigurationseinstellungen und Logs. Die Datei wird mit dem Passwort verschlüsselt und auf einen für den Support zugänglichen Server gespeichert. Diese Datei wird 30 Tage nach Schließen des Support-Falls gelöscht. Im oberen Bereich des Fensters werden die letzten drei Ereignisse angezeigt, bei denen Debug-Daten gesendet wurden. Eine **Anleitung zum Einsenden von Debug-Daten** erhalten Sie in *diesem Knowledgebase-Artikel*.
7. Die Zeitangabe bis zum automatischen Logout aus dem Webclient.

Die Kopfzeile zeigt außerdem nicht gespeicherte Konfigurationsanpassungen an, wenn Sie ein Bearbeitungsfenster durch Drücken der [Esc]-Taste schließen. Wenn Sie ein Bearbeitungsfenster durch Klicken der Schaltfläche ✖ in der rechten oberen Ecke des Fensters schließen, werden nicht gespeicherte Änderungen nicht angezeigt.

Die aktuelle-Version des Benutzerhandbuchs der LANCOM R&S®Unified Firewall ist auch auf der Login-Seite verfügbar. Klicken Sie auf den Link **Benutzerhandbuch**, um auf die Datei zuzugreifen.

3.1.1.1 Hinweise zum automatischen Logout

Sie werden automatisch nach 10 Minuten Inaktivität ausgeloggt, d. h., wenn keine HTTP-Anfragen an den Server gesendet werden. Alle Aktionen, wie Öffnen eines Dialogs, Speichern von Einstellungen oder aktive Logs, die regelmäßig aktualisiert werden (z. B. das *Alarmprotokoll* auf Seite 70), veranlassen einen Neustart des Timers. Ausnahmen sind Hintergrundanfragen, durch die kein Neustart des Timers erfolgt.

Wenn Sie Einstellungen in einem Dialog ändern, Ihre Änderungen nicht speichern und den Dialog geöffnet lassen, werden Sie automatisch nach 10 Minuten ausgeloggt.

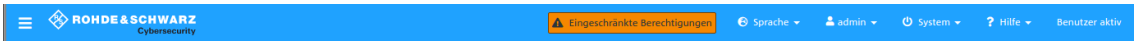
3.1.1.2 Mehrere angemeldete Administratoren

Mehrere Administratoren können zur gleichen Zeit am LANCOM R&S®Unified Firewall-Webclient angemeldet sein. Allerdings kann nur einer dieser Administratoren über Schreibrechte verfügen, also Änderungen an der Konfiguration

vornehmen. Dies ist immer der zuerst angemeldete Administrator, alle anderen erhalten ausschließlich Leserechte. Falls sich der Administrator abmeldet, der aktuell über Schreibrechte verfügt, dann werden diese Rechte dem nächsten Administrator verliehen, der in der zeitlichen Abfolge der Anmeldungen der Nächste wäre. Dieser Administrator bekommt darüber eine entsprechende Meldung.

Bei der Anmeldung werden Sie darüber informiert, dass bereits eine Sitzung mit Schreibrechten aktiv ist. Falls Sie über Berechtigungen auf den Einstellungen der Administratoren verfügen, dann wird Ihnen auch eine Liste mit den zurzeit angemeldeten Administratoren angezeigt. Siehe auch *Einstellungen zu Administratoren* auf Seite 34 Sollten Sie sich mit einem bereits angemeldeten Account erneut anmelden, dann können Sie die existierende Sitzung beenden und somit eine neue beginnen. Dies ist z. B. sinnvoll, wenn Sie ein Browserfenster einer Sitzung ohne Abmeldung einfach geschlossen hatten.

In der Kopfzeile wird angezeigt, ob Sie nur über eingeschränkte Berechtigungen verfügen.

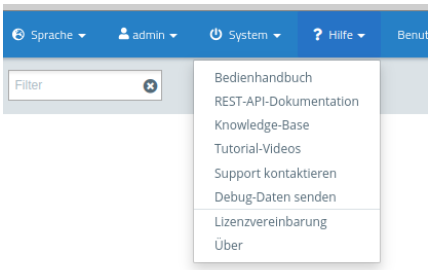


Ein Administrator mit Schreibrechten wird ebenfalls in der Kopfzeile darüber informiert, wenn sich weitere Administratoren anmelden.

Durch einen Klick auf die jeweilige Meldung in der Kopfzeile können Sie auch die bei der Anmeldung angezeigte Meldung erneut aufrufen.

3.1.1.3 REST-API-Dokumentation

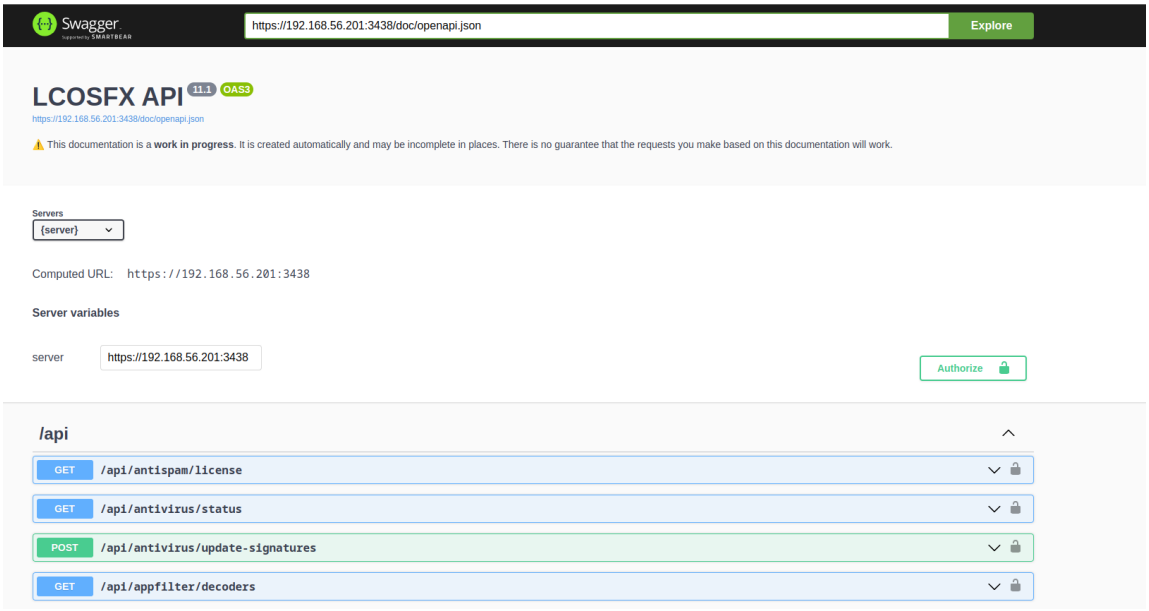
In der Kopfzeile unter **Hilfe** > **REST-API-Dokumentation** finden Sie eine automatisch generierte Dokumentation der REST-API.



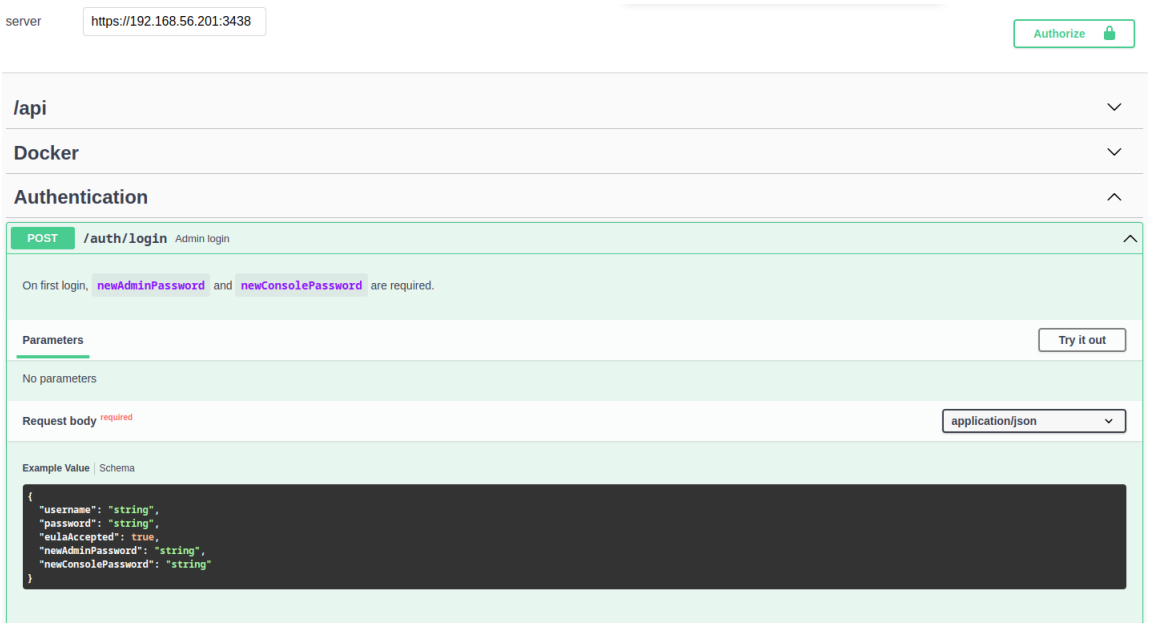
Die Dokumentation wird in einem separaten Tab geöffnet mit der derzeit verwendeten Adresse für den Web-Client-Zugriff als Server.

Die API kann sich ändern und die Dokumentation kann in Teilen auch unvollständig sein.

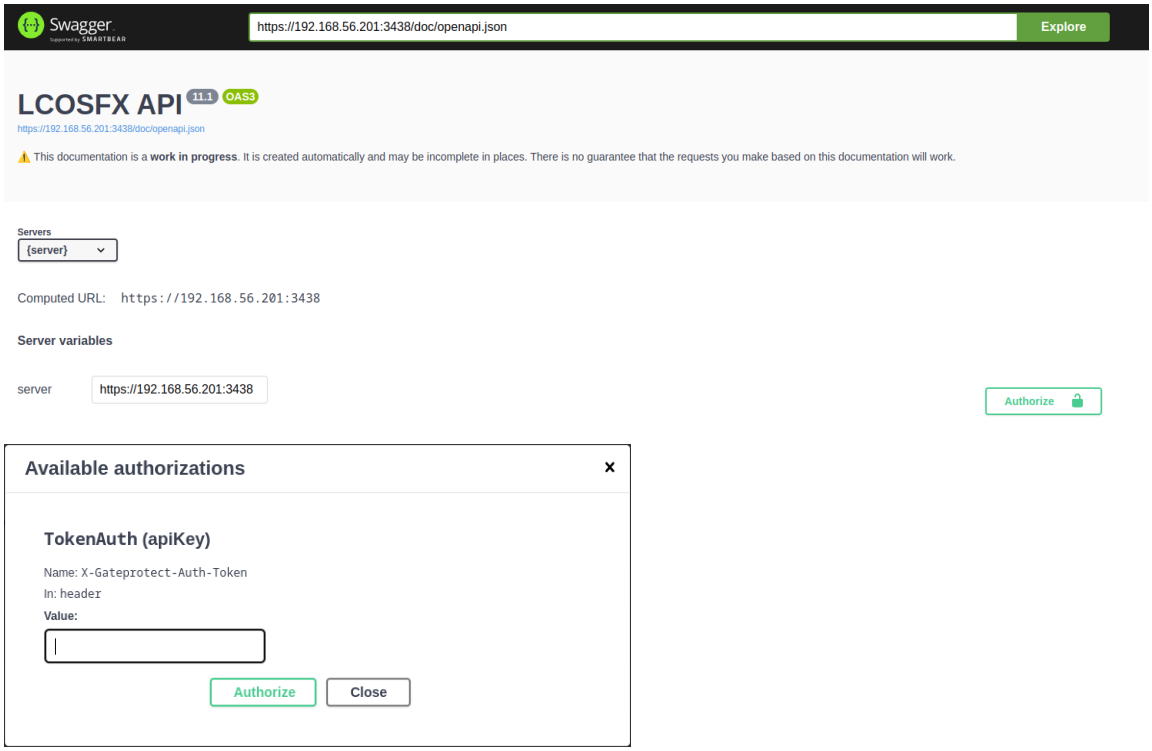
Sie können die Server-Variable auch ändern und somit eine andere Firewall referenzieren. Dies wird nicht empfohlen, da verschiedene Geräte mit unterschiedlichen Firmware-Versionen arbeiten und daher unterschiedliche APIs bereitstellen können.



Das Ausführen eines API-Requests gegen eine Firewall benötigt einen Auth-Token, den der Benutzer nach einem erfolreichen Login erhält. Dieses Token kann auf folgende Weise erhalten werden: Unter der Kategorie **Authentication** der API-Dokumentation ist auch der Login-Endpunkt enthalten, in dem Sie mit **Try it out** einen Login durchführen und so den Auth-Token erhalten kann. Das Feld **token** in der Antwort nach erfolgreichem Login enthält das Token.



Ist das Auth-Token vorhanden, kann jetzt über die Schaltfläche **Authorize** der Wert eingetragen werden.



Danach sollten alle in der Dokumentation aufgeführten Requests gegen die angegebene Firewall ausgeführt werden können.

3.1.2 Navigationsbereich

Der Navigationsbereich (2) befindet sich auf der linken Seite des Webclients. Je nach Auswahl in der ersten Leiste wird rechts davon eine zweite Leiste angezeigt. Die Menüeinträge in der ersten Navigationsleiste bieten Zugriff auf die LANCOM R&S®Unified Firewall-Einstellungen. Die Objektleiste rechts davon wird nach Auswahl eines Menüeintrags in der Navigationsleiste angezeigt. Sie dient der Anzeige von Informationen zur aktuellen Desktopkonfiguration.

Beide Leisten enthalten oben ein **Filter**-Eingabefeld, das Ihnen dabei hilft, bestimmte Menüelemente oder Listeneinträge schneller zu finden. Die Funktion der Eingabefelder beschränkt sich auf die jeweilige Leiste, in der Sie sich befinden. Während Sie Ihren Suchbegriff in eines der Eingabefelder eintippen, grenzt Ihre LANCOM R&S®Unified Firewall die jeweilige Liste auf die Dienste ein, die die eingegebenen Zeichen enthalten. Klicken Sie im Eingabefeld auf ⊗, um die Sucheingabe zu entfernen und zur ungefilterten Ansicht der Leiste zurückzukehren.

In der rechten oberen Ecke der Navigationsleiste können Sie mit Klick auf ⌄⌄ alle Menüs in der Navigationsleiste ausklappen und sie mit Klick auf ⌃⌃ wieder einklappen. Sie können die Navigationsleiste mit einem Klick auf ☰ in der Kopfzeile ausblenden. Weitere Informationen finden Sie unter *Kopfzeile* auf Seite 21.

Welche Informationen die Objektleiste anzeigt, hängt einerseits davon ab, welches Menüelement Sie in der Navigationsleiste ausgewählt haben und andererseits davon, wie viele Informationen Sie anzeigen lassen möchten. Sie können weitere Informationen ausklappen, indem Sie auf ≫ klicken, oder die Menge der angezeigten Informationen reduzieren, indem Sie auf ≪ in der rechten oberen Ecke dieses Felds klicken.

Einzelheiten zu den in jeder Ansicht verfügbaren Optionen finden Sie unter *Menüreferenz* auf Seite 33.

3.1.3 Desktop

Der Desktop (3) nimmt den größten Teil des Bildschirms unter dem Kopfzeilenbereich und rechts vom Navigationsbereich ein. Die hier angezeigten Knoten und Verbindungen hängen davon ab, welches Element in der Navigationsleiste oder auf dem Desktop ausgewählt ist.

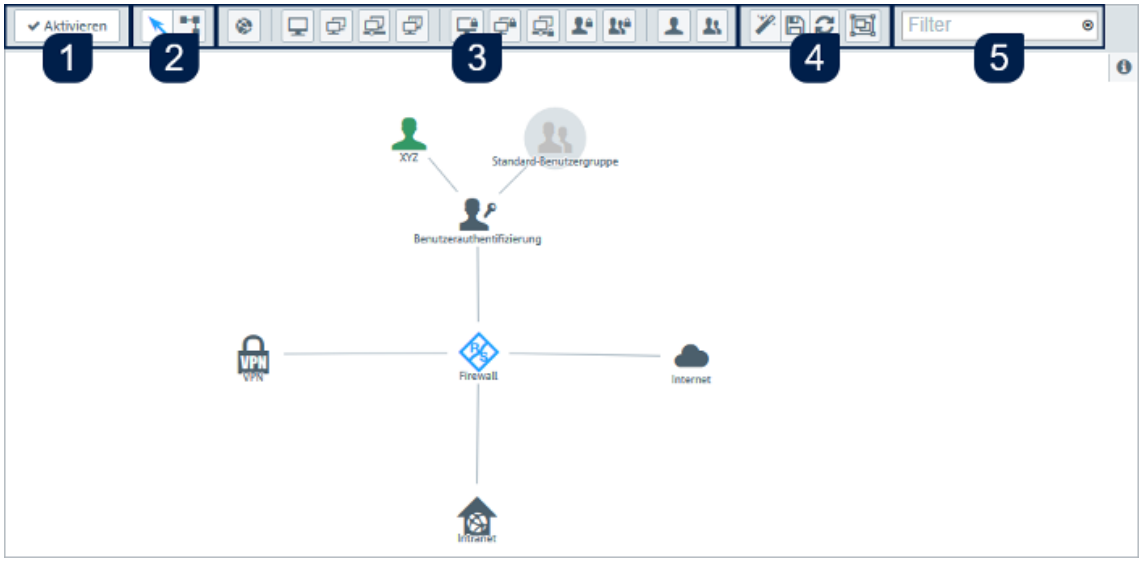


Abbildung 13: Desktop des LANCOM R&S®Unified Firewall-Webclients

Auf dem Desktop sehen Sie eine Übersicht Ihres gesamten konfigurierten Netzwerkes. Sie können in diesem Bereich verschiedene Einstellungen bearbeiten oder Details zu einer Konfiguration einsehen.

Eine Symbolleiste oben auf dem Desktop bietet schnellen Zugriff auf häufig verwendete Funktionen (von links nach rechts):

1. Aktivierungsschaltfläche
2. Auswahlwerkzeug, Verbindungswerkzeug
3. Werkzeuge zum Erstellen von Objekten
4. Werkzeuge zum Speichern, Wiederherstellen und Anordnen von Objekten
5. Filter- / Suchwerkzeug

Alle Schaltflächen in der Symbolleiste verwenden Popup-Beschriftungen, wenn Sie den Mauszeiger darüber bewegen, um eine einfache Identifizierung zu ermöglichen.

Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28.

3.1.3.1 Systemkonfiguration speichern (1)

Wenn sich die Systemkonfiguration ändert, wird die Schaltfläche ✔ **Aktivieren** im ersten Abschnitt der Symbolleiste hervorgehoben und fordert Sie auf, Ihre Konfiguration zu ändern. Klicken Sie auf diese Schaltfläche, um auf dem Desktop vorgenommene Konfigurationsänderungen zu speichern und sie auf Ihrer LANCOM R&S®Unified Firewall zu aktivieren.

3.1.3.2 Desktop-Objekte auswählen oder verbinden (2)

Mit dem Auswahlwerkzeug können Sie alle Aktionen auf dem Desktop ausführen, etwa Objekte verschieben oder bestimmte Funktionen auswählen. Mit dem Verbindungswerkzeug können Sie Verbindungen zwischen zwei Desktop-Objekten anlegen oder bearbeiten. Weitere Informationen finden Sie unter *Einstellungen für Firewall-Regeln* auf Seite 30.

Wenn Sie mit der linken Maustaste auf ein Desktop-Objekt klicken, werden je nach Objekttyp verschiedene Schaltflächen in einem kreisförmigen Menü angezeigt. Mit diesen Schaltflächen können Sie die Einstellungen zu einem vorhandenen

Objekt anpassen und eine Verbindung zwischen zwei vorhandenen Objekten erstellen oder bearbeiten. Außerdem können Sie Objekte, die an ein anderes Objekt angehängt sind, verstecken oder entfernen, Objekte von einer bestimmten Stelle auf dem Desktop loslösen oder ein Objekt vom Desktop entfernen.

3.1.3.3 Desktop-Objekt erstellen (3)

Um ein Desktop-Objekt zu erstellen, klicken Sie auf die jeweilige Schaltfläche. Es öffnet sich ein Bearbeitungsfenster, in das Sie die für das Objekt erforderlichen Daten eingeben können.

3.1.3.4 Desktoplayout anpassen (4)

Sie können das Layout des Desktops anpassen, indem Sie Objekte an die gewünschte Stelle ziehen, wo sie dann automatisch angeheftet werden. Sie können das angepasste Layout speichern und wiederherstellen oder die Objekte automatisch anordnen lassen.

3.1.3.5 Desktop-Objekte suchen (5)

Mit dem Filter-Eingabefeld **Filter** im letzten Bereich der Symbolleiste können Sie Desktop-Objekte auf der Grundlage folgender Kriterien schnell identifizieren:

- Name des Desktop-Objektes
- Beschreibung
- Tags
- Verwendetes Interface inkl. Any- und Internet-Interface
- IP-Adressen, IP-Netzwerke und IP-Bereiche
- Benutzer- oder Benutzergruppennamen
- Internet-Verbindungen
- IPsec und VPN SSL Verbindungsnamen
- verwendete lokale und remote Netzwerke in IPsec-Verbindungen

Es kann auch nach Desktop-Verbindungen gefiltert werden, aber aufgrund der Funktionsweise des Desktops können Verbindungen nur indirekt durch Anzeigen der verbundenen Desktop-Objekte angezeigt werden. Werte, nach denen gefiltert werden kann:

- Service-Namen
- Ports (bei Port-Bereichen wird zusätzlich zum Textfilter überprüft, ob der Suchtext eine Nummer ist und innerhalb des Portbereiches liegt)
- verwendetes Protokoll (TCP, UDP, ICMP …)
- aktiviertes DMZ, für die DMZ verwendete externe IP-Adresse
- aktivierter Proxy

Klicken Sie in das Eingabefeld, um eine Drop-down-Liste mit den Namen der möglichen Eingaben zu öffnen. Sie können entweder ein Element aus der Liste auswählen, um es in die Filtereingabe zu übernehmen, oder über das Eingabefeld nach einem bestimmten Element suchen. Für die Verbindungen werden Pseudo-Elemente angezeigt, die zum Auffinden von Verbindungen mit aktiviertem Proxy und DMZ hinzugefügt werden. Während Sie Ihre Suche in das Eingabefeld eintippen, zeigt Ihre LANCOM R&S®Unified Firewall nur Elemente der Drop-down-Liste an, die die eingegebenen Zeichen enthalten. Sie können beliebig viele Einträge in die Filtereingabe übernehmen, die jeweils „Oder"-Verknüpft werden. Groß- und Kleinschreibung wird nicht berücksichtigt.

Ihre LANCOM R&S®Unified Firewall schränkt die angezeigten Desktop-Objekte anhand der ausgewählten Filterkriteruen ein. Desktopknoten entlang des Pfades vom **Firewall**-Stammknoten zu einem Knoten, der den ausgewählten Filterkriterien entspricht, werden immer angezeigt, selbst wenn keines Zwischenobjekte den Suchkriterien entspricht.

Klicken Sie auf ⊗ im Eingabefeld, um die Sucheingabe zu löschen und zur ungefilterten Listenansicht zurückzukehren.
Weitere Informationen finden Sie unter *Desktop-Tags* auf Seite 129.

3.1.4 Infobereich

Der Infobereich (4) befindet sich auf der rechten Seite des Desktops.

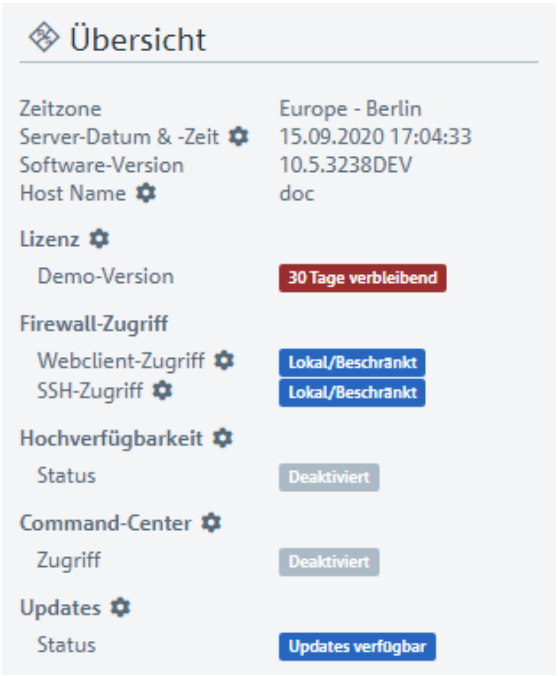


Abbildung 14: Infobereich des LANCOM R&S®Unified Firewall-Webclients

Nach dem Login ist der Infobereich sichtbar und zeigt grundlegende Firewall-Informationen an.

In diesem Bereich werden auch einige grundlegende Daten des Hardware-Monitorings angezeigt. So haben Sie jederzeit einen schnellen Überblick über die folgenden Daten:

- **Betriebszeit**: abgelaufene Zeit seit Start der Firewall
- **CPU**: durchschnittliche Auslastung aller CPUs in Prozent
- **RAM**: Belegung des Arbeitsspeichers in Prozent
- **var-Partition**: Belegung der var-Partition in Prozent. Die Belegung dieser Partion wird hier verwendet, weil auf dieser Partion u. a. Daten für Logs oder Statistiken gespeichert werden.

Abbildung 15: Übersicht > Hardware-Monitoring

Mit einem Klick auf den Titel kommen Sie direkt zum Bereich *Hardware-Monitoring* auf Seite 66.

Wählen Sie ein Desktop-Objekt aus, um dessen Informationen im Infobereich anzuzeigen, z. B.:

- Beschreibung
- Tags
- IP-Adressen
- Gruppenmitglieder
- Aufgebaute VPN-Verbindungen

Die Menge und Art der angezeigten Informationen ist für die verschiedenen Arten von Desktop-Objekten (Hosts, Internet-Objekte, Benutzer, etc.) unterschiedlich. Dynamische Informationen (z. B. der Status einer VPN-Verbindung) werden periodisch automatisch aktualisiert.

Einträge mit ⚙ können Sie anklicken, um einen dazu passenden Einstellungsdialog zu öffnen.

Klicken Sie auf ≫, um den Infobereich zu minimieren. Klicken Sie auf das **Info**-Icon, um den Infobereich wieder anzuzeigen.

Sollten Einträge im Infobereich mit **not available** gekennzeichnet sein, verfügt der eingeloggte Nutzer nicht über entsprechende Rechte, diese Informationen einsehen zu können.

3.2 Symbole und Schaltflächen

In diesem Abschnitt werden die gängigen Symbole und Schaltflächen erläutert, die auf der Benutzeroberfläche und im Verlauf dieses Handbuchs verwendet werden.

Wenn Sie den Mauszeiger über die Schaltflächen bewegen, werden zur vereinfachten Identifizierung Pop-up-Beschriftungen angezeigt.

Symbol / Schaltfläche	Beschreibung
	Anzeigen oder Ausblenden der Navigationsleiste.
	Bewegen von Objekten oder Auswählen von Objekten oder Funktionen auf dem Desktop.
	Erstellen oder Bearbeiten einer Verbindung zwischen zwei Desktop-Objekten.
	Erstellen eines Internetobjekts.
	Erstellen eines Hosts.
	Erstellen einer Hostgruppe.
	Erstellen eines Netzwerks.
	Erstellen eines IP-Bereichs.
	Erstellen eines VPN-Hosts.
	Erstellen einer VPN-Gruppe.
	Erstellen eines VPN-Netzwerks.
	Erstellen eines VPN-Benutzers.
	Erstellen einer VPN-Benutzergruppe.
	Erstellen eines Benutzers.
	Erstellen einer Benutzergruppe.
	Erstellen einer LANCOM Trusted Access Benutzergruppe.

Symbol / Schaltfläche	Beschreibung
	Verwerfen aller manuellen Layoutänderungen auf dem Desktop und Anwenden des automatischen Layouts.
	Speichern des aktuellen Desktop-Layouts.
	Wiederherstellen des zuletzt gespeicherten Desktop-Layouts. Wiederherstellen eines Backups. Wiederherstellen eines Zertifikats durch den Import eines neuen Zertifikats.
	Anpassen des gesamten Netzwerks an die Desktopgröße.
	Hebt ein Menüelement mit Einstellungen, die in der Navigationsleiste konfiguriert werden können, hervor. Hebt eine Tabellenspalte mit für einen Tabelleneintrag verfügbaren Aktionen hervor.
	Loslösen eines Desktop-Objekts, um es per Drag & Drop zusammen mit dem zugehörigen Desktopknoten über das Desktop zu bewegen.
	Anzeigen und Bearbeiten der Einstellungen für ein Desktop-Objekt, ein Listenelement oder einen Tabelleneintrag.
	Erstellen eines Listenelements oder eines Tabelleneintrags ausgehend von einer Kopie eines bestehenden Eintrags.
	Löschen eines Desktop-Objekts oder Listeneintrags aus dem System nach Bestätigen der Sicherheitsabfrage. Permanentes Widerrufen eines Zertifikats.
	Löschen einer benutzerdefinierten Firewall-Regel aus dem System. Entfernen einer Firewall-Regel mit vordefiniertem Dienst aus der Tabelle der Firewall-Regeln.
	Importieren eines Zertifikats oder einer Black- / Whitelist aus einer Datei. Signieren eines Certificate Signing Request.
	Exportieren eines Zertifikats oder einer Black- / Whitelist in eine Datei.
	Importieren eines Backups aus einer Datei.
	Exportieren eines Backups in eine Datei.
	Erstellen eines Listenelements in der Objektleiste.
	Ausklappen eines Menüelements in der Navigationsleiste, um untergeordnete Elemente anzuzeigen. Ausklappen einer Webfilterkategorie, um deren Unterkategorien anzuzeigen. Ausklappen einer Dienstkategorie für Firewall-Regeln, um untergeordnete Dienste anzuzeigen. Ausklappen einer Statistik oder Tabelle.
	Verbergen eines Menüelements in der Navigationsleiste, um untergeordnete Elemente anzuzeigen. Verbergen der Unterkategorien einer Webfilterkategorie. Verbergen der untergeordneten Dienste in einer Dienstkategorie für Firewall-Regeln. Verbergen einer Statistik oder Tabelle.
	Ausklappen detaillierterer Informationen in der Objektleiste.
	Reduzieren der Informationen in der Objektleiste.

Symbol / Schaltfläche	Beschreibung
	Einklappen aller Menüs in der Navigationsleiste. Erweitern eines Desktopknotens, um die damit verknüpften Desktop-Objekte anzuzeigen.
	Ausklappen aller Menüs in der Navigationsleiste. Einklappen eines Desktopknotens, um die damit verknüpften Desktop-Objekte zu verbergen.
	Zeigt an, dass ein Zertifikat noch gültig ist oder verschiebt ein nicht vertrauenswürdiges Proxy-CA in die Liste der vertrauenswürdigen Proxy-CAs.
	Zeigt an, dass ein Zertifikat ausgelaufen ist.
	Verifizieren eines Zertifikats.
	Temporäres Aussetzen eines Zertifikats oder einer CA.
	Reaktivieren eines ausgesetzten Zertifikats.
	Erneuern eines Zertifikats mit veränderter Gültigkeit.
	Schließen eines Pop-up-Fensters.
	Details eines Zertifikates ansehen.
	Zurücksetzen aller Suchkriterien eines Filters, um alle Ergebnisse anzuzeigen.
	Hiermit werden alle Objekte und Einstellungen gekennzeichnet, die durch die LANCOM Management Cloud (LMC) verwaltet werden. Diese können mit dem Webclient eingesehen, aber nicht bearbeitet werden. Durch die LMC verwaltete Objekte lassen sich nicht referenzieren. Somit kann z.B. ein durch die LMC erstelltes Application Filter-Profil nicht in einer selbst erstellten Desktop-Verbindung verwendet werden.

3.3 Einstellungen für Firewall-Regeln

Dieser Abschnitt beschreibt, wie Sie eine Firewall-Regel für eine Verbindung zwischen zwei Desktop-Objekten anlegen.

3.3.1 Einrichten einer Verbindung

Um eine Verbindung zwischen zwei Desktop-Objekten einzurichten, führen Sie die folgenden Schritte aus:

1. Klicken Sie auf die Schaltfläche in der Symbolleiste oben auf dem Desktop.

   Die Desktop-Objekte, die für diese Verbindung und mögliche weitere Verbindungen zwischen Desktop-Objekten ausgewählt werden können, werden durch gepunktete Kreise und Linien hervorgehoben.
2. Wählen Sie das Quellobjekt der Verbindung aus, indem Sie auf das entsprechende Desktop-Objekt klicken.
3. Wählen Sie das Zielobjekt für die Verbindung aus, indem Sie auf das entsprechende Desktop-Objekt klicken.

   Der Teilbereich **Verbindung** öffnet sich. Darin werden, sofern zutreffend, bereits bestehende Firewall-Regeln für diese Verbindung angezeigt.

   Alternativ können Sie auf die Schaltfläche im kreisförmigen Menü des Quellobjekts auf dem Desktop klicken und anschließend das Zielobjekt auswählen.

3.3.2 Erstellen einer Firewall-Regel

Führen Sie die folgenden Schritte aus, um eine Firewall-Regel zu erstellen:

1. Wählen Sie im Tab **Regeln** des Bearbeitungsfensters **Verbindung** mindestens einen Dienst aus, auf den Sie die Firewall-Regel anwenden möchten.

   Eine Liste der Dienste, auf die die Firewall-Regel angewendet werden kann, wird in der Leiste auf der rechten Seite des Browserfensters angezeigt. Die Leiste ist in Kategorien von Diensten mit einer jeweils ähnlichen Funktion eingeteilt. Die Kategorien können mit einem Klick auf das entsprechende Symbol ein- und ausgeklappt werden.

   Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28.

   Mithilfe des **Filter**-Eingabefelds oben in der Leiste mit der Diensteauswahlliste können Sie schnell und einfach einen bestimmten Dienst oder eine bestimmte Dienstgruppe finden. Während Sie Ihren Suchbegriff in das Eingabefeld eintippen, werden nur diejenigen Dienste und Dienstgruppen angezeigt, die die eingegebenen Zeichen enthalten. Klicken Sie im Eingabefeld auf ⊗, um die Sucheingabe zu löschen und zur ungefilterten Listenansicht zurückzukehren.

   a. Es gibt zwei Möglichkeiten, Dienste zu einer Firewall-Regel hinzuzufügen:

      - Um einen einzelnen Dienst hinzuzufügen, klicken Sie auf die Schaltfläche ⊕ vor dem jeweiligen Dienst in der Leiste mit der Dienstauswahlliste.
      - Um alle Dienste einer Kategorie gleichzeitig hinzuzufügen, klicken Sie auf die Schaltfläche ⊕ (Gefilterte Dienste hinzufügen) direkt unter dem Titel der jeweiligen Kategorie.

      Die ausgewählten Dienste werden in der Tabelle im Tab **Regeln** angezeigt. Außerdem werden auch die Regeln angezeigt, die zwischen übergeordneten Objekten konfiguriert sind. Diese vererbten Regeln können nicht direkt editiert werden. Mit Klick auf den Namen der Regel können aber die Einstellungen für diese Regeln angesehen werden. In der Spalte **Ändern / Vererbt von** werden statt den Editier-Buttons die Namen der Verbindungen angezeigt, aus denen diese Regeln verwendet werden. Mit Klick auf diese Namen, kann die dazugehörige Verbindung direkt geöffnet werden.

      Über die Filterfunktion können Sie die Anzeige der Regeln einschränken, so dass Sie schneller feststellen können, ob eine bestimmte Regel bereits vorhanden ist. Filterkriterien sind

      - Text für Namen, Regelnamen, Verbindungsnamen und Protokolle
      - Zahlen für Ports und Portbereiche
      - Booleans z. B. für DMZ, Proxy oder NAT

   b. Um die Einstellungen für eine Firewall-Regel zu bearbeiten, klicken sie auf die Schaltfläche ✎ (Klicken zum Bearbeiten dieser Regel).

   Ein Bearbeitungsfenster für den jeweiligen Dienst öffnet sich.

2. Im Bearbeitungsfenster können Sie die folgenden Informationen einsehen und die folgenden Elemente der Firewall-Regel konfigurieren:

   a. Unter **Beschreibung** geben Sie zusätzliche Informationen zur Firewall-Regel für die interne Verwendung ein.

   b. Im Tab **Ports / Protokolle** können Sie einsehen, welche Ports und Protokolle zur Verwendung für den Dienst festgelegt wurden. Weitere Informationen finden Sie unter *Dienste* auf Seite 130.

   c. Im Tab **Zeitsteuerung** können Sie die Zeitspanne festlegen, während der die Firewall-Regel aktiv ist. Im Tab stehen die folgenden Optionen zur Verfügung:

      - Mit den Schiebereglern können Sie bestimmte Zeiten und Wochentage einstellen.
      - Klicken Sie auf **Immer an** – die Regel ist immer aktiv.
      - Klicken Sie auf **Immer aus** – die Regel ist immer inaktiv.

   d. Im Tab zu den Einstellungen unter **Erweitert** stehen die folgenden Optionen zur Verfügung:

Eingabefeld	Beschreibung
Proxy	Für vordefinierte Firewall-Regeln mit vordefinierten Diensten, nur wenn die vordefinierten Dienste einen Proxy (HTTP, HTTPS, FTP, SMTP, SMTPS, IMAP, IMAPS, POP3 oder POP3S) erlauben: Setzen Sie den Haken in diesem Kontrollkästchen, um den Proxy für diese Regel zu aktivieren. Für Firewall-Regeln mit ausschließlich benutzerdefinierten Diensten: Wählen Sie einen Proxy für diese Regel aus der Drop-down-Liste aus. Um den Proxy zu entfernen, klicken Sie auf ✖ auf der rechten Seite des ausgewählten Proxys.
NAT	Wählen Sie aus den folgenden Optionen: › **Verbindungs-Einstellungen verwenden** – Mit dieser Einstellung verwenden Sie die auf dem Reiter *NAT* vorgenommenen Einstellungen für Verbindungen für NAT. › **Servicespezifische-Einstellungen verwenden** – Über diese Einstellung können sie die NAT-Einstellungen pro Service einstellen. Dazu werden die im Folgenden beschriebenen Einstellungen eingeblendet.
NAT / Masquerading	Geben Sie für NAT / Masquerading die gewünschte Richtung an (`bidirektional`, `links-nach-rechts` oder `rechts-nach-links`) oder deaktivieren Sie (`Aus`) die Funktion für diese Regel, indem Sie die entsprechende Optionsschaltfläche auswählen. Die Standardeinstellung hängt von den für die Verbindung ausgewählten Quell- und Zielobjekten ab.
NAT-Quell-IP	Optional: Wenn Sie mehrere ausgehende IP-Adressen haben, geben Sie die IP-Adresse an, die für Source-NAT verwendet werden soll. Wenn Sie keine IP-Adresse angeben, wählt das System automatisch die Haupt-IP-Adresse des ausgehenden Interface aus.
DMZ / Port-Weiterleitung für diesen Dienst aktivieren	Ist ein einzelnes Hostobjekt Ziel der Firewall-Regel, können Sie den Haken in diesem Kontrollkästchen setzen, um eine DMZ und Port-Weiterleitung für diese Regel zu aktivieren.
Externe IP-Adresse	Optional: Geben Sie die Ziel-IP-Adresse des zu bearbeitenden Datenverkehrs an. Die DMZ-Regel wird nur auf diesen Datenverkehr angewandt. Diese IP-Adresse muss eine der IP-Adressen der Firewall sein.
Externer Port	Zeigt den ursprünglichen Ziel-Port des zu bearbeitenden Datenverkehrs abhängig von dem im Tab **Ports / Protokolle** festgelegten Port an.
Ziel-IP-Adresse	Zeigt die neue Ziel-IP-Adresse des Datenverkehrs (nach der Bearbeitung) an.
Ziel-Port	Optional: Geben Sie den Ziel-Port des Datenverkehrs (nach der Bearbeitung) an.

e. Im Tab zu den Einstellungen unter **Traffic-Shaping** stehen die folgenden Optionen zur Verfügung:

Eingabefeld	Beschreibung
Traffic-Shaping	Wählen Sie aus den folgenden Optionen: › **Verbindungs-Einstellungen verwenden** – Mit dieser Einstellung werden die auf Verbindungsebene vorgenommenen Traffic-Shaping-Einstellungen übernommen. Siehe *Einstellungen für Desktopverbindungen* auf Seite 115. › **Servicespezifische-Einstellungen verwenden** – Über diese Einstellung können sie die Traffic-Shaping-Einstellungen pro Service einstellen. Dazu werden die im Folgenden beschriebenen Einstellungen eingeblendet.
Traffic-Gruppe	Wählen Sie optional den Namen einer Traffic-Gruppe aus. Dadurch werden die für diese Gruppe definierten Regeln für den Datenverkehr auf dieser Verbindung angewendet. Siehe auch *Traffic Shaping* auf Seite 105. ⓘ Falls es sich um einen Routen-basierten IPsec-Tunnel handelt, kann der Datenverkehr innerhalb eines Tunnels mit Hilfe einer eigenen Shaping-Konfiguration priorisiert werden.

Eingabefeld	Beschreibung
DSCP ausgehend	Wählen Sie einen optionalen DSCP-Wert für ausgehenden Datenverkehr aus der Liste aus. Die Liste enthält die Bezeichnungen aus den relevanten RFCs (z. B. „CS0“) und der Gruppe (z. B. „Standard“). Zusätzlich wird der Wert ebenfalls in seiner numerischen Repräsentation zu verschiedenen Basen (binär, hexadezimal und dezimal) angezeigt. Die Liste kann entsprechend dieser Darstellungen durchsucht werden, so dass Sie unabhängig von der individuell bevorzugten Darstellung schnell den gewünschten Wert finden.

f. Mit den Schaltflächen unten rechts im Bearbeitungsfenster können Sie Ihre Änderungen an einer vorhandenen Regel speichern (**OK**), die Bearbeitung einer vorhandenen Regel abbrechen (**Abbrechen**) und Ihre Änderungen verwerfen (**Zurücksetzen**).

Die konfigurierte Regel wird in der Tabelle im Tab **Regeln** angezeigt. Um eine Regel aus der Tabelle zu löschen, klicken Sie auf die Schaltfläche ⊖ (Klicken zum Löschen dieser Regel) in der letzten Spalte.

3. Weitere Informationen zu den Tabs **URL- / Content-Filter**, **Application Filter** und **NAT** finden Sie unter *Desktopverbindungen* auf Seite 114
4. Mit den Schaltflächen unten rechts im Bearbeitungsfenster können Sie das Bearbeitungsfenster schließen (**Schließen**), sofern Sie keine Änderungen vorgenommen haben, Ihre Änderungen speichern (**Speichern**) oder verwerfen (**Zurücksetzen**).
5. Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28.

3.4 Menüreferenz

Dieses Referenzkapitel beschreibt die einzelnen Menüelemente in der Navigationsleiste links im Browserfenster. Ihre von LANCOM Systems erworbene Lizenz bestimmt, welche Menüelemente in Ihrer LANCOM R&S®Unified Firewall verfügbar sind. Die Funktionen, die in Ihrer LANCOM R&S®Unified Firewall-Lizenz nicht enthalten sind, werden in der Navigationsleiste ausgegraut angezeigt.

In den folgenden Abschnitten finden Sie Informationen zu den in jeder Ansicht verfügbaren Optionen.

3.4.1 Firewall

Nutzen Sie die Einstellungen unter **Firewall** , um LANCOM R&S®Unified Firewall für Ihre lokale Umgebung anzupassen. Außerdem können Sie hier Zugriffsmöglichkeiten auf Ihre LANCOM R&S®Unified Firewall aus externen Netzwerken oder dem Internet einrichten und Ihre LANCOM R&S®Unified Firewall mit einem Command Center Server verbinden.

3.4.1.1 Administratoren

Legen Sie mithilfe der Einstellungen unter **Administratoren** Administratoren und deren Zugriff auf bestimmte Dienste fest.

Weiterführende Informationen zu Administratoren finden Sie in den folgenden Abschnitten.

3.4.1.1.1 Übersicht Administratoren

Navigieren Sie zu **Firewall** > **Administratoren**, um die Liste der derzeit im System angelegten Administratoren in der Objektleiste anzuzeigen.

Mit der Schaltfläche ⊕ über der Liste können Sie neue Administratoren hinzufügen.

In der erweiterten Ansicht zeigt die Spalte **Name** den Namen des Administrators an. Die Spalte **Admin** zeigt einen der folgenden Statusindikatoren an:

- Grün – Der Administrator hat Zugriff auf den Webclient.
- Orange – Der Administrator hat keinen Zugriff auf den Webclient.

Mit den Schaltflächen in der letzten Spalte können Sie die Einstellungen für einen vorhandenen Administrator einsehen und bearbeiten. Außerdem können Sie mithilfe der Schaltflächen einen neuen Administrator ausgehend von einer Kopie eines vorhandenen Administrators anlegen oder einen Administrator aus dem System löschen.

Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28

3.4.1.1.2 Einstellungen zu Administratoren

Unter **Firewall** > **Administratoren** können Sie einen neuen Administrator hinzufügen, oder einen vorhandenen Administrator bearbeiten.

Der Standardbenutzer `admin` kann nicht gelöscht oder umbenannt werden. Außerdem können die Zugriffsrechte dieses Benutzers auf den Webclient nicht widerrufen werden.

Im Bearbeitungsfenster **Administrator** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Name	Geben Sie einen eindeutigen Namen für den Administrator ein.
Beschreibung	Optional: Geben Sie zusätzliche Informationen zum Administrator für die interne Verwendung ein.

Im Tab **Client-Zugang** :

Eingabefeld	Beschreibung
Web-Client-Zugriff	Setzen Sie den Haken in diesem Kontrollkästchen, um dem Administrator Zugriff auf den Webclient zu gewähren.
Administrator-Passwort	Zum Anlegen eines neuen Administrors oder bei einer Kennwort-Änderung wird das Kennwort des gegenwärtig eingeloggten Benutzers benötigt.
Kennwort	Für neu hinzugefügte Administratoren, nur wenn der Haken im Kontrollkästchen **Web-Client-Zugriff** gesetzt ist: Geben Sie ein Passwort ein und bestätigen Sie es. Für bearbeitete Administratoren, nur wenn der Haken im Kontrollkästchen **Ändern** gesetzt ist: Geben Sie ein Passwort ein und bestätigen Sie es.
Ändern	Optional und für bearbeitete Administratoren, nur wenn der Haken im Kontrollkästchen **Web-Client-Zugriff** gesetzt ist: Setzen Sie den Haken in diesem Kontrollkästchen, um das Passwort des Administrators zu ändern.
Zeige Passwort	Optional und für neu hinzugefügte Administratoren, nur wenn der Haken im Kontrollkästchen **Web-Client-Zugriff** gesetzt ist: Setzen Sie den Haken in diesem Kontrollkästchen, um das Passwort zu verifizieren. Optional und für bearbeitete Administratoren, nur wenn der Haken im Kontrollkästchen **Ändern** gesetzt ist: Setzen Sie den Haken in diesem Kontrollkästchen, um das Passwort zu verifizieren.
Kennwort-Änderung erforderlich nach nächster Anmeldung	Optional und für neu hinzugefügte Administratoren, nur wenn der Haken im Kontrollkästchen **Web-Client-Zugriff** gesetzt ist: Wenn Sie den Haken in diesem Kontrollkästchen setzen, muss der Benutzer sein Passwort nach der nächsten Anmeldung ändern.

Eingabefeld	Beschreibung
	Optional und für bearbeitete Administratoren, nur wenn der Haken im Kontrollkästchen **Ändern** gesetzt ist: Wenn Sie den Haken in diesem Kontrollkästchen setzen, muss der Benutzer sein Passwort nach der nächsten Anmeldung ändern.

Im Tab **Webclient-Rechte** können Sie festlegen, welche Aktionen der Administrator in bestimmten Bereichen des Webclients ausführen darf.

Treffen Sie eine Auswahl aus den folgenden Berechtigungen, indem Sie die entsprechende Optionsschaltfläche auswählen.

- **Verboten** – Der Administrator hat keinen Zugriff auf den angegebenen Bereich des Webclients.
- **Lesen / Öffnen** – Der Administrator kann die Elemente im angegebenen Bereich des Webclients öffnen und lesen, kann aber keine Änderungen daran vornehmen.
- **Schreiben / Ausführen** – Der Administrator hat vollen Zugriff auf die Elemente im angegebenen Bereich des Webclients.

Die Schaltflächen rechts unten im Bearbeitungsfeld hängen davon ab, ob Sie einen neuen Administrator hinzufügen oder einen bestehenden bearbeiten. Klicken Sie für einen neu konfigurierten Administrator auf **Erstellen**, um ihn zur Liste der verfügbaren Administratoren hinzuzufügen, oder auf **Abbrechen**, um Ihre Änderungen zu verwerfen. Zum Bearbeiten eines vorhandenen Administrators klicken Sie auf **Speichern**, um den neu konfigurierten Administrator zu speichern, oder auf **Zurücksetzen**, um Ihre Änderungen zu verwerfen.

Wenn Sie Änderungen vorgenommen haben, können Sie diese mit den Schaltflächen unten rechts im Bearbeitungsfenster speichern (**Speichern**) oder verwerfen (**Zurücksetzen**). Andernfalls können Sie das Fenster schließen (**Schließen**).

3.4.1.2 Allgemeine Einstellungen

Navigieren Sie zu **Firewall** > **Allgemeine Einstellungen**, um ein Bearbeitungsfenster zu öffnen, in dem Sie einige zentrale Einstellungen für Ihre LANCOM R&S®Unified Firewall vornehmen können.

Im Bearbeitungsfenster **Allgemeine Einstellungen** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Hostname	Hostname der Firewall.
Domain	Domain der Firewall. Falls die Firewall mit einem Active Directory verbunden ist, dann sollte hier die entsprechende Active Directory Domain eingetragen werden.
Nutzungs-Statistiken senden	Informationen über die Auslastung und den Zustand der Firewall aufzeichnen und an die LANCOM Systems GmbH übertragen. Es werden keine persönlichen Informationen und keine Bestandteile des über die Firewall erfolgten Datenverkehrs übertragen.
Absturzberichte senden	Im Fehlerfall allgemeine Informationen zum Sytemzustand, zur aktuellen Systemkonfiguration und zum aufgetretenen Fehler an die LANCOM Systems GmbH übertragen. Die Daten werden nur zur Fehleranalyse verwendet und anschließend wieder gelöscht. Es erfolgt keine Weitergabe irgendwelcher Daten an Dritte.
TFTP	Zugriff auf die Firewall per TFTP erlauben oder verbieten. Voreingestellt ist TFTP erlaubt. Der TFTP-Zugriff wird nur im internen Netzwerk für den sysinfo-Zugriff freigeschaltet.

Wenn Sie Änderungen vorgenommen haben, können Sie diese mit den Schaltflächen unten rechts im Bearbeitungsfenster speichern (**Speichern**) oder verwerfen (**Zurücksetzen**). Andernfalls können Sie das Fenster schließen (**Schließen**).

3.4.1.3 Backup

Ihre LANCOM R&S®Unified Firewall speichert Einstellungen in Konfigurationsdateien, die jedes Mal automatisch erstellt werden, wenn Einstellungen über den Webclient angepasst werden. Mithilfe der Optionen unter **Backup** können Sie

regelmäßige Backups der aktuellen Systemkonfiguration konfigurieren, manuell ein Backup der aktuellen Systemkonfiguration erstellen und vorherige Konfigurationen wiederherstellen.

Backups können erstellt werden, sobald eine Lizenz importiert wurde (also nicht während der 30-tägigen Probezeit).

Weiterführende Informationen zu Backups finden Sie in den folgenden Abschnitten.

3.4.1.3.1 Einstellungen für automatische Backups

Mit den Einstellungen unter **Auto-Backup** können Sie eine Verbindung zu einem entfernten Backup-Server erstellen, auf dem Sie automatisch erstellte Backups speichern möchten. Außerdem können Sie in diesem Teilbereich die Intervalle für das automatische Backup der Firewall-Konfiguration festlegen. Die Anzahl und Intervalle der Backup-Erstellung sind unbegrenzt.

Bevor Sie fortfahren, vergewissern Sie sich, dass Sie die Zeitzone Ihrer LANCOM R&S®Unified Firewall wie unter *Zeiteinstellungen* auf Seite 53 beschrieben festgelegt haben. Andernfalls werden die Backups nach der Zeitzone „Europa – Berlin (CET/UTC +1)" anstatt der von Ihnen in den Einstellungen für automatische Backups festgelegten Zeitzone erstellt.

Navigieren Sie zu **Firewall** > **Backup** > **Auto-Backup**, um ein Bearbeitungsfenster zu öffnen, in dem Sie die Einstellungen für automatische Backups anzeigen und anpassen können.

Im Teilbereich unter **Auto-Backup** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Server-Adresse	Geben Sie die IP-Adresse des entfernten Backup-Servers ein, auf dem Sie automatisch erstellte Backups speichern möchten.
Benutzername	Geben Sie den Benutzernamen für den entfernten Backup-Server ein.
Kennwort	Geben Sie, falls erforderlich, das Benutzerpasswort für den entfernten Backup-Server ein.
Zeige Passwort	Optional: Setzen Sie den Haken in diesem Kontrollkästchen, um das Benutzer-Passwort zur Überprüfung anzuzeigen.
Server-Typ	Wählen Sie die entsprechende Optionsschaltfläche aus, um das zum Hochladen der Backups auf den Server genutzte Netzwerkprotokoll zu definieren. Diese Option ist standardmäßig auf **FTP** gesetzt, bei Bedarf können Sie die Einstellungen aber auch auf **SCP** ändern.
Dateiname	Geben Sie einen Namen für automatisch erstellte Backup-Dateien ein.
Verschlüsselungs-Passwort	Geben Sie ein Passwort für die Verschlüsselung der Backup-Dateien ein. Das Passwort muss aus bis zu 32 Zeichen bestehen (erlaubt sind Buchstaben mit Ausnahme von ä, ö, ü und ß, Zahlen und die Sonderzeichen `\-][/.,~!@#$%^*()_+:?><{}`).
Zeige Verschlüsselungs-Passwort	Optional: Wählen Sie dieses Kontrollkästchen, um das Verschlüsselungs-Passwort zu verifizieren.
Optionen	Wählen Sie die entsprechende Optionsschaltfläche aus, um festzulegen, was an die Dateinamen angefügt wird, um die Backups zu unterscheiden. Diese Option ist standardmäßig auf **Aktuelles Datum an Dateinamen anhängen** gesetzt, bei Bedarf können Sie die Einstellungen aber auch auf den anderen Wert ändern: › **Aktuelles Datum an Dateinamen anhängen** – Das Datum und der Zeitstempel der Erstellung des Backups werden an den Namen angefügt (z. B. `Backup_20171130-1527.gp`). Da sich diese Dateinamen niemals wiederholen, können alte Backup-Dateien nicht versehentlich überschrieben werden. › **Max. Datei-Anzahl** – Eine Nummer (Backupnummer) wird an den Namen angefügt. Geben Sie die maximale Anzahl zu speichernder Backup-Dateien an, indem Sie eine

Eingabefeld	Beschreibung
	Zahl im Eingabefeld unter dieser Option eingeben. Diese Option ist standardmäßig auf `20` Einträge gesetzt. Wenn die festgelegte Anzahl erreicht ist, wird wieder von vorne gezählt und die jeweils älteste Backup-Datei wird automatisch überschrieben.
Zeitsteuerung	Legen Sie fest, wie oft die Firewall-Konfiguration automatisch gesichert wird. Klicken Sie in das Eingabefeld unter **Beginn**, um Datum und Zeitpunkt des ersten automatisch erstellten Backups festzulegen. Wenn Sie auf das Eingabefeld klicken, öffnet sich ein Pop-up-Fenster mit einem Kalender und Eingabefeldern, mit dem Sie Datum und Uhrzeit ändern können. Sie können das Datum im Format MM/TT/JJJJ eingeben oder im Auswahlfenster ein Datum auswählen. Optional können Sie die Uhrzeit im Format hh:mm:ss eingeben. Unter **Intervall** und **Unit**, können Sie angeben, wie oft die Konfiguration automatisch gesichert wird. Bestimmen Sie das Intervall, indem Sie mit den Pfeiltasten nach oben oder unter navigieren, oder geben Sie eine Zahl ein. Diese Option ist standardmäßig auf `1` Einträge gesetzt. Wählen Sie daraufhin eine Einheit aus der Drop-down-Liste aus. Diese Option ist standardmäßig auf `Tage` gesetzt, Sie können die Einstellungen jedoch bei Bedarf auf einen der anderen Werte setzen: › `Einmalig` › `Stunden` › `Tage` › `Monate` Klicken Sie auf **Hinzufügen**, um den Zeitplan zur Liste hinzuzufügen. Sie können einzelne Einträge in den Listen bearbeiten oder löschen, indem Sie auf die entsprechende Schaltfläche neben einem Eintrag klicken. Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28. Wenn Sie einen Zeitplan bearbeiten, erscheint auf der rechten Seite des Eintrags ein Haken. Sie müssen Ihre Änderung zunächst mit diesem Haken bestätigen, bevor Sie die Einstellungen für das Zertifikat speichern können.

Um die Verbindung zum konfigurierten Backup-Server zu überprüfen, klicken Sie auf die Schaltfläche **Server-Einstellungen testen** unten links im Bearbeitungsfenster. Das System versucht daraufhin, eine Testdatei (`file name_test`) auf dem Backup-Server zu speichern. War dieser Test erfolgreich, wird eine Textdatei auf dem Server gespeichert und ein Pop-up-Fenster mit einer Erfolgsmeldung erscheint. Nach dem Test können Sie diese Textdatei löschen.

Wenn Sie Änderungen vorgenommen haben, können Sie diese mit den Schaltflächen unten rechts im Bearbeitungsfenster speichern (**Speichern**) oder verwerfen (**Zurücksetzen**). Andernfalls können Sie das Fenster schließen (**Schließen**).

Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

3.4.1.3.2 Exportieren eines Backups

Mit den Einstellungen unter **Exportieren** können Sie ein manuelles Backup der aktuellen Firewall-Konfiguration erstellen und exportieren. Nutzen Sie diese Funktion zum Beispiel, um eine Konfiguration nach einer Systemaktualisierung neu zu laden.

Navigieren Sie zu **Firewall** > **Backup** > **Export**, um ein Bearbeitungsfenster zu öffnen, in dem Sie ein manuelles Backup im GP-Dateiformat erstellen und auf ihren Rechner übertragen können, sodass Sie die gespeicherte Konfiguration bei Bedarf zu einem späteren Zeitpunkt wiederherstellen können.

Im Bearbeitungsfenster **Exportieren** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Verschlüsselungs-Passwort	Geben Sie ein Passwort für die Verschlüsselung der Backup-Datei ein und bestätigen Sie es. Das Passwort muss aus bis zu 32 Zeichen bestehen. Erlaubt sind Buchstaben mit Ausnahme von ä, ö, ü und ß, Zahlen und die Sonderzeichen `\-][/.,~!@#$%^*()_+:?><}{.`
Zeige Passwort	Optional: Setzen Sie den Haken in diesem Kontrollkästchen, um das Passwort zu verifizieren.
Backup-Passwort verwenden	Optional: Setzen sie den Haken in diesem Kontrollkästchen, wenn Sie das Passwort für die Verschlüsselung automatischer Backup-Dateien (siehe *Einstellungen für automatische Backups* auf Seite 36) übernehmen möchten, statt ein neues Passwort einzugeben.

Klicken Sie auf **Exportieren**, wenn Sie die Backup-Datei exportieren möchten. Klicken Sie ansonsten auf **Abbrechen**, um das Bearbeitungsfenster zu schließen.

3.4.1.3.3 Importieren eines Backups

Mit LANCOM R&S®Unified Firewall können Sie eine zuvor heruntergeladene Backup-Datei hochladen, um die Systemkonfiguration wiederherzustellen (z. B. nach einer Neuinstallation).

Navigieren Sie zu **Firewall** > **Backup** > **Import**, um eine Firewall-Konfiguration aus einer zuvor erstellten Backup-Datei aufzurufen und zu aktivieren.

Um eine automatisch erstellte Backup-Datei hochzuladen, die auf dem Backup-Server gespeichert ist, müssen Sie die Backup-Datei zunächst vom Backup-Server auf Ihren lokalen Datenträger übertragen.

Im Bearbeitungsfenster **Importieren** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Backupdatei	Klicken Sie auf **Auswählen**, um die Suchfunktion des lokalen Datenträgers zu öffnen. Wählen Sie auf Ihrem lokalen Datenträger eine Backup-Datei im GP-Dateiformat zur Übertragung aus. Klicken Sie auf **Öffnen**, um die Suchfunktion des lokalen Datenträgers zu schließen. Der Name der Backup-Datei erscheint im Feld.
Kennwort	Geben Sie das Verschlüsselungs-Passwort ein, das Sie für den Export der Datei gewählt haben.
Zeige Passwort	Optional: Setzen Sie den Haken in diesem Kontrollkästchen, um das Passwort zu verifizieren.

Klicken Sie auf **Importieren**, wenn Sie die Backup-Datei importieren möchten. Klicken Sie ansonsten auf **Abbrechen**, um das Bearbeitungsfenster zu schließen.

War der Upload erfolgreich, erscheint eine Erfolgsmeldung. Bestätigen Sie den Neustart des Systems, indem Sie auf **Neustarten** klicken. Das System wird neu gestartet, Sie werden ausgeloggt und die Login-Seite Ihrer LANCOM R&S®Unified Firewall öffnet sich. Geben Sie Ihre Login-Daten ein und klicken Sie auf **Anmelden**. Der Webclient erscheint.

3.4.1.4 Command Center

Mit dem LANCOM R&S®UF Command Center können Sie mehrere LANCOM R&S®Unified Firewall-Geräte in einer Anwendung administrieren.

Navigieren Sie zu **Firewall** > **Command-Center**, um ein Bearbeitungsfenster zu öffnen, in dem Sie Ihre LANCOM R&S®Unified Firewall über eine VPN-Verbindung mit einem LANCOM R&S®UF Command Center-Server verbinden können.

Um die VPN-Verbindung herzustellen, benötigen Sie VPN-Zertifikate für alle Geräte, die von derselben Zertifizierungsstelle (CA) signiert wurden. Es empfiehlt sich daher, die VPN-Zertifizierungsstelle und die

VPN-Zertifikate an einem Standort zu verwalten und die VPN-Zertifikate von dort an alle weiteren Standorte zu exportieren.

Weitere Informationen zur Erstellung, zum Exportieren und zum Importieren von Zertifikaten finden Sie unter *Zertifikate* auf Seite 205.

Im Bearbeitungsfenster **Command-Center** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
I/**0**	Ein Schiebeschalter gibt an, ob die Verbindung zum LANCOM R&S®UF Command Center derzeit aktiv (**I**), oder inaktiv (**0**) ist. Mit einem Klick auf den Schiebeschalter können Sie den Status der Verbindung ändern. Die Verbindung zum LANCOM R&S®UF Command Center ist standardmäßig inaktiv.
Host	Geben Sie den Hostnamen oder die IP-Adresse ein, unter dem / der das LANCOM R&S®UF Command Center von der LANCOM R&S®Unified Firewall erreichbar sein soll.
Port	Geben Sie die Port-Nummer ein, unter der das LANCOM R&S®UF Command Center erreichbar ist (üblicherweise Port-Nummer `11940`).
Command-Center CA	Wählen Sie die CA, von der das Zertifikat für das LANCOM R&S®UF Command Center signiert wurde, aus der Drop-down-Liste aus.
Firewall-Zertifikat	Wählen Sie das VPN-Zertifikat für die LANCOM R&S®Unified Firewall aus der Drop-down-Liste aus.
Breite/Länge	Optional: Geben Sie die Koordinaten des Standorts Ihrer LANCOM R&S®Unified Firewall in Dezimalgradnotation ein, z. B. `53.555483`. Die Koordinaten werden verwendet, um Ihre LANCOM R&S®Unified Firewall auf einer Karte im LANCOM R&S®UF Command Center anzuzeigen.

Wenn Sie Änderungen vorgenommen haben, können Sie diese mit den Schaltflächen unten rechts im Bearbeitungsfenster speichern (**Speichern**) oder verwerfen (**Zurücksetzen**). Andernfalls können Sie das Fenster schließen (**Schließen**).

3.4.1.5 E-Mail-Einstellungen

Die E-Mail-Einstellungen sind die Voraussetzung für die Nutzung des Benachrichtigungs-Systems. Über dieses können Sie entweder sofort oder regelmäßig in aggregierter Form per E-Mail Nachrichten über bestimmte Benachrichtigungstypen erhalten. Näheres hierzu unter *Benachrichtigungs-Einstellungen* auf Seite 57.

Navigieren Sie zu **Firewall** > **E-Mail-Einstellungen**, um ein Bearbeitungsfenster zu öffnen, in dem Sie die entsprechenden Daten für Absender und Verschlüsselung der Nachrichten konfigurieren können. Optional sind Einstellungen für einen Relay-Server möglich, wenn die E-Mails nicht direkt versendet werden können.

Im Bearbeitungsfenster **E-Mail-Einstellungen** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
I/**0**	Ein Schiebeschalter gibt an, ob die E-Mail-Einstellungen derzeit aktiv (**I**), oder inaktiv (**0**) sind. Mit einem Klick auf den Schiebeschalter können Sie den Status ändern.
Absender-Adresse	Absender-E-Mail-Adresse des Firewall-Systems.
Verbindungssicherheit	Wählen Sie eine der möglichen Optionen `Keine`, `TLS` oder `StartTLS`.
Remote-Zertifikat verifizieren	Falls dieses angegeben wird, dann verifiziert die Firewall das Zertifikat des Zielservers bzw. Relays.
S/MIME-Zertifikat	Falls dieses angegeben wird, dann verschlüsselt die Firewall alle ausgehenden E-Mails mit dem Public Key des gewählten Zertifikats.

Im Tab **Relay** können Sie Vorgaben für die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Server	Adresse des E-Mail-Servers.

Eingabefeld	Beschreibung
Port	Port des E-Mail-Servers.
Benutzername	Name, mit dem die Firewall sich beim E-Mail-Server anmeldet.
Passwort	Passwort, mit dem die Firewall sich beim E-Mail-Server anmeldet.

Um die vorgenommenen Einstellungen zu testen, können Sie über die Schaltfläche **Test-Mail versenden** eine E-Mail versenden. Es wird ein Dialog geöffnet, in dem Sie eine **Empfänger-Adresse** angeben können und dann über die Schaltfläche **Versenden** diese abschicken.

Beachten Sie, dass, falls ein Relay Server verwendet wird, die darauffolgende Status-Nachricht nur Auskunft darüber gibt, ob die E-Mail vom Relay Server akzeptiert wurde. Kann der Relay Server die Nachricht nicht zustellen, ist das nur auf dem Relay Server zu sehen.

Wenn Sie Änderungen vorgenommen haben, können Sie diese mit den Schaltflächen unten rechts im Bearbeitungsfenster speichern (**Speichern**) oder verwerfen (**Zurücksetzen**). Andernfalls können Sie das Fenster schließen (**Schließen**).

3.4.1.6 Hochverfügbarkeit

Mit den Einstellungen unter **Firewall** > **Hochverfügbarkeit** können Sie zwei unabhängige LANCOM R&S®Unified Firewall-Systeme in einer Master- / Slave-Konfiguration über ein dediziertes Interface verbinden. Das sogenannte HA-Cluster bietet eine Ausfallsicherungsfunktion. Falls das Master-Gerät ausfällt, übernimmt das Standby-Gerät (Slave) dessen Aufgaben.

Die Master- und Slave-Systeme werden über ein Cluster-Interconnect-Kabel verbunden, über das sie miteinander kommunizieren und den Status des verbundenen Systems überwachen können. Die Konfiguration des Slave-Geräts wird mit der des Master-Geräts synchronisiert. Auf dem Slave-Gerät werden bestimmte Regeln angewandt, die Netzwerk-Kommunikation ausschließlich mit dem Master-Gerät erlauben. Falls das Slave-System kein „Heartbeat"-Signal vom Master empfängt, übernimmt es die Rolle des Master-Systems (z. B. im Fall von Stromausfällen oder Hardwareausfällen / -abschaltung).

Im Fall einer solchen Übernahme durch das Slave-Gerät entfernt dieses die spezifischen Blockaden und sendet eine Gratuitous-ARP-Anfrage. Der mit der LANCOM R&S®Unified Firewall verbundene Switch muss den ARP-Befehl-erlauben. Möglicherweise dauert es einige Sekunden, bis das Client-Gerät im Netzwerk seinen ARP-Cache aktualisiert hat und der neue Master erreichbar ist.

Die folgende Abbildung zeigt eine typische Netzwerkumgebung mit einer redundanten Master- / Slave-Konfiguration für die Hochverfügbarkeit.

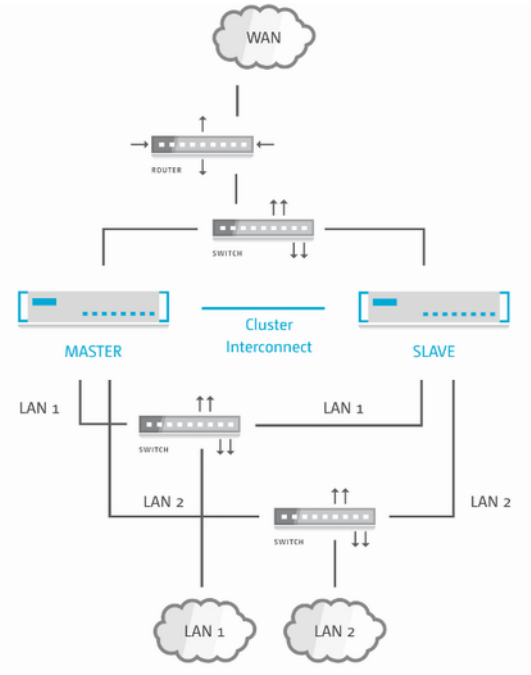


Abbildung 16: Beispiel-Netzwerk für Hochverfügbarkeit

Hochverfügbarkeit ist nicht für die Produktmodelle LANCOM R&S®Unified Firewall UF-50 und UF-100 verfügbar.

In den folgenden Abschnitten finden Sie weiterführende Informationen zu Hochverfügbarkeit.

3.4.1.6.1 Einstellungen für Hochverfügbarkeit

Mit den Einstellungen unter **Hochverfügbarkeit** können Sie die Verbindungsparameter für die Master- / Slave-Konfiguration anpassen.

Für die Hochverfügbarkeit sind zwei identische Systeme des gleichen Hardwaretyps (z. B. UF-200 mit UF-200 oder UF-500 mit UF-500) und mit der gleichen Softwareversion erforderlich. Außerdem benötigen Sie ein freies Netzwerk-Interface (NIC) auf beiden Systemen, das von keinem anderen Interface (z. B. VLAN oder Bridge) und keiner anderen Netzwerkverbindung verwendet wird. Weitere Informationen finden Sie unter *Interfaces* auf Seite 96 und *Netzwerkverbindungen* auf Seite 81. Für die Cluster-Verbindung muss in beiden Systemen das gleiche NIC verwendet werden.

Das Master-System synchronisiert seine anfängliche Konfiguration und alle späteren Konfigurationsänderungen auf das Slave-System, um sicherzustellen, dass bei einem Ausfall die gleiche Konfiguration angewendet wird.

Hochverfügbarkeit kann nur aktiviert werden, wenn keine Prozesse (wie z. B. Aktualisierungen oder Backups) im Hintergrund laufen.

Navigieren Sie zu **Firewall** > **Hochverfügbarkeit**, um die Hochverfügbarkeitsfunktion einzurichten.

Im Bearbeitungsfenster **Hochverfügbarkeit** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
I/**0**	Ein Schiebeschalter gibt an, ob Hochverfügbarkeit derzeit aktiv (**I**) oder inaktiv (**0**) ist. Indem Sie auf den Schiebeschalter klicken, können Sie den Status der Hochverfügbarkeit ändern. Hochverfügbarkeit ist standardmäßig deaktiviert.
Status	Zeigt den Status der Hochverfügbarkeit der LANCOM R&S®Unified Firewall an. Folgende Status sind möglich: › `Deaktiviert` – Hochverfügbarkeit ist auf dieser Firewall nicht aktiviert. › `Keine Verbindung` – Hochverfügbarkeit ist auf dieser Firewall aktiviert, die andere Firewall ist jedoch nicht erreichbar. › `Nicht synchronisiert` – Hochverfügbarkeit ist auf dieser Firewall aktiviert, die andere Firewall ist erreichbar, die Konfiguration des Master-Systems ist allerdings noch nicht auf das Standby-System (Slave) synchronisiert worden. › `Synchronisiert und bereit` – Hochverfügbarkeit ist auf dieser Firewall aktiviert. Die andere Firewall ist erreichbar und synchronisiert. › `Update wird installiert` – Hochverfügbarkeit ist auf dieser Firewall aktiviert. Die andere Firewall ist erreichbar. Beide Systeme werden gerade aktualisiert. Der Updatevorgang beinhaltet mehrere Schritte, die in den Update-Einstellungen und im Infobereich ersichtlich sind.
Initiale Rolle	Wählen Sie die entsprechende Optionsschaltfläche aus, um die Rolle der LANCOM R&S®Unified Firewall im HA-Cluster festzulegen. › **Master** – LANCOM R&S®Unified Firewall ist aktiv und synchronisiert seine Konfiguration mit LANCOM R&S®Unified Firewall als Slave. › **Slave** – LANCOM R&S®Unified Firewall ist nicht aktiv (d. h. nicht aus dem Webclient erreichbar), empfängt aber die Konfiguration des Master und ist für die Übernahme vorbereitet.
HA-Interface	Wählen Sie aus der Drop-down-Liste das Interface aus, das für die HA-Cluster-Kommunikation verwendet werden soll. Dieses Interface ist nicht für andere Firewall-Dienste nutzbar. Für die Cluster-Vernetzung muss das gleiche NIC in beiden LANCOM R&S®Unified Firewall-Systemen verwendet werden.
Lokale IP	Geben Sie die IP-Adresse, die Sie dem HA-Interface auf Ihrer LANCOM R&S®Unified Firewall zuweisen wollen, in CIDR-Schreibweise ein (IP-Adresse gefolgt von einem Schrägstrich „/" und der Anzahl der in der Subnetzmaske festgelegten Bits, beispielsweise `192.168.50.1/24`).
Remote-IP	Geben Sie die IP-Adresse ein, unter der die LANCOM R&S®Unified Firewall die andere LANCOM R&S®Unified Firewall des HA-Clusters erreichen kann.

Lokale IP und **Remote-IP** müssen sich im selben Subnetz befinden. HA-Cluster-Kommunikation über geroutete Netzwerke wird nicht unterstützt.

Wenn Sie Änderungen vorgenommen haben, können Sie diese mit den Schaltflächen unten rechts im Bearbeitungsfenster speichern (**Speichern**) oder verwerfen (**Zurücksetzen**). Andernfalls können Sie das Fenster schließen (**Schließen**).

Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

Bevor Sie das Slave-System mithilfe des Cluster-Verbindungskabels mit dem Master verbinden und Hochverfügbarkeit im Slave-System konfigurieren, muss die Konfiguration des Master-Systems vollständig und aktiviert sein.

Verbinden Sie das Slave-System mit den gleichen „WAN" und „LAN" Netzwerkkomponenten wie das Master-System (siehe *Abbildung 16: Beispiel-Netzwerk für Hochverfügbarkeit* auf Seite 41).

Nur das Master-System kann über den Webclient erreicht und konfiguriert werden.

Wenn Sie die Konfiguration der Hochverfügbarkeit anpassen möchten (zum Beispiel, um das HA-Interface zu ändern), deaktivieren Sie zunächst die Hochverfügbarkeit und nehmen Sie daraufhin Ihre Konfigurationsänderungen vor. Aktivieren Sie die Hochverfügbarkeit erneut mit der neuen Konfiguration.

Um die Firewalls mit dem LANCOM R&S®UF Command Center verwalten zu können, ist es nicht notwendig, beide Firewalls separat zu konfigurieren. Bei aktivierter Hochverfügbarkeit werden die Einstellungen des LANCOM R&S®UF Command Center über den Slave-Knoten synchronisiert, sodass das LANCOM R&S®UF Command Center nur einmal konfiguriert werden muss. Weitere Informationen finden Sie unter *Command Center* auf Seite 38.

Damit die Hochverfügbarkeitsfunktion zuverlässig funktioniert, müssen die Zeiteinstellungen beider Firewalls synchron sein. Sobald Sie die Hochverfügbarkeitsfunktion aktivieren, wird die Zeiteinstellung automatisch wie folgt eingerichtet:

1. NTP-Client und -Server werden auf beiden Firewalls aktiviert.
2. Die Cluster-Link-IPs werden zu beiden Knoten der NTP-Server-Liste hinzugefügt.

Weitere Informationen dazu finden Sie unter *Zeiteinstellungen* auf Seite 53.

Um das Slave-System aus der Hochverfügbarkeitskonfiguration zu entfernen und es als eigenständiges System zu betreiben, klicken Sie den Schiebeschalter, um die Hochverfügbarkeitsfunktion zu deaktivieren. Damit werden die Konfigurationseinstellungen des Slave-Systems und die IP-Adressen der Netzwerk-Interfaces auf Werkseinstellungen zurückgesetzt.

Möglicherweise stehen die Standard-IP-Adressen des Slave nach Zurücksetzen auf Werksteinstellungen mit den Master-IP-Adressen im Konflikt. Weitere Informationen finden Sie unter *Inbetriebnahme* auf Seite 7. Kontaktieren Sie in diesem Fall den Support, um die Master-Einstellungen entsprechend rekonfigurieren zu lassen, bevor Sie die Hochverfügbarkeitsfunktion deaktivieren.

3.4.1.6.2 Arbeitsweise der Hochverfügbarkeitsfunktion

In diesem Kapitel erfahren Sie, wie Sie Hochverfügbarkeit für Ihre LANCOM R&S®Unified Firewall einrichten und bedienen.

Initiale Einrichtung

Zur Verwendung der Hochverfügbarkeitsfunktion benötigen Sie eine dedizierte Cluster-Verbindung für die Kommunikation zwischen zwei Firewalls. Diese Verbindung ist für die korrekte Arbeitsweise der Hochverfügbarkeit essentiell. Verwenden Sie deshalb ein redundantes Interface, z. B. ein gebündeltes Interface, das durch Link Aggregation bereitgestellt wird.

Folgende Interfaces sind als Cluster-Verbindung nicht verwendbar: VLAN, WLAN, PPP, Bridge-Interface.

Verwenden Sie einen Switch, um die Cluster-Verbindung aufzuteilen und somit das Master-System und das Slave-System über SNMP nahtlos überwachen zu können.

Synchronisierung

In diesem Kapitel erhalten Sie Informationen über die Synchronisierung des Master- und Slave-Systems im Rahmen der HA-Konfiguration, des Connection Tracking, der Protokolle und Statistiken sowie Einschränkungen bei der Synchronisierung.

Konfiguration

Alle Konfigurationsänderungen werden mit dem Slave-System synchronisiert. Während des Synchronisierungs- und Aktivierungsprozesses wird die Hochverfügbarkeitsfunktion als **Nicht synchronisiert** angezeigt. Ein Rollenwechsel während der Synchronisierung kann zu Verlust von Daten oder Konfigurationsänderungen führen.

Die Konfigurationsänderungen werden mit einer Verzögerung von 15 Sekunden synchronisiert, um unnötige Aktivierungen im Slave-System zu vermeiden.

Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um eine vollständige Synchronisierung zu starten.

Connection Tracking

Verbindungsbasierte Protokolle, wie TCP, werden in der Firewall getrackt. Die Tracking-Tabellen werden automatisch mit dem Slave-System synchronisiert. Dadurch bleiben die Verbindungen auch nach einem Rollenwechsel erhalten, z. B. während eines Downloadvorgangs.

Protokolle und Statistiken

Ihre LANCOM R&S®Unified Firewall synchronisiert die Protokoll- und Statistikdatenbanken zwischen dem Master- und Slave-System. Die Protokolle des Slave-Systems werden nicht gespeichert, da auf die Slave-Datenbank nur Leserechte bestehen.

Einschränkungen

Die UTM-Features speichern den Status aller Verbindungen, die die Firewall passieren.

Beispiel: Die DPI-Engine speichert Metadaten von bereits analysierten Paketen, bis die Verbindung endet.

Ihre LANCOM R&S®Unified Firewall synchronisiert diesen Verbindungsstatus nicht, speichert diesen aber im Speicher des Master-Systems. Nach einem Rollenwechsel werden alle Verbindungen, die von den UTM-Systemen analysiert wurden, unterbrochen.

Beispiel: Bei der DPI-Engine führt der Verlust der Metadaten dazu, dass neue Pakete zu einer alten Verbindung als unbekannt abgelehnt werden.

Rollenwechsel

Für die Aktiv-Passiv-Hochverfügbarkeitsfunktion bietet die LANCOM R&S®Unified Firewall-Lösung die folgenden Rollen:

- Master-System

  Das Master-System verarbeitet aktiv den Netzwerkverkehr. Der Master ist außerdem verantwortlich für die Weitergabe aller Konfigurations- und Statusänderungen an den Slave, sodass beide Systeme synchron bleiben.

- Slave-System

  Das Slave-System ist ein passives System und fungiert als sofort einsetzbarer Ersatz, um bei Ausfall des Master dessen Aufgaben übernehmen zu können. Der Slave erkennt Konfigurations- und Statusänderungen, wendet diese an und aktiviert sie.

Sobald die Firewall fehlerhaft arbeitet, z. B. aufgrund von Hardware- oder Kernelfehlern, stellt die Hochverfügbarkeitsfunktion eine reibungslose Übernahme der Funktionen durch den Slave sicher. Damit werden Netzwerkausfälle verhindert. Der Übergang wird durch Senden von Gratuitous-ARP-Paketen an alle Hosts in jeder Broadcast-Domäne der Firewall ermöglicht. Diese Hosts lernen, dass die IP-Adressen ab sofort durch den neuen Master beantwortet werden.

ⓘ Die Verwendung der Hochverfügbarkeitsfunktion ist sinnvoll, wenn Sie Ihre Firewalls mit neuerer Hardware ohne Ausfallzeiten ausstatten möchten, z. B. mit Netzwerkmodulen oder SSD-Festplatten.

Lizenzierung

Ihre LANCOM R&S®Unified Firewall-Geräte müssen mit einer digitalen Lizenz für jedes Gerät lizenziert werden. Falls Sie zwei LANCOM R&S®Unified Firewall-Geräte erworben haben, um diese in einer Hochverfügbarkeitsumgebung zu verwenden, erhalten Sie nur eine Lizenz. Beide Firewalls müssen bereits während der Lizenzierung als Hochverfügbarkeits-Cluster konfiguriert und in Betrieb genommen werden. Andernfalls kann die Firewall die Lizenz ablehnen.

Update

Die Installation eines Updates kann in einer Hochverfügbarkeitsumgebung mit hoher Zuverlässigkeit und ohne Ausfallzeiten durchgeführt werden, auch wenn das Update fehlschlägt.

Erstellen Sie eine Sicherung Ihrer Konfiguration, bevor Sie ein Update durchführen. Weitere Informationen zu Updates finden Sie unter *Update-Einstellungen* auf Seite 54.

Der Master steuert den Updatevorgang automatisch wie folgt:

1. Downloaden des Updates oder Upgrades.

   Dieser Schritt wird übersprungen, falls Sie das Update oder Upgrade bereits heruntergeladen haben, oder falls Sie das Firmware-Update manuell auf der Firewall installiert haben, z. B. in einer Offline-Umgebung.
2. Synchronisieren des Updates oder Upgrades mit dem Slave-System über die Cluster-Verbindung.
3. Installation auf dem Slave-System.

   Der Master initiiert die Installation des Updates oder Upgrades auf dem Slave-System. Im Fehlerfall arbeitet der Master wie gewohnt weiter, und der Updatevorgang wird abgebrochen. Kontaktieren Sie in diesem Fall den Support, da ab diesem Zeitpunkt Ausfallzeiten möglich sind.
4. Installation auf dem Slave-System

   Nach der Installation des Updates auf dem Slave wird es auf dem Master-System installiert.

Automatische Updates sind bei aktivierter Hochverfügbarkeitsfunktion nicht erlaubt, um Datenverlust oder Netzwerkausfall zu vermeiden, da nach einer fehlerhaften Updateinstallation ein erfolgreicher Rollenwechsel nicht gewährleistet werden kann.

Wenn beide Systeme nicht synchronisiert sind, können Updates nicht gestartet werden.

Update mit Neustart

Die meisten Updates erfordern einen Neustart nach der Installation. Ein Neustart in einer Hochverfügbarkeitsumgebung steuert einen Rollenwechsel an. Wir empfehlen deshalb die Betreuung des Updates durch einen Administrator.

Der Master steuert den Updatevorgang mit Neustart wie folgt:

1. Downloaden des Updates.
2. Synchronisieren des Updates mit dem Slave-System über die Cluster-Verbindung.
3. Installation auf dem Slave-System.
4. Neustart des Slave.

   Der Slave startet sich automatisch nach erfolgreicher Installation neu.
5. Warten auf Bestätigung durch den Benutzer.

   Der Webclient fordert den Administrator auf, den Updatevorgang fortzusetzen. Fehler, die vor diesem Schritt auftreten, können behoben werden. Wenden Sie sich an den Support, falls Sie hierzu Unterstützung benötigen.
6. Installation auf dem Slave-System.
7. Neustart des Masters.

   Der Master startet sich automatisch nach erfolgreicher Installation neu. Der Rollenwechsel erfolgt bei Neustart.

Upgrade

Um ein Upgrade zu installieren, startet sich Ihre LANCOM R&S®Unified Firewall neu. Der Neustart steuert die Upgrade-Installation an, durch die das System mit der neuen Version neu aufgesetzt wird. Auch bei einem Upgrade wird ein Rollenwechsel angesteuert. Wir empfehlen deshalb die Betreuung des Upgradevorgangs durch den Administrator.

Der Master steuert den Upgradevorgang wie folgt:

1. Downloaden des Updates oder Upgrades.
2. Synchronisieren des Updates oder Upgrades mit dem Slave-System über die Cluster-Verbindung.
3. Installation auf dem Slave-System.
4. Upgrade des Slave-Systems.

   Das Slave-System startet sich neu und startet die Upgrade-Installation automatisch.
5. Warten auf Bestätigung durch den Benutzer.

   Der Webclient fordert den Administrator auf, den Updatevorgang fortzusetzen. Fehler, die vor diesem Schritt beim Slave-System auftreten, können behoben werden. Wenden Sie sich an den Support, falls Sie hierzu Unterstützung benötigen.
6. Installation auf dem Master-System.
7. Upgrade des Master-Systems.

   Der Master startet sich automatisch nach erfolgreicher Installation neu und startet die Upgrade-Installation automatisch. Der Rollenwechsel erfolgt mit dem Neustart.

Synchronisierung

Vor der Updateinstallation deaktiviert Ihre LANCOM R&S®Unified Firewall die Synchronisierung, um die Konfiguration des Slave-Systems nach Installation einer neuen Version abzusichern. Alle Änderungen, die Sie nach Beginn der Update-Installation vorgenommen haben, werden erst nach erfolgreichem Update gespeichert.

Während des Upgrades synchronisiert Ihre LANCOM R&S®Unified Firewall die Protokolle und Statistiken von der alten zur neuen Version.

3.4.1.6.3 Monitoring

Falls sich ein Gerät offline schaltet und sich nicht selbständig wieder verbinden kann, z. B. aufgrund von Hardwareproblemen, muss der Administrator schnellstmöglich reagieren und das Problem beheben oder das fehlerhafte Gerät ersetzen. Ein Cluster, der nicht korrekt arbeitet, kann Ausfallzeiten nicht vermeiden. Deshalb ist es notwendig, die Firewalls bei aktivierter Hochverfügbarkeitsfunktion zu überwachen. Dies kann folgendermaßen erfolgen:

- Webclient

  Sie können die Hochverfügbarkeitsfunktion im *Infobereich* und im Hochverfügbarkeitsmenü (siehe *Hochverfügbarkeit* auf Seite 40) überwachen. Welche Firewall aktuell als Master konfiguriert ist, entnehmen Sie aus der lokalen IP-Adresse.
- SNMP

  SNMP ist der Standard für das Monitoring der Firewall. Informationen zur Konfiguration der Firewall und Hinweise zum Download der notwendigen MIB-Dateien entnehmen Sie *SNMP-Einstellungen* auf Seite 75. SNMP-Anfragen an die Firewall helfen Ihnen, die aktive Firewall zu identifizieren, indem Sie die IP-Adresse der Cluster-Verbindung ablesen.

  Die Überwachung des Slave-Knotens kann nur über die Cluster-Verbindung erfolgen. Um auf diese Schnittstelle zugreifen zu können, verwenden Sie einen Switch, wie in *Initiale Einrichtung* auf Seite 43 beschrieben.
- Remote Syslog-Server

Sie können einen entfernten Syslog-Server verwenden, um Hochverfügbarkeitsereignisse zu überwachen, da Clustermeldungen in den Syslog-Protokollen enthalten sind. Rollenwechsel werden klar protokolliert. Die IP-Adresse des Masters können Sie ebenfalls aus den Protokollen entnehmen.

Die Protokolle des Slave-Knotens werden nicht an den entfernten Syslog-Server gesendet. Die Protokolle des Masterknotens sind ausreichend, um die wichtigsten Informationen zu erhalten.

- Command Center

  Verwenden Sie das LANCOM R&S®UF Command Center, um den Hochverfügbarkeitsstatus mehrerer Firewalls zu überwachen, sowie Lizenzstatus und Hardwareressourcen zu prüfen.

3.4.1.7 Lizenz

Die genauen Funktionen Ihrer LANCOM R&S®Unified Firewall Software sind abhängig von der Lizenz, die Sie von Ihrem Lieferanten erworben haben.

Folgende Features sind einzeln mit der erworbenen Lizenzdatei lizenzierbar:

- Antispam (UTM-Lizenz)
- Antivirus (UTM-Lizenz)
- Application-Filter
- Contentfilter
- IDS/IPS (UTM-Lizenz)
- WLAN

Navigieren Sie zu **Firewall** > **Lizenz**, um den **Lizenzmanager** zu öffnen, mithilfe dessen Sie die Gültigkeitsdauer Ihrer LANCOM R&S®Unified Firewall-Lizenz und zusätzliche Funktionslizenzen einsehen oder neue Lizenzen hochladen können.

Beim ersten Start nach der Lieferung oder nach einer Neuinstallation läuft die LANCOM R&S®Unified Firewall für 30 Tage als Testversion. Während des Testzeitraums können Sie kein Backup erstellen. Nach Ablauf des Testzeitraums bleibt die Firewall weiterhin mit Ihrer Konfiguration erhalten. Die UTM-Features werden deaktiviert und Sie können keine Änderungen mehr speichern.

Das System prüft in regelmäßigen Abständen die Ablaufdaten der Lizenzen in der Lizenzdatei. Läuft eine Lizenz ab oder endet der Testzeitraum, werden alle lizenzierbaren Funktionen deaktiviert, bis Sie eine neue Lizenz über den Webclient hochladen. Nach Ablauf der Lizenz wird Web- und E-Mail-Verkehr blockiert oder fortan ungefiltert durch die LANCOM R&S®Unified Firewall geleitet. Im ersten Fall sehen Sie sofort, daß Sie eine neue Lizenz herunterladen müssen, wenn Ihre aktuell verwendeten Lizenzdaten ausgelaufen sind. Wenn Sie das System nach Lizenzablauf in einem unsicheren Modus betreiben, werden Sie nur auf der Benutzeroberfläche der LANCOM R&S®Unified Firewall benachrichtigt. Sie können dieses im **Lizenzmanager** konfigurieren:

Abbildung 17: Konfiguration des End-Of-License-Verhaltens

Unabhängig vom konfigurierten End-of-License-Verhalten werden Funktionen in der Benutzeroberfläche stets deaktiviert, wenn die Hauptlizenz abgelaufen ist.

Nach Ablauf einer Featurelizenz wird das entsprechende Feature deaktiviert. Der Einstellungsdialog für dieses Feature kann weiterhin geöffnet werden. Im Dialog wird angezeigt, dass die Lizenz abgelaufen ist. Falls Sie versuchen, Änderungen vorzunehmen, erscheint eine Fehlermeldung.

Die Lizenzinformationen im *Infobereich* des Webclients erscheinen in roter Schrift, sobald der Zeitraum bis zum Ablauf der Lizenz weniger als 30 Tage beträgt.

Für eine nichtlizenzierte LANCOM R&S®Unified Firewall wird im Infobereich eine temporäre Seriennummer angezeigt. Diese wird nach Erwerb einer Lizenz durch eine gültige Lizenznummer ersetzt.

Falls Sie die LANCOM R&S®Unified Firewall auf einer virtuellen Maschine installiert haben, wird die UUID der virtuellen Maschine im Infobereich angezeigt.

Unter **Lizenz-Upload** können Sie eine neue Lizenz für Ihre LANCOM R&S®Unified Firewall-Software hochladen. Gehen Sie dazu wie folgt vor:

1. Klicken Sie neben dem **Datei auswählen**-Eingabefeld auf **Lizenzdatei**.

   Die Suchfunktion des lokalen Datenträgers öffnet sich.

2. Wählen Sie eine Lizenzdatei im GPLF- oder LIC-Format aus.

   Die neue Lizenz muss der Versionsnummer der LANCOM R&S®Unified Firewall-Software und der Hardware entsprechen.

3. Klicken Sie auf **Öffnen**.

   Die Suchfunktion des lokalen Datenträgers schließt sich.

4. Um die Lizenzdatei hochzuladen, klicken Sie auf **Speichern**.

   Die Lizenz wird hochgeladen. War der Upload erfolgreich, werden alle Lizenzen und die zugehörigen Informationen automatisch auf Ihre LANCOM R&S®Unified Firewall übertragen und eine Erfolgsmeldung erscheint.

5. Bestätigen Sie, dass Sie sich ausloggen möchten, indem Sie auf **OK** klicken.

   Sie werden ausgeloggt. Die Login-Seite der Firewall wird geöffnet.

6. Geben Sie Ihre Login-Daten ein.

7. Klicken Sie auf **Anmelden**.

   Der Webclient erscheint.

Die hochgeladene Lizenz können Sie auch wieder herunterladen. Dazu einfach die weiter oben neben **Download** als Link angezeigte Lizenzdatei anklicken, sodass der Download der Datei startet.

Im Tab **Details** können Sie weiterführende Lizenzinformationen Ihrer LANCOM R&S®Unified Firewall-Software einsehen, z. B. Informationen zu den UTM-Lizenzen. Außerdem können Sie dort die maximale Anzahl gleichzeitiger VPN-Tunnel sehen. Ist diese Anzahl erreicht, werden Verbindungsversuche weiterer IPsec-Clients oder Gegenstellen abgelehnt.

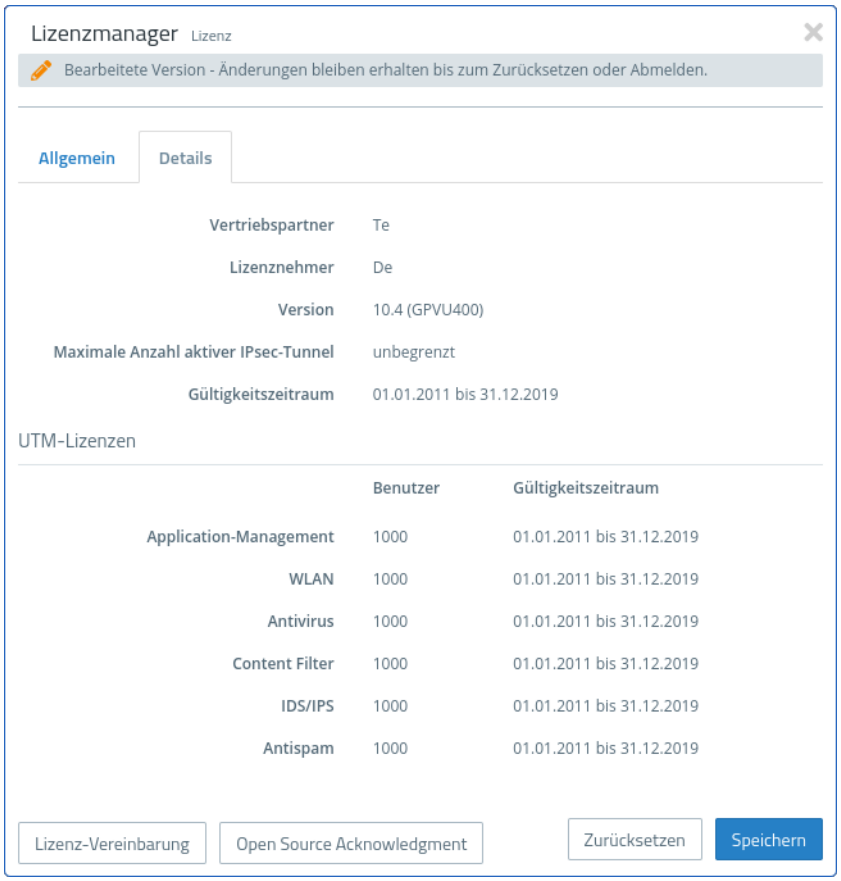


Abbildung 18: Beispiel für weiterführende Lizenzinformationen

3.4.1.8 LANCOM Management Cloud-Einstellungen

Hier finden Sie die Einstellungen für die Konfiguration und das Monitoring Ihres Gerätes durch die LANCOM Management Cloud (LMC).

Navigieren Sie zu **Firewall** > **LMC-Einstellungen**, um ein Bearbeitungsfenster zu öffnen, in dem Sie die Einstellungen für die LMC anzeigen und anpassen können.

Im Bearbeitungsfenster **LMC-Einstellungen** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
I/0	Ein Schiebeschalter gibt an, ob die Verwaltung der Firewall über die LANCOM Management Cloud aktiv (**I**) oder inaktiv (**0**) ist. Mit einem Klick auf den Schiebeschalter ändern Sie den Status dieser Option.
LMC-Domain	Geben Sie hier den Domain-Namen der LMC an. Standardmäßig ist die Domain für den ersten Verbindungsaufbau mit der Public LMC eingetragen. Möchten Sie Ihr Gerät von einer eigenen Management Cloud verwalten lassen („Private Cloud“ oder „on premise installation“), tragen Sie bitte die entsprechende LMC-Domain ein.

Eingabefeld	Beschreibung
Aktivierungscode	Alternativ zur Eingabe der Seriennummer und der dem Gerät beiliegenden Cloud-PIN kann ein Gerät auch über einen Aktivierungscode einem Projekt in der LMC zugewiesen werden. Klicken Sie dazu in der LMC unter **Geräte** auf **Aktivierungscodes**, danach auf **Aktivierungscode erstellen**. Sie können dort einen zeitlich beschränkt gültigen Aktivierungscode generieren. Dieser kann innerhalb des Gültigkeitszeitraums auf beliebig vielen LANCOM Geräten zur Aktivierung, also zur Übernahme in die LMC, genutzt werden.

3.4.1.9 Zugriff auf die Firewall

Mit den Einstellungen unter **Firewall-Zugriff** können Sie den Zugriff auf Ihre LANCOM R&S®Unified Firewall aus externen Netzwerken oder dem Internet regeln. Außerdem können Sie festlegen, wie Ihre LANCOM R&S®Unified Firewall beispielsweise auf eine Ping-Anforderung reagieren soll.

Die Einstellungen unter **Firewall-Zugriff** gelten nur für den externen Zugriff auf die LANCOM R&S®Unified Firewall für festgelegte Benutzer. Der Zugriff auf die LANCOM R&S®Unified Firewall aus dem internen Netzwerk ist immer möglich.

Navigieren Sie zu **Firewall** > **Firewall-Zugriff**, um festzulegen, ob und wie der Zugriff auf die LANCOM R&S®Unified Firewall aus externen Netzwerken erlaubt wird.

Weiterführende Informationen zu den Einstellungen unter **Firewall-Zugriff** finden Sie in den folgenden Abschnitten.

3.4.1.9.1 Ping-Einstellungen

Mit den **Ping-Einstellungen** können Sie festlegen, wie Ihre LANCOM R&S®Unified Firewall mit ICMP-Echoanfragen (Pings) an die Firewall aus dem internen Netzwerk und dem Internet umgeht.

Navigieren Sie zu **Firewall** > **Firewall-Zugriff** > **Ping-Einstellungen**, um ein Bearbeitungsfenster zu öffnen, in dem Sie die Ping-Einstellungen anzeigen und anpassen können.

Eingabefeld	Beschreibung
IPv4-Ping zur Firewall erlauben **IPv6-Ping zur Firewall erlauben**	Konfigurieren Sie getrennt für IPv4 bzw. IPv6, wie Ihre LANCOM R&S®Unified Firewall mit ICMP-Echoanfragen an die Firewall aus dem internen Netzwerk und dem Internet umgeht. Die Option ist standardmäßig auf „Verweigern“ gesetzt, bei Bedarf können Sie dies aber auch auf „Erlauben“ ändern. › „Verweigern“ – Ihre LANCOM R&S®Unified Firewall antwortet nicht auf ICMP-Echoanfragen aus dem internen Netzwerk und aus dem Internet. › „Erlauben“ – Ihre LANCOM R&S®Unified Firewall antwortet auf ICMP-Echoanfragen aus dem internen Netzwerk und aus dem Internet. Obwohl das Blockieren von ICMP-Echoanfragen die Sicherheit der LANCOM R&S®Unified Firewall erhöhen kann, kann es beim Troubleshooting im Netzwerk hinderlich sein. Wenn ein Fehler im Netzwerk auftritt, wird daher empfohlen, diese Option auf `Erlauben` zu setzen, bevor Sie mit dem Troubleshooting beginnen.

Wenn Sie diese Einstellungen ändern, klicken Sie zum Speichern Ihrer Änderungen auf **Speichern** oder auf **Zurücksetzen**, um sie zu verwerfen. Klicken Sie ansonsten auf **Schließen**, um das Bearbeitungsfenster zu schließen.

Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

3.4.1.9.2 SSH-Einstellungen

Mit den Einstellungen unter **SSH-Einstellungen** können Sie den SSH-Zugriff auf Ihre LANCOM R&S®Unified Firewall aus dem Internet regeln.

Navigieren Sie zu **Firewall** > **Firewall-Zugriff** > **SSH-Einstellungen**, um ein Bearbeitungsfenster zu öffnen, in dem Sie die SSH-Einstellungen anzeigen und anpassen können.

Im Teilbereich unter **SSH-Einstellungen** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
I/0	Ein Schiebeschalter gibt an, ob der jeweilige SSH Dienst derzeit aktiv (**I**) oder inaktiv (**0**) ist. Indem Sie auf den Schiebeschalter klicken, können Sie den Status des Dienstes ändern. Der SSH-Dienst ist standardmäßig aktiviert.
Port	Legen Sie den Listening-Port fest, indem Sie die Portnummer eingeben. Die Standardeinstellung ist Port 22.
Passwort-Authentifizierung	Mittels Passwort-Authentifizierung können Sie sich mit einem Passwort über SSH bei Ihrer LANCOM R&S®Unified Firewall anmelden. Die Passwort-Authentifizierung ist standardmäßig aktiviert. Die Passwort-Authentifizierung kann nur deaktiviert werden, wenn stattdessen mindestens ein öffentlicher SSH-Schlüssel aktiv zur Authentifizierung mittels Schlüssel genutzt wird.
SSH Öffentliche Schlüssel	Diese Tabelle zeigt die öffentlichen SSH-Schlüssel an, die zur Authentifizierung von Benutzern ohne Passwort verwendet werden. Klicken Sie auf **Hinzufügen**, um das Fenster **SSH-Schlüssel** zu öffnen und einen neuen Schlüssel hinzuzufügen. In diesem Fenster können Sie die folgenden Einstellungen vornehmen: › Fügen oder geben Sie im Feld **Schlüssel** den öffentlichen SSH-Schlüssel ein. › Geben Sie im Feld **Titel** einen Namen für den öffentlichen SSH-Schlüssel ein. LANCOM R&S®Unified Firewall unterstützt nur Schlüssel im Secure Shell (SSH) Public Key File Format. Wenn Sie diese Einstellungen ändern, klicken Sie zum Speichern Ihrer Änderungen auf **Speichern** oder auf **Zurücksetzen**, um sie zu verwerfen. Klicken Sie ansonsten auf **Schließen**, um das Bearbeitungsfenster zu schließen. Der öffentliche SSH-Schlüssel erscheint als Listeneintrag (**Fingerprint**). Sie können einzelne Einträge in den Listen bearbeiten oder löschen, indem Sie auf die entsprechende Schaltfläche neben einem Eintrag klicken. Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28. Sie können die beiden Authentifizierungsmethoden (**Passwort-Authentifizierung**, **SSH Öffentliche Schlüssel**) einzeln oder in Kombination verwenden.
Zugriffs-Beschränkungen	Diese Tabelle zeigt die benutzerdefinierten IP-Adressen oder IP-Netzwerke an, denen Zugriff auf Ihre LANCOM R&S®Unified Firewall gewährt werden kann (Whitelist-Modus). Setzen Sie den Haken im Kontrollkästchen neben einem Eintrag, um den Zugriff zu erlauben. Um eine IP-Adresse oder ein Netzwerk zur Liste hinzuzufügen, geben Sie **Titel** sowie **Quelle** ein und klicken Sie auf **Hinzufügen**. Der neue Eintrag wird zur Liste hinzugefügt und automatisch aktiviert. Die folgenden Einträge sind standardmäßig angelegt und können nicht entfernt werden: › **Lokale Netzwerke** stellt den internen Zugriff dar und ist standardmäßig aktiviert.

Eingabefeld	Beschreibung
	› **Internet** ermöglicht SSH-Zugriff auf Ihre LANCOM R&S®Unified Firewall aus dem Internet. Unter gewissen Umständen kann dies Angreifern Zugriff auf Ihre LANCOM R&S®Unified Firewall ermöglichen. Daher wird diese Option nicht als dauerhafte Lösung empfohlen. › **VPN Tunnel** Die folgenden standardmäßig angelegten Einträge enthalten Netzwerkabschnitte für den Kundensupport. Diese Einträge sind standardmäßig deaktiviert. › **Rohde & Schwarz Internet Gateway** › **Rohde & Schwarz Cybersecurity Kundensupport**

Wenn Sie diese Einstellungen ändern, klicken Sie zum Speichern Ihrer Änderungen auf **Speichern** oder auf **Zurücksetzen**, um sie zu verwerfen. Klicken Sie ansonsten auf **Schließen**, um das Bearbeitungsfenster zu schließen.

Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

3.4.1.9.3 Webclient-Einstellungen

Mit den Einstellungen unter **Webclient-Einstellungen** können Sie den externen-Webzugriff auf Ihre LANCOM R&S®Unified Firewall aus dem Internet regeln.

Navigieren Sie zu **Firewall** > **Firewall-Zugriff** > **Webclient-Einstellungen**, um ein Bearbeitungsfenster zu öffnen, in dem Sie die Webclient-Einstellungen anzeigen und anpassen können.

Im Teilbereich unter **Webclient-Einstellungen** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Port	Legen Sie den Listening-Port fest, indem Sie die Portnummer eingeben. Die Standardeinstellung ist Port 3438.
Webclient-Zertifikat	Wählen Sie ein Webclient-Zertifikat aus, das zur Verifikation der SSL-Verbindung dient. Wenn Sie kein Webclient-Zertifikat auswählen, wird ein automatisch generiertes, selbst signiertes Systemzertifikat verwendet. Das Systemzertifikat ist nicht Teil der Zertifikatsverwaltung. Damit Ihr Browser beim Verbinden mit dem Webclient keine Zertifikatswarnung anzeigt, wählen Sie ein Zertifikat, das von einer Zertifizierungsstelle (CA) ausgestellt wurde, der Ihr Browser vertraut.
Zugriffs-Beschränkungen	Diese Tabelle zeigt benutzerdefinierte IP-Adressen oder IP-Netzwerke an, denen einzeln Zugriff gewährt werden kann (Whitelist-Modus). Geben Sie **Titel** und **Quelle** ein. Klicken Sie auf **Hinzufügen**, um die IP-Adresse zur Liste hinzuzufügen. Die folgenden Einträge sind schreibgeschützt, können aber aktiviert und deaktiviert werden. › **Lokale Netzwerke** stellt den internen Zugriff dar und ist standardmäßig aktiviert. › **Internet** ermöglicht SSH-Zugriff auf Ihre LANCOM R&S®Unified Firewall aus dem Internet. Unter gewissen Umständen kann dies Angreifern Zugriff auf Ihre LANCOM R&S®Unified Firewall ermöglichen. Daher wird diese Option nicht als dauerhafte Lösung empfohlen. › **VPN Tunnel**

Eingabefeld	Beschreibung
	Die folgenden standardmäßig angelegten Einträge enthalten Netzwerkabschnitte für den Kundensupport. Die Einträge sind standardmäßig deaktiviert. › **Rohde & Schwarz Internet Gateway** › **Rohde & Schwarz Cybersecurity Kundensupport** Optional: Entfernen Sie den Haken im Kontrollkästchen neben einem Eintrag, um den Zugriff darauf zu beschränken. Der Zugriff auf den Server erfolgt hauptsächlich über den Webclient. Sie müssen mindestens einen Eintrag in der Liste der IP-Adressen auswählen.

Wenn Sie diese Einstellungen ändern, klicken Sie zum Speichern Ihrer Änderungen auf **Speichern** oder auf **Zurücksetzen**, um sie zu verwerfen. Klicken Sie ansonsten auf **Schließen**, um das Bearbeitungsfenster zu schließen.

Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

3.4.1.10 Zeiteinstellungen

Ihre LANCOM R&S®Unified Firewall arbeitet mit zeitempfindlichen Regeln. Darüber hinaus ist die Systemzeit für Dienste wie die Protokollierung und Berichterstattung besonders wichtig, da diese auf genaue und allgemein akzeptierte Zeitstempel angewiesen sind. Daher ist es notwendig, die korrekten Daten und Uhrzeiten festzulegen.

Navigieren Sie zu **Firewall** > **Zeit-Einstellungen**, um ein Bearbeitungsfenster zu öffnen, in dem Sie die Zeiteinstellungen für das System anzeigen und anpassen können.

Im Bearbeitungsfenster **Zeiteinstellungen** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Zeitzone	Wählen Sie aus der Drop-down-Liste eine der vordefinierten Zeitzonen aus. Die Zeitzone ist standardmäßig auf `(+01:00) Europa - Berlin` gesetzt.
Aktuelle Zeit	Prüfen Sie das aktuelle Systemdatum (MM/TT/JJJJ) und Uhrzeit (hh:mm:ss) der LANCOM R&S®Unified Firewall.
Datum & Zeit	Optional: Klicken Sie auf das Eingabefeld, um Systemdatum oder Uhrzeit manuell neu einzustellen. Ein Pop-up-Fenster mit einem Kalender und Eingabefeldern zum Ändern von Datum und Uhrzeit öffnet sich. Sie können das Datum im Format MM/TT/JJJJ eingeben oder im Auswahlfenster ein Datum auswählen. Optional können Sie die Uhrzeit im Format hh:mm:ss eingeben. Um die Zeit manuell einzustellen, muss NTP deaktiviert sein. Entfernen Sie hierzu den Haken im Kontrollkästchen **NTP-Client**. Andernfalls wird die Zeit automatisch zurückgesetzt, sobald das System die nächste NTP-Anfrage sendet.
NTP-Client	Optional: Setzen Sie den Haken in diesem Kontrollkästchen, um entfernte Netzwerkzeit-Protokollserver zu nutzen, um Datum und Uhrzeit für das System automatisch zu beziehen.
NTP-Server	Optional und nur verfügbar, wenn der Haken im Kontrollkästchen **NTP-Client** gesetzt wurde: Verwenden Sie entweder die vordefinierten NTP-Server oder fügen Sie eigene NTP-Server zur Liste hinzu. Die Standard-NTP-Server sind: *de.pool.ntp.org* und *europe.pool.ntp.org*. Sie können beliebig viele NTP-Server hinzufügen. Geben Sie im Eingabefeld die IP-Adresse oder den vollständig qualifizierten Domain-Namen eines NTP-Servers ein. Klicken Sie anschließend auf **Hinzufügen**, um den NTP-Server zur Liste hinzuzufügen. Sie können einzelne Einträge in der Liste bearbeiten oder löschen, indem Sie auf die entsprechende Schaltfläche neben einem Eintrag klicken. Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28.

Eingabefeld	Beschreibung
	Wenn Sie einen NTP-Server bearbeiten, erscheint auf der rechten Seite des Eintrags ein Haken. Sie müssen Ihre Änderungen an den Einstellungen zum NTP zunächst mit diesem Haken bestätigen, bevor Sie sie speichern können. Wenn mehr als ein NTP-Server konfiguriert ist, synchronisiert Ihre LANCOM R&S®Unified Firewall die Systemuhr automatisch mit dem Server, der das beste Zeitsignal übermittelt.
Als lokaler NTP-Server verwenden	Optional und nur verfügbar, wenn der Haken im Kontrollkästchen **NTP-Client** gesetzt wurde: Aktivieren Sie dieses Kontrollkästchen, wenn Sie die Systemuhrzeit Ihrer LANCOM R&S®Unified Firewall im internen Netzwerk zur Verfügung stellen wollen. Ihre LANCOM R&S®Unified Firewall agiert dann als interner, lokaler NTP-Server.

Wenn Sie diese Einstellungen ändern, klicken Sie zum Speichern Ihrer Änderungen auf **Speichern** oder auf **Zurücksetzen**, um sie zu verwerfen. Klicken Sie ansonsten auf **Schließen**, um das Bearbeitungsfenster zu schließen.

Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

3.4.1.11 Update-Einstellungen

Im Bearbeitungsfenster **Updates-Einstellungen** können Sie Ihre LANCOM R&S®Unified Firewall immer auf dem neuesten Stand halten. Neue Versionen der Betriebssysteme LCOS FX, Sicherheits-Updates und neue Funktionen können automatisch vom Update-Server heruntergeladen und schnell und einfach auf der Firewall installiert werden. Das Updatesystem verfügt über verschiedene Funktionen, die den Systemadministrator über neue Updates benachrichtigen. Außerdem können Sie den Verlauf importierter Updates anzeigen lassen.

Um die Installation unberechtigter oder bösartiger Updates auf der Firewall zu vermeiden, werden alle LCOS FX-Updates digital signiert. Nur Updates mit gültiger Signatur werden angezeigt und installiert.

Navigieren Sie zu **Firewall** > **Updates-Einstellungen**, um ein Bearbeitungsfenster zu öffnen, in dem die Liste der verfügbaren Updates mit zusätzlichen Informationen und ihrem Status im Tab **Updates** angezeigt wird.

Im Eingabefeld **Filter** können Sie die Ergebnisse in der Tabelle darunter eingrenzen. Während Sie Ihre Suche in das Eingabefeld eintippen, zeigt Ihre LANCOM R&S®Unified Firewall nur diejenigen Einträge an, die die eingegebenen Zeichen im Namen, Typ oder in der Beschreibung enthalten. Klicken Sie auf ⊗ im Eingabefeld, um die Sucheingabe zu löschen und zur ungefilterten Listenansicht zurückzukehren.

Die Tabellenspalten der Updateliste enthalten die folgenden Informationen:

Spalte	Beschreibung
Name	Zeigt den Namen des verfügbaren Updates an.
Typ	Zeigt den Typ des Updates an. Das Updatesystem unterscheidet vier Typen von Updates: › `Sicherheit` – enthält Verbesserungen bezüglich der Sicherheit der Firewall. › `Empfohlen` – enthält sowohl Verbesserungen als auch Leistungs- und Stabilitätsoptimierungen. › `Hotfix` – enthält Verbesserungen einzelner Module der Firewall, aber auch neue Funktionen. › `Upgrade` – enthält ein Upgrade auf die nächste Softwareversion von LCOS FX.
Beschreibung	Zeigt ein Textfeld mit weiteren Informationen über das Update an. Klicken Sie das Textfeld an, um es zu erweitern und alle Informationen zum Update anzuzeigen.

Spalte	Beschreibung
Neustart	Gibt an, ob ein Neustart des Systems erforderlich ist, nachdem ein Update erfolgreich installiert wurde.
Release-Datum	Zeigt das Veröffentlichungsdatum des Updates an.
Status	Unterscheidet zwischen neuen Updates und Updates, die bereits installiert wurden. Ein Update kann nur einmal installiert werden.
Aktion / Abhängigkeiten	Wenn alle Abhängigkeiten erfüllt sind, ist die Aktion **Installieren** erlaubt. Andernfalls wird eine Liste der Abhängigkeiten angezeigt. Um die Abhängigkeiten zu erfüllen, installieren Sie die aufgelisteten Updates.

Klicken Sie auf **Liste der Updates aktualisieren**, um die Liste der verfügbaren Updates mit den neusten Versionen manuell zu aktualisieren.

Mit den Einstellungen im Tab **Einstellungen** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Automatisch nach Updates suchen	Setzen Sie den Haken in diesem Kontrollkästchen, um die Liste der verfügbaren Updates mit den neusten Versionen automatisch zu aktualisieren.
Intervall	Wählen Sie aus der Drop-down-Liste das gewünschte Aktualisierungsintervall für die Updateliste aus. Diese Option ist standardmäßig auf `Täglich` gesetzt. Mögliche Werte: › `Stündlich` › `Täglich` › `woechentlich`
Update-Zeit	Geben Sie Datum und Uhrzeit der ersten automatischen Aktualisierung der Updateliste und des ersten automatischen Updates ein. Ein Pop-up-Fenster mit einem Kalender und Eingabefeldern zum Anpassen von Datum und Uhrzeit öffnet sich. Sie können das Datum im Format MM/TT/JJJJ eingeben oder im Auswahlfenster ein Datum auswählen. Sie können außerdem die neue Uhrzeit im Format hh:mm:ss eingeben. Wenn Sie die unten beschriebene automatische Installation von Updates aktiviert haben, werden alle folgenden Updates zur hier angegebenen Uhrzeit ausgeführt.
Updates automatisch installieren	Wählen Sie die entsprechende Optionsschaltfläche aus, um festzulegen, welche Updates automatisch auf Ihrer LANCOM R&S®Unified Firewall installiert werden sollen. Diese Funktion beschränkt sich auf Sicherheitsupdates und empfohlene Hotfixes. Diese Option ist standardmäßig auf `Keine` gesetzt, Sie können die Einstellungen jedoch bei Bedarf auf einen der anderen Werte setzen.
Update-Server	Der Standard-Updateserver ist: **https://firmware.fx-update.lancom-systems.com** Sie können beliebig viele Update-Server hinzufügen. Geben Sie im Eingabefeld die URL des Updateservers ein und klicken Sie dann auf **Hinzufügen**. Der Server wird zur Liste hinzugefügt. Wenn die URL einen vollständig qualifizierten Domain-Namen (FQDN) enthält, müssen Sie die DNS-Einstellungen konfigurieren. Andernfalls kann der FQDN nicht aufgelöst werden.

Eingabefeld	Beschreibung
	Sie können einzelne Einträge in der Liste bearbeiten oder löschen, indem Sie auf die entsprechende Schaltfläche neben einem Eintrag klicken. Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28. Wenn Sie einen Update-Server bearbeiten, erscheint auf der rechten Seite des Eintrags ein Haken. Sie müssen Ihre Änderung zunächst mit diesem Haken bestätigen, bevor Sie die Einstellungen zum Update-Server speichern können.

Mit den Einstellungen im Tab **Automatische Wiederherstellung** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Automatische Wiederherstellung	Setzen Sie den Haken in diesem Kontrollkästchen, um die automatische Wiederherstellung im Fehlerfall durchzuführen. Falls nach einem Update auf eine neue Firmware-Version innerhalb der in **Timeout** konfigurierten Zeit keine Anmeldung durch einen Administrator, die LANCOM Management Cloud oder das LANCOM R&S®UF Command Center erfolgt ist, dann wird ein Problem angenommen und eine automatische Wiederherstellung der vorherigen Firmware-Version durchgeführt. Die Wiederherstellungspunkte können über das System-Menü angezeigt werden. Die Wiederherstellung ist auch bei aktivierter Hochverfügbarkeit möglich, hat aber die Einschränkung, dass lediglich die Hauptfirewall wiederhergestellt wird. Die Ersatzfirewall ist nicht mehr verwendbar und muss neu aufgesetzt werden.
Timeout	Zeitlimit in Minuten, nach dem die automatische Wiederherstellung ggfs. durchgeführt wird.

Im Tab **Verlauf** wird der Verlauf der LANCOM R&S®Unified Firewall-Updates angezeigt.

Wenn Sie diese Einstellungen ändern, klicken Sie zum Speichern Ihrer Änderungen auf **Speichern** oder auf **Zurücksetzen**, um sie zu verwerfen. Klicken Sie ansonsten auf die Schaltfläche **Schließen**, um das Fenster zu schließen und zur Übersicht Ihres gesamten konfigurierten Netzwerks zurückzukehren.

Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

Informationen zur Installation von Systemupdates in einer Hochverfügbarkeit-Konfiguration finden Sie unter *Update* auf Seite 45.

3.4.2 Monitoring & Statistiken

Die **Monitoring & Statistiken** Einstellungen zeigen detaillierte Informationen zum Datenverkehr an, der durch Ihre LANCOM R&S®Unified Firewall fließt. Mit den Einstellungen können Sie Remote-SNMP- und Syslog-Server konfigurieren, um von verschiedenen Meldungsquellen erzeugte Ereignisprotokoll-Meldungen weiterzuleiten. Außerdem können Sie konfigurieren, wie mit verschiedenen erkannten Ereignistypen umgegangen werden soll und für welche davon Statistiken geführt werden sollen.

3.4.2.1 Einstellungen zu Statistiken

Navigieren Sie zu **Monitoring & Statistiken** > **Einstellungen**, um die Statistiken anzupassen.

Außerdem können Sie konfigurieren, wie mit verschiedenen von Ihrer LANCOM R&S®Unified Firewall erkannten Ereignistypen umgegangen werden soll und für welche davon Statistiken geführt werden sollen. Wählen Sie aus den Drop-down-Listen für jeden **Ereignis-Typ** eine der folgenden Optionen aus:

Modus	Beschreibung
Deaktiviert	Für diesen Ereignistyp werden keine Daten erhoben.

Modus	Beschreibung
Statistiken führen	Daten über Ereignisse werden erhoben, um Statistiken zu führen
Rohdaten an externe Syslog-Server weitergeben	Daten über Ereignisse werden für die Erstellung von Statistiken erhoben und an einen konfigurierten externen Syslog-Server weitergegeben.
Rohdaten lokal speichern	Daten über Ereignisse werden für die Erstellung von Statistiken erhoben, an einen konfigurierten externen Syslog-Server weitergegeben und auf dem Gerät gespeichert. Dieser Modus kann dazu führen, dass die Speicherkapazität des Geräts schnell erreicht wird.

Bewegen Sie die Maus über das Icon ❶ neben der Bezeichnung eines Ereignistyps, um eine Erklärung dazu anzuzeigen, in welchen Graph ein bestimmtes Ereignis fließt. Mit der Drop-down-Liste **Alle Ereignis-Typen** können Sie alle Ereignistypen auf einmal auf den gleichen Modus setzen.

In der Spalte **LMC** wird angezeigt, wenn in der LANCOM Management Cloud die Weiterleitung von generierten Meldungen zu Ereignistypen eingestellt wurde. Alle an die LANCOM Management Cloud gesendeten Ereignistypen werden mit einem grünen Haken dargestellt. Für die Ereignistypen mit einem X werden zwar keine einzelnen Ereignisse übertragen, aber die Anzahl der aufgetretenen Ergeignisse dennoch an die LANCOM Management Cloud gesendet.

Diese Einstellungen lassen sich über die LANCOM R&S®Unified Firewall nicht direkt ändern. Dies ist nur über die LANCOM Management Cloud möglich. Die Einstellungen werden hier nur der Transparenz halber angezeigt.

Wenn Sie Änderungen vorgenommen haben, können Sie diese mit den Schaltflächen unten rechts im Bearbeitungsfenster speichern (**Speichern**) oder verwerfen (**Zurücksetzen**). Andernfalls können Sie das Fenster schließen (**Schließen**).

Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

3.4.2.2 Benachrichtigungs-Einstellungen

Über das Benachrichtigungs-System können Sie entweder sofort oder regelmäßig in aggregierter Form per E-Mail Nachrichten über bestimmte Benachrichtigungstypen erhalten. Voraussetzung hierfür ist eine aktive E-Mail-Funktion, in der zumindest ein Absender eingestellt ist. Zur Absicherung sind die optionalen Einstellungen **Remote-Zertifikat verifizieren** für die Sicherstellung der korrekten Gegenstelle für den E-Mail-Empfang und **S/MIME-Zertifikat** zur Verschlüsselung der ausgehenden Mail. Näheres hierzu unter *E-Mail-Einstellungen* auf Seite 39

Navigieren Sie zu **Monitoring & Statistiken** > **Benachrichtigungs-Einstellungen**, um ein Bearbeitungsfenster zu öffnen, in dem Sie die folgenden Elemente konfigurieren können:

Tabelle 1: Allgemein

Eingabefeld	Beschreibung
I/**0**	Ein Schiebeschalter gibt an, ob die Benachrichtigungs-Einstellungen derzeit aktiv (**I**), oder inaktiv (**0**) sind. Mit einem Klick auf den Schiebeschalter können Sie den Status ändern.
Benachrichtigungssprache	Stellen Sie die in den Benachrichtigungsmails verwendete Sprache ein. Beim ersten Öffnen des Dialogs wird die für den Webclient eingestellte Sprache verwendet.
Betreff-Vorlage	Legen Sie den Betreff der Benachrichtigungsmail fest.
Empfänger	Liste an Empfänger-Adressen, an die alle Benachrichtigungen verschickt werden. Klicken Sie rechts auf ⊕, um Ihren Eintrag zur Liste hinzuzufügen.

Im Bereich **Aggregierte Benachrichtigungen** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Aggregations-Intervall	Die aufgezeichneten Ereignisse werden gesammelt und in einem festgelegten Intervall zusammengefasst als Mail verschickt. Geben Sie hier die Zeitdauer in Minuten an, in der die Ereignisse gesammelt werden, bevor sie als eine Nachricht verschickt werden.
Max. Anzahl Benachrichtigungen pro Mail	Hier legen Sie fest, wie viele Ereignisse in einer Mail zusammengefasst werden. Dies bestimmt somit, wie viele Mails nach Ablauf eines Aggregations-Intervalls auf einmal verschickt werden. Gleichzeitig wird dadurch die maximale Größe der E-Mail begrenzt. ⓘ Beachten Sie ggfs. vorhandene Spam-Richtlinien des Empfängers.
Mails nicht senden, die keine Benachrichtigungen enthalten	Mit dieser Option können Sie verhindern, dass Benachrichtigungs-Mails gesendet werden, die keine bzw. keine neuen Benachrichtigungen enthalten.

Im Bereich **Sofort-Benachrichtigungen** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Max. Anzahl Mails pro Stunde	Wenn ein Ereignis auftritt, für das als Benachrichtigungstyp **Sofort** eingestellt wurde, dann wird sofort eine Mail an die Empfänger verschickt. Abhängig von den Einstellungen im Benachrichtigungstypen-Bereich und den auftretenden Ereignissen könnten viele Mails in kurzer Zeit verschickt werden, die dazu führen, dass diese Mails wegen Nicht-Einhaltung von Richtlinien der Provider auf Empfängerseite blockiert werden. Um dieses zu vermeiden, können Sie hier die maximale Anzahl der verschickten Sofort-Benachrichtigungen pro Stunde begrenzen. ⓘ Alle Sofort-Benachrichtigungen werden auch in der nächsten aggregierten E-Mail verschickt.

Im Bereich **Benachrichtigungstypen** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Filtern	Die angezeigten Benachrichtigungsfelder können nach Name und gesetztem Wert gefiltert werden.
Für alle ausgewählten Benachrichtigungen setzen	Alle momentan angezeigten Felder für Benachrichtigungen werden auf den hier eingestellen Wert gesetzt. Um z.B. alle Felder für IPsec auf den **Sofort** einzustellen, geben Sie bei **Filtern** „ipsec“ ein und können dann hier alle IPsec betreffenden Benachrichtigungsfelder auf **Sofort** einstellen.
Erwarteter System-Neustart	Benachrichtigung, wenn das System erwartet neu gestartet wird.
Unerwarteter System-Neustart	Benachrichtigung, wenn das System unerwartet neu gestartet wird.
HA-Rollenwechsel	Benachrichtigung, wenn ein Rollenwechsel in der Hochverfügbarkeit durchgeführt wird.
Internet-Verbindung offline	Benachrichtigung, wenn eine Internet-Verbindung getrennt wird.
Backup-Internet-Verbindung aktiviert	Benachrichtigung, wenn die Standard-Internet-Verbindung durch die Backup-Verbindung ersetzt wird.
Internet-Verbindung online	Benachrichtigung, wenn eine Verbindung zum Internet hergestellt wird.
Standard-Internet-Verbindung reaktiviert	Benachrichtigung, wenn wieder die Standard-Internet-Verbindung genutzt wird.
IPsec Site-to-Site-Verbindung online	Benachrichtigung, wenn eine IPsec Site-to-Site-Verbindung hergestellt wird.
IPsec Site-to-Site-Verbindung offline	Benachrichtigung, wenn eine IPsec Site-to-Site-Verbindung getrennt wird.

Wenn Sie Änderungen vorgenommen haben, können Sie diese mit den Schaltflächen unten rechts im Bearbeitungsfenster speichern (**Speichern**) oder verwerfen (**Zurücksetzen**). Andernfalls können Sie das Fenster schließen (**Schließen**).

3.4.2.3 BGP-Status

Im Fenster **BGP-Status** können Sie den BGP-Status in drei Tabellen einsehen.

Navigieren Sie zu **Monitoring & Statistiken** > **BGP-Status**, um ein Fenster zu öffnen, in dem diese Tabellen angezeigt werden.

Die obere „Nachbarn"-Tabelle beinhaltet Information über die auf der Firewall konfigurierten Nachbarn:

Spalte	Beschreibung
Status	Status der BGP Session, kann die folgenden Werte annehmen: › established: BGP kann mit dem Peer kommunizieren, Status grün › connect: BGP wartet bis die TCP-Verbindung aufgebaut werden kann, Status orange › active: BGP wartet auf einen Verbindungsversuch von dem Peer, Status orange › opensent: BGP wartet auf eine OPEN-Nachricht vom Peer, Status orange › openconfirm: BGP wartet auf KEEPALIVE oder NOTIFICATION-Nachrichten, Status orange › idle: Im Zustand idle versucht der Router derzeit nicht, eine BGP-Sitzung aufzubauen. Gründe dafür können sein, dass es keine Route zum Nachbarn gibt, oder der Nachbar einen früheren Verbindungsversuch abgelehnt hat, Status rot
Nachbar-IP	Zeigt die Nachbar-IP an.
Remote-AS	Zeigt die AS des Nachbarn an.
Akzeptierte Präfixe	Zeigt die Anzahl der akzeptierten Präfixe an.
Gesendete Präfixe	Zeigt die Anzahl der gesendeten Präfixe an.
Uptime	Zeigt die Laufzeit der BGP-Session an.
Verbindungen abgebrochen	Zeigt die Anzahl der abgebrochenen Verbindungen an.
Verbindungen hergestellt	Zeigt die Anzahl der hergestellten Verbindungen an.
OPENs gesendet: Anzahl	Zeigt die Anzahl der gesendeten Eröffnungen an.
OPENs empfangen: Anzahl	Zeigt die Anzahl der empfangenen Eröffnungen an.
Letztes Update	Zeigt den Zeitstempel des letzten Updates an.

Die unteren beiden Tabellen werden angezeigt, wenn auf eine Zeile in der Nachbar-Tabelle geklickt wird. Die Tabellen zeigen die von dem Nachbarn empfangenen oder an den Nachbarn gesendeten Routen an.

Tabelle 2: Empfangene Routen

Spalte	Beschreibung
Netzwerk	Das Netzwerk des ausgewählten BGP-Nachbarn für empfangene Routen.
Pfad	Die Nachbar-AS des ausgewählten BGP-Nachbarn für empfangene Routen.
Next Hop	Die nächste IP-Adresse des ausgewählten BGP-Nachbarn für gesendete Routen.

Tabelle 3: Gesendete Routen

Spalte	Beschreibung
Netzwerk	Das Netzwerk des ausgewählten BGP-Nachbarn für gesendete Routen.
Pfad	Die Nachbar-AS des ausgewählten BGP-Nachbarn für gesendete Routen.
Next Hop	Die nächste IP-Adresse des ausgewählten BGP-Nachbarn für gesendete Routen.

Klicken Sie auf **Neu laden**, um die Liste der BGP-Verbindungen in der Tabelle neu zu laden.

Mit der Schaltfläche **Schließen** unten im Bearbeitungsfenster können Sie das Fenster schließen.

3.4.2.4 Connection Tracking

Im Bearbeitungsfenster **Connection Tracking** können Sie das In-Kernel Connection Tracking System einsehen und bearbeiten, um eine Liste aller auf Ihrer LANCOM R&S®Unified Firewall aktiven Verbindungen anzuzeigen.

Navigieren Sie zu **Monitoring & Statistiken** > **Connection Tracking**, um ein Bearbeitungsfenster zu öffnen, in dem eine Liste aller im System verfolgten Verbindungen angezeigt wird.

Mithilfe von Filteroptionen können Sie die Ergebnisse in der unteren Tabelle eingrenzen. Wählen Sie zunächst eine Option aus der Drop-down-Liste aus oder tippen Sie in das Eingabefeld. Klicken Sie dann auf **Neu laden**, um nur diejenigen Einträge anzuzeigen, die die eingegebene Option oder die eingegebenen Zeichen enthalten. Klicken Sie auf ✖ in der Drop-down-Liste oder ⊗ im Eingabefeld, um die ausgewählte Option oder die Sucheingabe zu löschen oder klicken Sie auf **Filter zurücksetzen**, um alle Eingaben zu löschen und zur ungefilterten Listenansicht zurückzukehren.

Die Filteroptionen sind `AND`-verbunden.

Die Tabellenspalten der Liste der derzeit aktiven Verbindungen enthalten die folgenden Informationen:

Spalte	Beschreibung
#	Zeigt die Folgenummer der Tabellenzeile an.
Protokoll	Zeigt den IP-Protokolltypen an, der für die Verbindung genutzt wird. Der Typ kann entweder `TCP` oder `UDP` sein.
TTL	Zeigt die Lebensdauer des Conntrack-Eintrags in Sekunden. Sobald dieser Zeitraum abgelaufen ist, wird der Eintrag verworfen.
TCP-Status	Zeigt den aktuellen Status der TCP-Verbindung an. Der TCP-Status kann einer der Folgenden sein: › `SYN_SENT` › `SYN_RECV` › `ESTABLISHED` › `FIN_WAIT` › `CLOSE_WAIT` › `LAST_ACK` › `TIME_WAIT` › `CLOSE` › `LISTEN`
Quelle	Zeigt die Quell-IP-Adresse und den Quell-Port der Verbindungsanfrage an.
Ziel	Zeigt die Ziel-IP-Adresse und den Ziel-Port der Verbindungsanfrage an.
Pakete	Zeigt die Anzahl der Pakete an, die in die Ursprungsrichtung der angegebenen Verbindung gesendet wurden. Ursprungsrichtung bedeutet hier von der Quelle zum Ziel.
Bytes	Zeigt an die Anzahl der Bytes an, die in die Ursprungsrichtung der angegebenen Verbindung gesendet wurden. Ursprungsrichtung bedeutet hier von der Quelle zum Ziel.

Spalte	Beschreibung
Status	Zeigt den Status der Verbindung in der Ursprungsrichtung an. Ursprungsrichtung bedeutet hier von der Quelle zum Ziel. Der Status kann einer der folgenden sein: › ASSURED › ESTABLISHED – Die Verbindung wurde hergestellt. › EXPECTED – Es handelt sich um eine erwartete Verbindung. Dies bedeutet, dass noch keine übereinstimmenden Pakete empfangen wurden, die Firewall solche Pakete aber in Kürze erwartet. › FIXED_TIMEOUT › INVALID – Die Verbindung verhält sich nicht entsprechend dem erwarteten Verhalten einer Verbindung und wird daher als ungültig betrachtet. › NEW – Die Verbindung startet gerade. › RELATED – Die Verbindung wurde bereits erwartet. › SEEN_REPLY – Das erste Antwortpaket vom Ziel wurde empfangen, der Handshake wurde jedoch noch nicht abgeschlossen. › UNREPLIED – Ein erstes Paket von der Quelle wurde empfangen, aber noch nicht beantwortet. › UNSET › UNTRACKED – Die Verbindung wird nicht verfolgt.
Status (Antwort)	Zeigt den Status der Verbindung in Antwortrichtung. Antwortrichtung bedeutet hier vom Ziel zur Quelle. Der Status kann einer der folgenden sein: › ASSURED › ESTABLISHED – Die Verbindung wurde hergestellt. › EXPECTED – Es handelt sich um eine erwartete Verbindung. Dies bedeutet, dass noch keine übereinstimmenden Pakete empfangen wurden, die Firewall solche Pakete aber in Kürze erwartet. › FIXED_TIMEOUT › INVALID – Die Verbindung verhält sich nicht entsprechend dem erwarteten Verhalten einer Verbindung und wird daher als ungültig betrachtet. › NEW – Die Verbindung startet gerade. › RELATED – Die Verbindung wurde bereits erwartet. › SEEN_REPLY – Das erste Antwortpaket von der Quelle wurde empfangen, der Handshake wurde jedoch noch nicht abgeschlossen. › UNREPLIED – Ein erstes Paket von der Quelle wurde empfangen, aber noch nicht beantwortet. › UNSET › UNTRACKED – Die Verbindung wird nicht verfolgt.
Quelle (Antwort)	Zeigt die Quell-IP-Adresse und den für die Antwortpakete erwarteten Port an (üblicherweise identisch mit dem unter **Ziel**).
Ziel (Antwort)	Zeigt die Ziel-IP-Adresse und den für die Antwortpakete erwarteten Port an (üblicherweise identisch mit dem unter **Quelle**).

Spalte	Beschreibung
Pakete (Antwort)	Zeigt die Anzahl der Pakete an, die in die Antwortrichtung der angegebenen Verbindung gesendet wurden. Antwortrichtung bedeutet hier vom Ziel zur Quelle.
Bytes (Antwort)	Zeigt die Anzahl der Bytes an, die in die Antwortrichtung der angegebenen Verbindung gesendet wurden. Antwortrichtung bedeutet hier vom Ziel zur Quelle.
Markieren	Zeigt das Zeichen der Verbindung an. Das Zeichen wird durch Ihre LANCOM R&S®Unified Firewall gesetzt.
Verwendet	Zeigt das Conntrack- `Use` -Feld an.

Klicken Sie auf **Neu laden**, um die Liste der Verbindungen in der Tabelle neu zu laden.

Mit der Schaltfläche **Schließen** unten im Bearbeitungsfenster können Sie das Fenster schließen und zur kompletten Übersicht Ihres gesamten konfigurierten Netzwerks zurückkehren.

3.4.2.5 Management-Bericht

Navigieren Sie zu **Monitoring & Statistiken** > **Management-Bericht**, um einen Bericht über die aktuelle Desktopkonfiguration und einige Statistiken zu erstellen und diesen auf Ihren Computer zu übertragen. Alternativ können Sie diesen auch per E-Mail versenden.

3.4.2.5.1 Aktueller Bericht

Navigieren Sie zu **Monitoring & Statistiken** > **Management-Bericht** > **Aktueller Bericht**, um einen Bericht über die aktuelle Desktopkonfiguration und einige Statistiken zu erstellen und diesen auf Ihren Computer zu übertragen.

Im Fenster **Management-Bericht** können Sie zwischen den Dateiformaten PDF, HTML und CSV wählen, indem Sie die entsprechende Optionsschaltfläche auswählen. Bei dem Format CSV werden die Tabellen als einzelne `csv`-Dateien

erstellt und zusammengepackt als ZIP-Datei zum Speichern angeboten. So wird eine eventuelle Weiterverarbeitung der Daten vereinfacht.

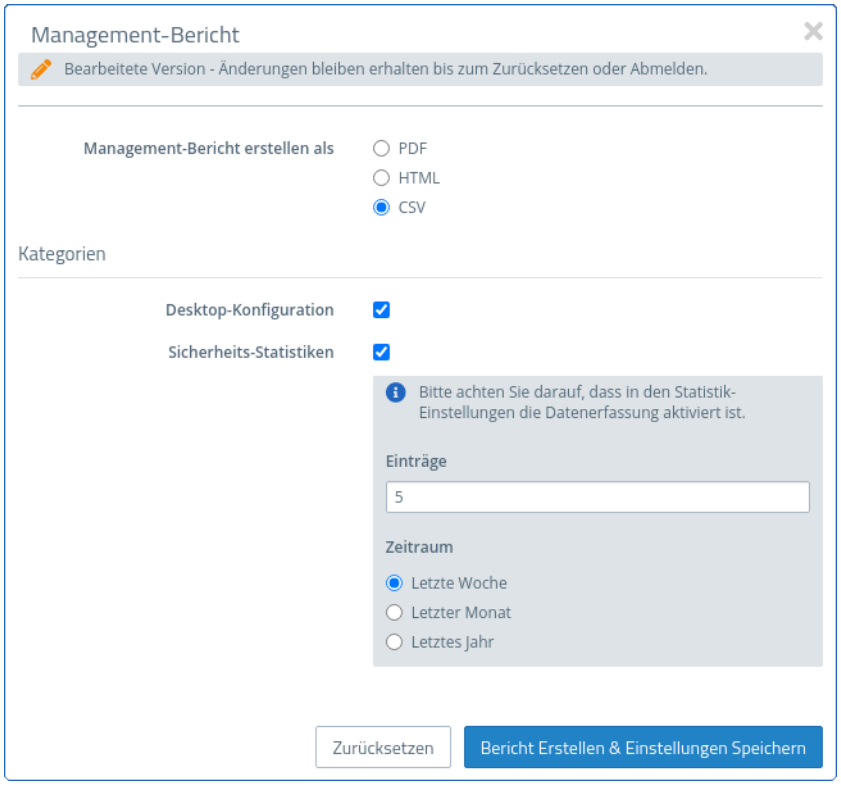


Abbildung 19: Management-Bericht – Einstellungen für den Bericht

Im Bereich **Kategorien** können Sie die folgenden Elemente konfigurieren:

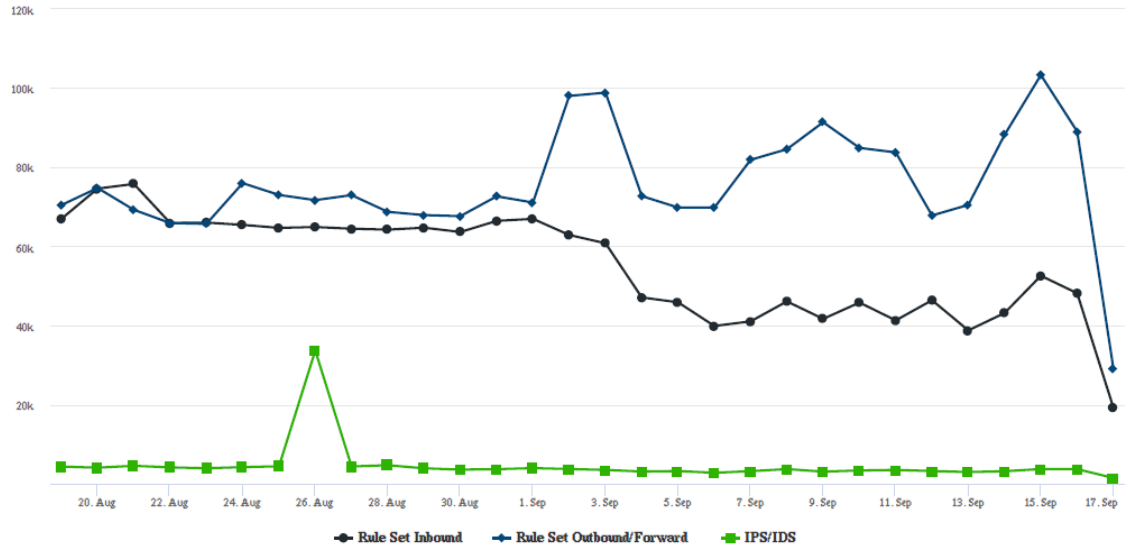
Eingabefeld	Beschreibung
Desktop-Konfiguration	Die Exportdatei enthält eine Tabelle mit allen konfigurierten Firewall-Regeln, inklusive zusätzlicher Informationen wie NAT, DMZ, IP-Adressen der Hostobjekte und dem Inhalt der Beschreibungsfelder der konfigurierten Desktop-Objekte und -Verbindungen. Desktop-Objekte werden nur mit eingeschlossen, wenn sie mit anderen Desktop-Objekten verknüpft sind.
Sicherheits-Statistiken	Voraussetzung für die Erzeugung von Statistiken ist, dass unter **Monitoring & Statistiken** > **Einstellungen** mindestens der Wert „Statistiken führen“ für die Ereignis-Typen eingestellt wurde. Beinhaltet die Statistiken, die auch unter dem Menüpunkt **Monitoring & Statistiken** > **Statistiken** > **Übersicht** verfügbar sind, sowohl als Graph als auch als Tabelle: › Blockierte Verbindungen › Blockierter Inhalt › Top aufgerufene Domains › Top blockierte Domains › Top Traffic pro Quelle Wenn Sicherheits-Statistiken aktiviert sind, können weitere Einstellungen vorgenommen werden: › Anzahl der Einträge (diese Einstellung gilt nur für die Toplisten)

Eingabefeld	Beschreibung
	› Zeitraum, Festlegung des zu erfassenden Zeitraums beginnend mit dem aktuellen Zeitpunkt

Klicken Sie auf **Bericht erstellen**, wenn Sie die Exportdatei erstellen und übertragen möchten. Ihre Einstellungen werden gesichert und ein Dateiname mit einem Datumspräfix (YYYY-MM-DD_HH-mm) vorgeschlagen. Klicken Sie ansonsten auf **Zurücksetzen**, um die Einstellungen auf die zuletzt gespeicherten Einstellungen zurück zu setzen.

LANCOM Systems ROHDE&SCHWARZ

Blocked Connections



Date	Rule Set Inbound	Rule Set Outbound/Forward	IPS/IDS
17. Sep	19272	29097	1559
16. Sep	48169	88978	3784
15. Sep	52570	103212	3815
14. Sep	43177	88127	3261
13. Sep	38790	70447	3052

Abbildung 20: Beispiel aus einem Management-Bericht

LANCOM Systems ROHDE&SCHWARZ

Source	Action	NAT	Destination	Service	Rule Settings	Connection Settings
eth2 LAN Connection 10.10.21.0/24	➡	➡	**WAN** eth0 WAN Connection	**IMAP4** 143 TCP	Proxy: IMAP4	**Webfilter:** Sex: Content Filter Kriminelles: Content Filter Werbung: Content Filter
	➡	➡		**POP3s** 995 TCP	Proxy: POP3S	
	➡	➡		**SMTP** 25 TCP	Proxy: SMTP	
	➡	➡		**IMAP4s** 993 TCP	Proxy: IMAP4S	
	➡	➡		**POP3** 110 TCP	Proxy: POP3	
	➡	➡		**SMTPs** 465 TCP	Proxy: SMTPS	
	➡	➡		**HTTPS** 443 TCP	Proxy: HTTPS	
	➡	➡		**HTTP** 80 TCP	Proxy: HTTP	
eth1 LAN Connection 10.10.20.0/24	➡	➡	**WAN** eth0 WAN Connection	**HTTPS** 443 TCP	Proxy: HTTPS	**Webfilter:** Sex: Content Filter Kriminelles: Content Filter Werbung: Content Filter
	➡	➡		**HTTP** 80 TCP	Proxy: HTTP	

Abbildung 21: Beispiel aus einem Management-Bericht

3.4.2.5.2 Mail-Bericht

Navigieren Sie zu **Monitoring & Statistiken** > **Management-Bericht** > **Mail-Bericht**, um einen regelmäßigen Bericht über die aktuelle Desktopkonfiguration und einige Statistiken zu erstellen und diesen per E-Mail zu versenden. Anders als im **Aktuellen Bericht** beinhaltet der **Mail-Bericht** immer sowohl die Desktop-Konfiguration als auch die Statistiken.

Der Mail-Bericht nutzt das Firewall-interne Mail-System. Deshalb müssen unter **Firewall** > **E-Mail-Einstellungen** die Basis-Einstellungen konfiguriert sein, damit E-Mails versendet werden können.

Eingabefeld	Beschreibung
I/**0**	Ein Schiebeschalter gibt an, ob das Versenden eines regelmäßig erzeugten Reports derzeit aktiv (**I**), oder inaktiv (**0**) ist. Mit einem Klick auf den Schiebeschalter können Sie den Status ändern.
Bericht anhängen als	Wählen Sie aus den möglichen Formaten PDF, HTML oder CSV eines aus.
Intervall	Geben Sie an, ob der Report wöchentlich oder monatlich versendet werden soll.
Start-Zeit	Geben Sie den Zeitpunkt für das erstmalige Versenden des Reports an.
Mail-Betreff	Geben Sie einen eigenen Betreff für die Report-E-Mail an.
Empfänger	Geben Sie in dieser Liste alle E-Mail-Adressen an, die den Report erhalten sollen.

Die Schaltflächen rechts unten im Bearbeitungsfeld hängen davon ab, ob Sie Änderungen vorgenommen haben. Um die Änderungen zu übernehmen, klicken Sie auf **Speichern**, um die Änderungen zu speichern, oder auf **Zurücksetzen**, um Ihre Änderungen zu verwerfen. Sie können auf **Schließen** klicken, um das Bearbeitungsfenster zu schließen, solange keine Änderungen darin vorgenommen wurden.

3.4.2.6 Hardware-Monitoring

Im Bearbeitungsfenster **Hardware-Monitoring** können Sie den aktuellen Zustand Ihrer LANCOM R&S®Unified Firewall anzeigen. Es werden Daten zu den folgenden Bereichen angezeigt:

- System-Informationen
- CPU-Auslastung
- Prozess-Liste
- Netzwerk-Auslastung

Benutzer müssen über die Berechtigung „Monitoring (Lesen/Öffnen)“ verfügen, um diese Daten anzeigen zu dürfen.

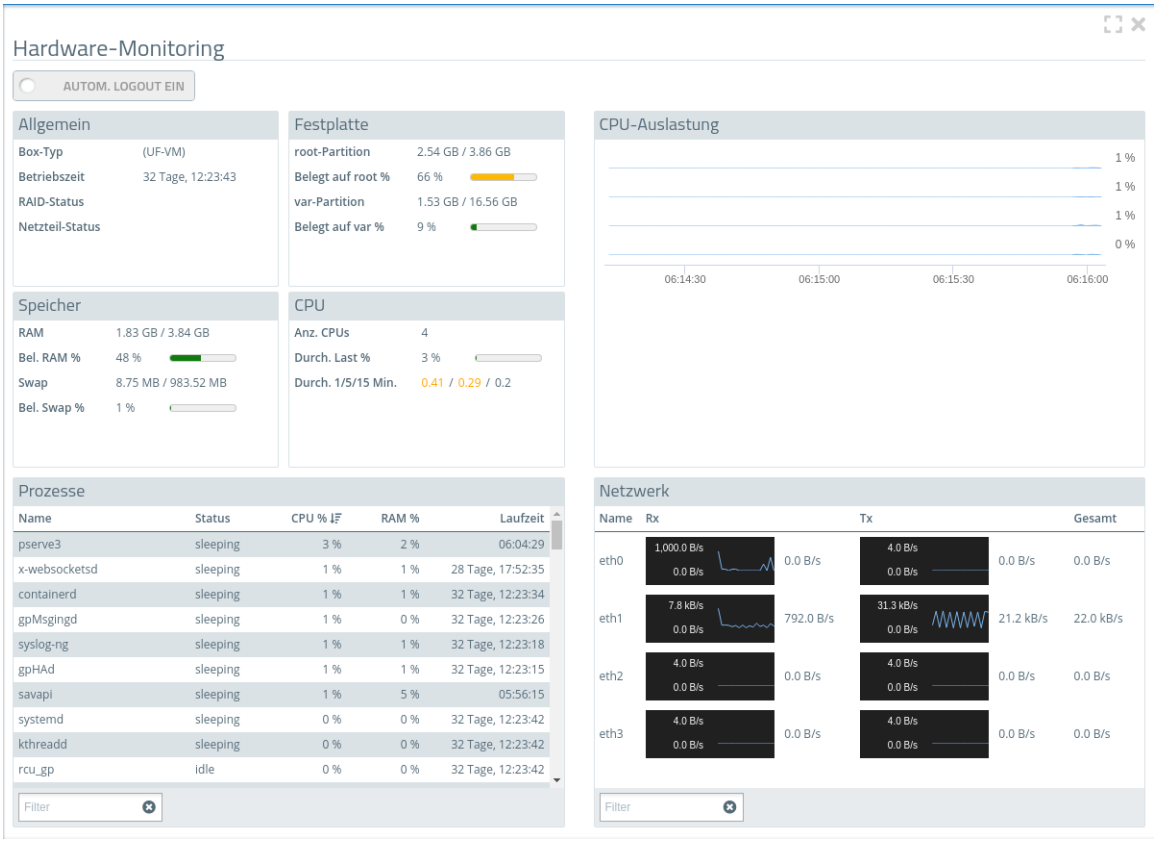


Abbildung 22: Monitoring & Statistiken > Hardware-Monitoring

Eingabefeld	Beschreibung
Automatischer Logout Ein / Aus	Über diesen Schalter können Sie die automatische Abmeldung des Web-Clients ein- bzw. ausschalten. Dadurch lassen sich die Monitordaten über einen längeren Zeitraum verfolgen. Dies schaltet eine Sicherheitsfunktion des Web-Clients ab. Nutzen Sie daher in diesem Fall ein von Ihnen anzulegendes Benutzerkonto, welches ausschließlich über die Berechtigung „Monitoring (Lesen/Öffnen)“ verfügt.
	Zeigen Sie den Monitoring-Dialog im Vollbild an.

3.4.2.6.1 System-Informationen

Die System-Informationen werden im oberen linken Bereich angezeigt. Es werden Informationen zu den folgenden Themen angezeigt:

- **Allgemein**: Informationen über den Firewall-Box-Typ, die Betriebszeit der Firewall, den RAID-Status (wenn vorhanden) und den Netzteil-Status (wenn vorhanden).
- **Festplatte**: Belegung der root- und var-Partionen, jeweils in absoluten und prozentualen Werten.
- **Speicher**: Belegung des Arbeitsspeichers und des Swap, jeweils in absoluten und prozentualen Werten.
- **CPU**: Anzahl der vorhandenen logischen CPUs, durchschnittliche Auslastung aller CPUs in Prozent und die durchschnittliche CPU-Auslastung der letzten 1, 5 und 15 Minuten. Die angezeigte Auslastung kann auch über 1

liegen. In diesem Fall werden mehr als ein CPU-Kern ausgelastet. Solange der Wert unter der Anzahl der CPUs liegt, ist das System nicht voll ausgelastet. Werte über der Anzahl der verfügbaren CPUs werden in Rot angezeigt.

Die durchschnittliche CPU-Auslastung der letzten 1 bzw. 5 Minuten wird jeweils gelb angezeigt, wenn:

- 1 Min-Wert: Die durchschnittliche CPU-Auslastung der letzten Minute liegt über dem Auslastungsdurchschnitt der letzten 5 oder 15 Minuten.
- 5 Min-Wert: Die durchschnittliche CPU-Auslastung der letzten 5 Minuten liegt über dem Auslastungsdurchschnitt der letzten 15 Minuten.

3.4.2.6.2 CPU-Auslastung

Die CPU-Auslastung wird im oberen rechten Bereich angezeigt. Hier wird die Auslastung der einzelnen CPUs über einen Zeitraum von bis zu 5 Minuten angezeigt (bei mehr als 10 CPUs werden zwei Spalten angezeigt, bei mehr als 20 CPUs maximal 3 Spalten).

Wenn der Durchschnitt der letzten 10 Werte der Auslastung einer CPU über 50% liegt, wechselt die Farbe des Diagramms für diese CPU zu orange. Liegt der Durchschnitt der letzten 10 Werte über 75%, wechselt die Farbe des Diagramms zu rot.

3.4.2.6.3 Prozesse

Die Prozesse werden im unteren linken Bereich angezeigt. Zu allen Prozessen werden jeweils die folgenden Informationen angezeigt:

- **Name**
- **Status**
- **CPU-Verwendung in Prozent**
- **RAM-Verwendung in Prozent**
- **Laufzeit des Prozesses**

Alle Spalten können auf- oder absteigend sortiert werden.

Zusätzlich kann die Tabelle nach Prozessnamen gefiltert werden. Der Filter unterstützt auch nur den Teil eines Namens.

Die Liste der verfügbaren Prozesse in dem Filter wird nur einmal beim Öffnen des Hardware-Monitorings geladen, somit werden neu startende Prozesse nicht aufgeführt.

3.4.2.6.4 Netzwerk

Die Netzwerkauslastung wird im unteren rechten Bereich angezeigt. Es wird die aktuelle Auslastung aller verfügbaren Ethernet-Ports mit jeweils den folgenden Informationen angezeigt:

- **Name**
- **Rx**: Empfangene Bytes
- **Tx**: Gesendete Bytes
- **Gesamt**: Rx + Tx

Über den Filter können einzelne Ethernet-Ports über den Namen gefiltert werden.

3.4.2.7 LLDP

Navigieren Sie zu **Monitoring & Statistiken** > **LLDP**, um ein Fenster zu öffnen, in dem die Informationen zum Link Layer Discovery Protocol (LLDP) eingesehen werden können, die empfangen wurden.

Spalte	Beschreibung
Port-ID (Lokal)	Lokales Interface der Firewall, auf dem die LLDP-Nachricht empfangen wurde.
Chassis-ID	Die MAC-Adresse des Nachbar-Geräts.

Spalte	Beschreibung
System-Beschreibung	Eine Beschreibung des Geräts, z. B. Betriebssystem, Version, etc.
System-Fähigkeiten	Eine Auflistung von Fähigkeiten, über die das Nachbar-Gerät verfügt.
Port-ID (Remote)	Remote-Interface des Nachbarn, von dem aus die LLDP-Nachricht gesendet wurde.
Port-Beschreibung	Beschreibung des Remote Nachbar-Ports.
Management-Adresse	Adresse, unter der weitere Informationen über den Nachbarn zu finden sind.
TTL	Time To Live, Dauer der Gültigkeit der Nachbar-Informationen in Sekunden.

Alle Spalten können auf Basis einer der Spalten auf- oder absteigend sortiert werden.

3.4.2.8 Protokolle

Ihre LANCOM R&S®Unified Firewall bewahrt Aufzeichnungen über Systemereignisse, Statusinformationen, Fehler und andere Kommunikation in einer Protokolldatenbank auf. Navigieren Sie zu **Monitoring & Statistiken** > **Protokolle**, um die Ereignisprotokolle einzusehen. Die Fenster zeigen die Inhalte jedes Ereignisprotokolls an. Falls ein Problem auftritt, können Sie in diesen Protokollen ggf. technische Details zur Ursache des Problems finden.

Die Ereignisprotokolle werden automatisch aktualisiert, um die neusten Einträge anzuzeigen. Sie können die automatische Aktualisierung deaktivieren, um den Schwerpunkt auf ältere Einträge zu legen, indem Sie auf den Schiebeschalter **AUTOM. LADEN EIN** klicken. Klicken Sie auf **Manuell neu laden**, um die Objektliste manuell zu aktualisieren. Um wieder auf die automatische Aktualisierung umzuschalten, klicken Sie auf den Schiebeschalter, der diese aktiviert.

Mit den Filteroptionen über den Tabellen können Sie die Ergebnisse eingrenzen, um nur Einträge anzuzeigen, die einen bestimmten Suchbegriff enthalten. Variieren Sie die Optionen, um Suchkriterien in den Eingabefeldern einzustellen. Die Filter **Meldung** und **Benutzer** geben alle Ergebnisse aus, die die Sucheingabe enthalten. Alle übrigen Filterfelder geben nur exakte Übereinstimmungen aus. Die verfügbaren Optionen hängen vom Typ des Ereignisprotokolls ab. Wenn Filteroptionen eingestellt wurden, werden die Ereignisprotokolle immer automatisch aktualisiert.

Klicken Sie auf das Eingabefeld **Zeit**, um den Inhalt eines Protokolls nach einer benutzerdefinierten Zeitspanne zu filtern. Es öffnet sich ein neues Fenster, in dem Sie entweder einen voreingestellten Zeitraum wählen oder einen eigenen eingeben können. Wenn Sie auf **Benutzerdefiniert** klicken, erscheinen ein Kalender und Drop-down-Listen, mit denen Sie Datum und Uhrzeit ändern können. Legen Sie die gewünschten Daten und Uhrzeiten fest. Klicken Sie auf **Anwenden**, um Ihre Änderungen zu speichern und das gefilterte Ereignisprotokoll anzuzeigen, oder auf **Abbrechen**, um Ihre Änderungen zu verwerfen.

Um zum vollständigen Protokoll zurückzukehren, entfernen Sie alle Suchkriterien, indem Sie entweder auf **Zurücksetzen**, die Schaltfläche ✖ rechts neben einem ausgewählten Eintrag in der Drop-down-Liste oder die Schaltfläche ⊗ in den Eingabefeldern klicken.

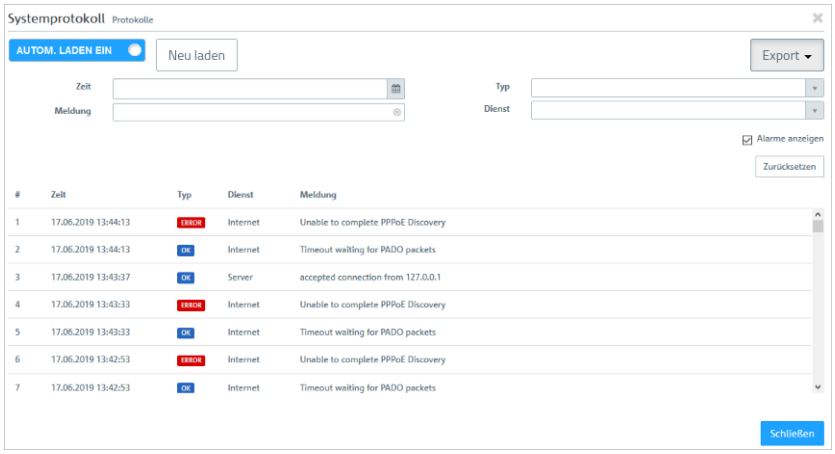


Abbildung 23: Beispiel eines gefilterten Systemprotokolls

Mit der Schaltfläche **Schließen** unten in den Protokollfeldern können Sie die Protokollfelder schließen und zur kompletten Übersicht Ihres gesamten konfigurierten Netzwerks zurückkehren.

In den folgenden Abschnitten finden Sie weiterführende Informationen zu lokalen Ereignisprotokollen.

3.4.2.8.1 Alarmprotokoll

Navigieren Sie zu **Monitoring & Statistiken** > **Protokolle** > **Alarmprotokoll**, um die Ereignisprotokolle zu Alarmen einzusehen und Filter zur Anzeige einzurichten. Im Bearbeitungsfenster **Alarmprotokoll** können Sie einsehen, welcher Traffic durch Ihre LANCOM R&S®Unified Firewall blockiert, oder in welcher Form Traffic durch die Firewall übertragen wurde.

Die Tabellenspalten enthalten die folgenden Informationen:

Tabelle 4: Filtertypen

Spalte	Beschreibung
Zeit	Zeitstempel des Protokolleintrags.
Kategorie	Ereigniskategorie, die eine der folgenden sein kann: › `Application-Filter` › `Connection Blocked` › `Connection Finished` › `IDPS` › `Mail Malware` › `Spam` › `Web Filter Allowed` › `Web Filter Blocked` › `Web Malware`
Meldung	Die Protokollmeldung selbst. Ggfs. lassen sich über das ⚙ auf der rechten Seite einer Meldung auch direkt Aktionen ausführen. So werden z. B. in der Kategorie `IDPS` Meldungen zu blockierten Diensten angezeigt. In dieser Meldung wäre dann auch die

Spalte	Beschreibung
	Signatur-ID enthalten, die man bei einer Regel angeben müsste, um diesen Dienst nicht mehr zu blockieren. Diese Ausnahme lässt sich somit aus dem Protokoll direkt hinzufügen.

Filterfunktion

Sie können das Alarmprotokoll mithilfe der Filterfunktion im Eingabefeld **Weitere Filter** um verschiedene Suchkriterien und -optionen eingrenzen. Diese Filter beziehen sich auf das Zeitintervall, das Sie unter **Zeit** eingestellt haben.

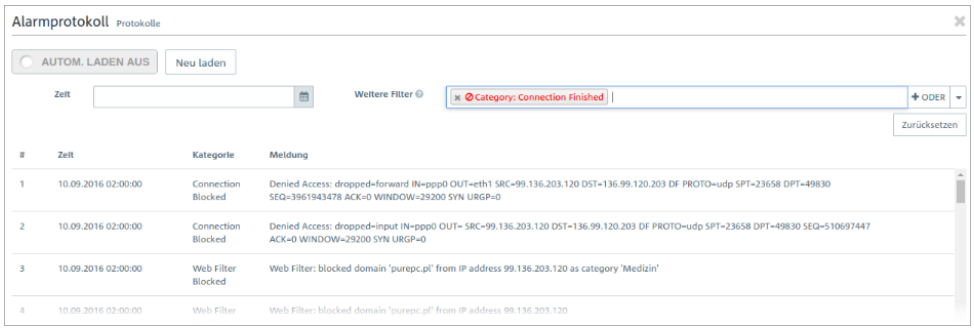


Abbildung 24: Alarmprotokoll mit angewandtem Filter

Um einen Filter zu erstellen, gehen Sie wie folgt vor:

1. Klicken Sie in das Eingabefeld.

   Der Webclient zeigt Filtervorschläge an.

   Mögliche Filtertypen, Eingabeformate und Vorgabewerte entnehmen Sie der Tabelle *Filtertypen*.

2. Wählen Sie einen der vorgeschlagenen Filter aus der Drop-down-Liste aus oder geben Sie einen beliebigen Suchtext ein, um weitere Vorschläge zu erhalten.

   Für jeden Vorschlag können Sie auswählen, ob dieser als Inklusionsfilter (✚ / UND-Verknüpfung) oder Exklusionsfilter (⊘ / UND-NICHT-Verknüpfung) verwendet werden soll.

   Nach der Auswahl wird der Filtervorschlag als Suchkriterium in das Eingabefeld eingefügt.

   Die Liste der Protokollmeldungen passt sich an die Suchabfrage an. Gefundene Übereinstimmungen werden in den Protokolleinträgen hervorgehoben.

Wiederholen Sie die obigen Schritte, bis Sie die gewünschten Filterkriterien zu Ihrer Suchanfrage hinzugefügt haben.

Es werden nur Einträge angezeigt, die mit allen Filterkriterien übereinstimmen.

Um ein Filterkriterium in einer Suchabfrage zu löschen, klicken Sie auf ✖.

Sie können mehrere Zeilen zu Ihrer Suchanfrage hinzufügen, indem Sie neben dem Eingabefeld auf **+ ODER** klicken. Sie können wählen, ob Sie eine neue leere Zeile einfügen, oder die zuletzt angelegte Zeile kopieren möchten. Jede Zeile ist in sich eine eigene Suchabfrage, die mit den anderen Zeilen ODER-verknüpft wird.

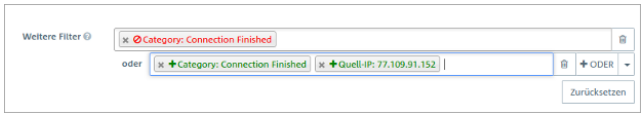


Abbildung 25: Kombinierte Filterabfrage

Löschen Sie die Zeile, indem Sie neben der Zeile auf 🗑 klicken.

Filtertypen

Filtertyp	Eingabeformat	Vorgabewerte	Unterarten
Text	Freitext		Meldung (Logeintrag) Domain / URI (Logeinträge von HTTP Proxys, Virenscanner und dem URL- / Contentfilter)
Protokoll	Freitext	ICMP, TCP, UDP Transportprotokolle oder Protokolle, die durch den Application Filter erfasst wurden	
Port	Zahlen von 0 bis 65535		TCP- / UDP-Quell- oder Zielport von IPDS- oder Firewallmeldungen
IPv4	Gültige IP-Adresse oder Teile davon		Quell- oder Ziel-IP-Adresse von Mail-Proxy-, IDPS-, Application-Filter- oder Firewallmeldungen
Kategorie	Freitext oder Auswahl aus der **Weitere Filter** Drop-down-Liste	› `Application-Filter` › `Connection Blocked` › `Connection Finished` › `IDPS` › `Mail Malware` › `Spam` › `Web Filter Allowed` › `Web Filter Blocked` › `Web Malware`	

Export

Die Einträge des Protokolls können in den Formaten PDF, HTML und CSV exportiert werden. Der Export berücksichtigt hierbei die gegenwärtigen Filter-Einstellungen.

3.4.2.8.2 Auditprotokoll

Das **Audit Log** erstellt Aufzeichnungen über jede Konfigurationsänderung, die auf Ihrer LANCOM R&S®Unified Firewall durchgeführt wurde (z. B. Aktualisierung der VPN-Einstellungen), jede ausgeführte Aktion (z. B. Importieren eines Backups) und von wem diese jeweils ausgelöst wurde. Um das Protokoll anzuzeigen, werden Rechte auf **Monitoring** benötigt. Weitere Informationen zu den Webclient-Rechten finden Sie unter *Einstellungen zu Administratoren* auf Seite 34.

Im oberen Bereich können für die angezeigten Zeilen für die jeweiligen Tabellenspalten Filter eingestellt werden. Die Tabellenspalten enthalten die folgenden Informationen:

Spalte	Beschreibung
Zeit	Zeitstempel des Protokolleintrags
Aktion	Ereignisprotokoll-Stufe, die eine der folgenden sein kann: › `Call` – Ausführen einer bestimmten Aktion (z. B. Importieren eines Backups) › `Delete` – Löschen eines Konfigurationselements (z. B. Löschen einer ausgelaufenen IPsec-Verbindung)

Spalte	Beschreibung
	› `Insert` – Einfügen eines neuen Konfigurationselements (z. B. Einfügen einer Hostgruppe) › `Update` – Änderung eines Konfigurationselements (z. B. Anpassen der Antivirus-Einstellungen)
Benutzer	Name des Benutzers, der den Eintrag angelegt hat, z. B. `admin`.
Meldung	Die Protokollmeldung selbst. Der Inhalt der Meldung hängt vom gewählten **Aktion** Typ ab: › Wenn die **Aktion** `Call` ist, beginnt die **Meldung** mit dem aufgerufenen API-Endpunkt. › Wenn die **Aktion** `Delete` ist, gibt die **Meldung** den Namen und internen Typen des entfernten Konfigurationselements an. › Wenn die **Aktion** `Insert` ist, gibt die **Meldung** den Namen und internen Typen des angelegten Konfigurationselements an. Sie zeigt auch den kompletten Payload der Meldung an, die zur Erstellung des Konfigurationselements verwendet wurde und die genauen verwendeten Einstellungen enthält. › Wenn die **Aktion** `Update` ist, gibt die **Meldung** den Namen und internen Typen des geänderten Konfigurationselements an. Sie listet auch die genauen Änderungen, die an einem bestimmten Pfad vorgenommen wurden, in kursiver Schrift auf. Der Pfad identifiziert die tatsächliche Einstellung eines Konfigurationselements, das verändert wurde.

Export

Zur Vereinfachung der Verwendung von AddIns in der LANCOM Management Cloud kann das Auditprotokoll im passenden Format exportiert werden. Damit lassen sich schnell und einfach Konfigurationen von einer Unified Firewall auf beliebig viele von der LANCOM Management Cloud (LMC) gemanagte Unified Firewalls multiplizieren. Dabei kann zwischen zwei Optionen gewählt werden:

› **Für LMC-Import exportieren**: Eine json-Datei wird erzeugt, die später in der LANCOM Management Cloud über die entsprechende Import-Funktion hochgeladen werden kann.
› **Script in Zwischenablage kopieren**: Die AddIn-Funktion wird in die Zwischenablage kopiert und kann dann direkt eingefügt werden.

Darüber hinaus lassen sich die Einträge des Protokolls auch in den Formaten PDF, HTML und CSV exportieren.

Der Export berücksichtigt hierbei die gegenwärtigen Filter-Einstellungen.

Klicken Sie rechts in einer Zeile auf , um diesen Audit-Eintrag als LMC-Funktionsaufruf zu exportieren.

3.4.2.8.3 Systemprotokoll

Das **Systemprotokoll** zeigt eine Liste neuerer Systemmeldungen an.

Die Tabellenspalten enthalten die folgenden Informationen:

Spalte	Beschreibung
Zeit	Zeitstempel des Protokolleintrags
Typ	Meldungstyp, der einer der Folgenden sein kann: › `OK` – Der Dienst funktioniert korrekt › `Error` – Ein Fehler ist aufgetreten. Eine Fehlermeldung wird angezeigt.
Dienst	Name des Dienstes, der den Eintrag angelegt hat. Folgende Filter sind verfügbar: › `Server` – Firewall-Dienste, darunter Meldungen zu Kernel, DHCP-Server, DNS-Server und SNMP-Server

Spalte	Beschreibung
	› `VPN` – IPsec- und SSL-Tunnel › `Internet` – NTP, DynDNS und DSL-Verbindungsstatus › `User` – Terminal-Login, SSH-Login und Aktionen mit Superuser-Privilegien (sudo) › `Connections` – Verbindungen, die erfolgreich fertiggestellt wurden. Diese Meldungen werden nur gespeichert, wenn Verbindung fertiggestellt in der **Monitoring & Statistiken** > **Einstellungen** auf Rohdaten lokal speichern gestellt ist. › `Proxy` – Meldungen zu Web- und Mailproxies › `Updates` – alle Meldungen zur Firewall-Software › `Appfilter` – Meldungen zu Anwendungsfiltern › `IDPS` – IDS/IPS-Meldungen › `Alerts` – alle für die Sicherheit relevanten Meldungen, unabhängig vom Ursprungsgerät (wenn etwa das Anti-Virus-Modul einen Virus erkennt oder das IDS/IPS-Modul eine Bedrohung erkennt) Warnmeldungen werden nur in der Kategorie `Alerts` angezeigt, auch wenn sie zusätzlich einer anderen Kategorie angehören. **Beispiel:** `Appfilter` gibt eine Warnmeldung aus. Die Warnmeldung erscheint nur in `Alerts` und nicht in `Appfilter`.
Meldung	Die Protokollmeldung selbst. Wählen Sie `Alerts` in der Spalte **Dienst**, um IDS/IPS-Protokollmeldungen zu filtern. **Tipp:** Sie können die Protokollmeldungen verwenden, um eine IDS/IPS-Regel zur Liste der ignorierten Regeln im Tab **Regeln** des Bearbeitungsfensters **IDS/IPS** hinzuzufügen. Klicken Sie auf ⚙ in der jeweiligen IDS/IPS-Protokollmeldung. Eine Drop-down-Liste öffnet sich. Wählen Sie den Eintrag **Regel ignorieren**. Die IDS/IPS-Regel wird automatisch zur Liste der ignorierten Regeln im Tab **Regeln** des Bearbeitungsfensters **IDS/IPS** hinzugefügt. Weitere Informationen finden Sie unter *IDS / IPS* auf Seite 142.

Setzen Sie das Häkchen bei **Alarme anzeigen**, um zusätzlich zu den Protokollmeldungen Alarme unabhängig vom ausgewählten Dienst anzuzeigen.

Alarme können zusätzliche Informationen zu Ereignissen enthalten, um den Ursprung eines Fehlers identifizieren zu können.

Export

Die Einträge des Protokolls können in den Formaten PDF, HTML und CSV exportiert werden. Der Export berücksichtigt hierbei die gegenwärtigen Filter-Einstellungen.

3.4.2.8.4 Regeln aus dem Protokoll erstellen

Sie können Regeln für abwiesene Zugriffe direkt aus dem Alarm- und Systemprotokoll erstellen. Vorzugsweise sollte das Alarm-Protokoll (**Monitoring & Statistiken** > **Protokolle** > **Alarmprotokoll**) verwendet werden, da dort direkt nach abgewiesenen Zugriffen (Connection Blocked) gefiltert werden kann.

Für die Nutzung dieser Funktionalität muss die Firewall entsprechend konfiguriert werden:

1. Unter **Monitoring & Statistiken** > **Einstellungen** muss für **Blockierter weiterzuleitender Verkehr** der Wert **Rohdaten lokal speichern** ausgewählt werden, damit die Firewall über die notwendigen Daten verfügen kann.

2. Eine Internet-Verbindung muss definiert sein, falls der Datenverkehr nicht zwischen internen Netzwerken an unterschiedlichen Schnittstellen der Firewall erfolgt.

Sobald Datenverkehr blockiert wurde, sollten im Alarmprotokoll Einträge der Kategorie „Connection Blocked" erscheinen.

Auf der rechten Seite jedes dieser Einträge kann der Benutzer über das Aktionsmenü eine **Neue Regel erstellen**. Daraufhin erscheint ein neuer Dialog, in dem Sie (eingeschränkter im Vergleich zum Verbindungsdialog) eine Regel definieren können.

Bereich / Eingabefeld	Beschreibung
Protokoll-Informationen	Hier sind die Informationen des ausgewählten Eintrags aufgelistet. Beispiel: Von einem Host (192.168.3.3) aus dem internen Netz sollten über die Schnittstelle „eth3" per „ICMP" Daten an das Ziel 192.168.5.5 geschickt werden.
Dienst	Im "Dienst"-Abschnitt kann der Benutzer entscheiden, ob ein vorhandener vordefinierter oder benutzdefinierter Dienst verwendet oder ein neuer benutzerdefinierter Dienst erstellt werden soll. Es werden nur Dienste angezeigt, die im Port und Protokoll dem blockierten Zugriff entsprechen. Im vorliegenden Beispiel ist es ICMP mit (Port 0/Kein Port) und dem ICMP-Protokoll. Der neu zu erstellende Dienst würde dieselben Port- und Protokoll-Einstellungen beinhalten. Lediglich ein benutzerdefinierter Name kann eingegeben werden.
Quelle, **Aktion** und **Ziel**	Im unteren Bereich sind die fehlenden Daten zur Erstellung der Desktop-Verbindung einzugeben. Auch hier können Sie bei Quelle und Ziel auswählen, ob vorhandene Desktop-Objekte verwendet werden oder neue Desktop-Objekte erstellt werden sollen. Es kann auch ein neues mit einem vorhandenen Objekt verbunden werden. Die zur Verfügung stehenden vorhandenen Desktop-Objekte beinhalten alle Internet-Objekte und Desktop-Objekte, die in der IP-Adresse und dem Interface übereinstimmen. Dieses kann auch auf VPN-Desktop-Objekte zutreffen. Das standardmäßig ausgewählte vorhandene Desktop-Objekt ist das, welches am nächsten zum Interface und der IP-Adresse passt. In unserem Beispiel würde also ein Host-Objekt mit 192.168.3.3 und eth3 vorrangig gewählt gegenüber einem Netzwerk-Objekt mit 192.168.3.0/24. Falls kein anderes Desktop-Objekt vorausgewählt werden konnte, wird ein Internet-Objekt verwendet. Falls Sie ein neues Desktop-Objekt erstellen wollen, sind Sie auf ein Host- oder Netzwerk-Objekt beschränkt , um das Erstellen einer Regel schnell und einfach zu gestalten. Das Interface und die IP-Adresse werden entsprechend des blockierten Eintrags vorausgewählt. Nur ein Name muss eingegeben werden. Beim Interface kann auch – falls notwendig – aus allen vorhandenen Interfaces ohne Einschränkung gewählt werden. Lediglich die Adresse muss entweder komplett dem blockierten Zugriff entsprechen oder zumindest ein Netzwerk sein, das diese IP-Adresse beinhaltet, z. B. 192.168.3.0/24, 192.168.0.0/16. Je nach ausgewählter Adresse wird ein Host- oder ein Netzwerk-Objekt erstellt. Nachdem Quelle und Ziel gewählt sind, können Sie noch ggf die Zugriffsart oder das NAT ändern, indem die entsprechenden Symbole angeklickt werden wie bei den Regeln einer Desktop-Verbindung. Normalerweise sollte der Zugriff von Quelle zum Ziel oder ein beidseitiger Zugriff verwendet werden. NAT wird auch normalerweise nur bei einem Zugriff auf eine Adresse im Internet benötigt, deshalb wird NAT immer in Richtung des Internet-Objektes vorausgewählt. Sollte kein Internet-Objekt gewählt sein, ist NAT standardmäßig deaktiviert.

Nach dem Erstellen der Regel, können über den Protokoll-Dialog weitere Regeln definiert werden oder der Protokoll-Dialog geschlossen werden. Sollten neue Regeln erstellt worden sein, werden Sie nach dem Schliessen des Protokoll-Dialoges aufgefordert, die Regeln zu aktivieren.

3.4.2.9 SNMP-Einstellungen

SNMP (Simple Network Management Protocol) ist ein Netzwerkprotokoll, das zum Senden und Empfangen von Statusmeldungen innerhalb eines Netzwerks verwendet wird. Die Teilnehmer eines SNMP-basierten Informationsaustausches sind der SNMP-Manager (z. B. Nagios) und SNMP-Clients (Geräte wie etwa Ihre LANCOM R&S®Unified Firewall, die vom SNMP-Manager überwacht werden sollen).

Der SNMP-Manager fordert Informationen an und empfängt und überwacht diese. Die SNMP-Clients antworten auf Informationsanforderungen (z. B. „Zeige die aktuelle CPU-Auslastung / den aktuellen Speicherverbrauch des Geräts").

Die von den überwachten Geräten ausgegebenen Statusmeldungen werden wie ein Baum angeordnet (die sogenannte Management Information Base, kurz *MIB*), an dem jedes Blatt eine abrufbare Informationseinheit darstellt. Jedes Blatt kann einzeln über seine individuelle numerische Adresse aufgerufen und abgefragt werden. Eine Datei, die diese numerischen Adressdaten in sinnvolle Namen übersetzt und damit eine Übersicht aller auf dem überwachten Gerät verfügbaren Optionen darstellt, kann dem SNMP-Manager zur Verfügung gestellt werden, um die Nutzbarkeit für den Menschen zu erhöhen (`29577.1.1` wird z. B. als `RSCS.SystemLoad.cpuLoad` übersetzt).

Mit den **SNMP-Einstellungen** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
I/**0**	Ein Schiebeschalter gibt an, ob der jeweilige SNMP derzeit aktiv (**I**) oder inaktiv (**0**) ist. Mit einem Klick auf den Schiebeschalter ändern Sie den Status dieser Option. SNMP ist standardmäßig deaktiviert.
Empfangs-IP	Optional: Geben Sie eine lokale IP-Adresse ein, die der Dienst abhört. Wenn Sie die vorgegebene IP-Adresse `0.0.0.0` beibehalten, werden die Anfragen von allen IP-Adressen angenommen.
Empfangs-Port	Optional: Geben Sie die Portnummer an, die der Dienst abhört. Standardmäßig ist Port Nummer `161` eingestellt.
Protokoll-Version	Wählen Sie aus der Drop-down-Liste die Version des SNMP-Protokolls, die verwendet werden soll. Je nach ausgewählter Version sind verschiedene Optionen verfügbar. Standardmäßig ist Version `v2c` vorausgewählt.
Community String	Nur verfügbar, wenn die ausgewählte **Protokoll-Version** `v2c` ist: Geben Sie den Pre-Shared Key ein, den jeder SNMP-Manager oder -Client verwenden muss, um sich beim SNMP-Dienst der Zugriffszone zu authentifizieren.
Zeige Community String	Nur verfügbar, wenn die ausgewählte **Protokoll-Version** `v2c` ist: Setzen Sie den Haken in diesem Kontrollkästchen, um den Pre-Shared Key zur Überprüfung anzuzeigen.
Benutzername	Nur verfügbar, wenn die ausgewählte **Protokoll-Version** `v3` ist: Geben Sie den Benutzernamen ein, den jeder SNMP-Manager oder -Client verwenden muss, um sich gegenüber dem SNMP-Dienst der Zugriffszone zu identifizieren. Der Benutzername wird vom SNMP-Dienst intern erstellt und verwendet.
Authentifizierungs-Protokoll	Nur verfügbar, wenn die ausgewählte **Protokoll-Version** `v3` ist: Wählen Sie aus der Drop-down-Liste den Hash-Algorithmus aus, der zu Authentifizierungszwecken verwendet wird. Sie können zwischen `Keine Authentifizierung`, `MD5` und `SHA`auswählen.
Authentifizierungs-Passwort	Nur verfügbar, wenn die ausgewählte **Protokoll-Version** `v3` ist und das ausgewählte **Authentifizierungs-Protokoll** `MD5` oder `SHA` ist: Geben Sie das Passwort ein, dass zu Authentifizierungszwecken verwendet wird. Es muss aus mindestens acht Zeichen bestehen.
Zeige Authentifizierungs-Passwort	Optional und nur verfügbar, wenn die ausgewählte **Protokoll-Version** `v3` ist und das ausgewählte **Authentifizierungs-Protokoll** `MD5` oder `SHA` ist: Setzen Sie den Haken in diesem Kontrollkästchen, um das Authentifizierungspasswort zur Überprüfung anzuzeigen.
Privacy-Protokoll	Optional und nur verfügbar, wenn die ausgewählte **Protokoll-Version** `v3` ist und das ausgewählte **Authentifizierungs-Protokoll** `MD5` oder `SHA` ist: Wählen Sie aus der Drop-down-Liste den Algorithmus aus, der zur Verschlüsselung der Kommunikation mit dem SNMP-Dienst verwendet wird. Sie können zwischen den Verschlüsselungsalgorithmen `3DES` und `AES` auswählen. Diese Option ist standardmäßig auf `Keine Verschlüsselung` gesetzt.

Eingabefeld	Beschreibung
Privacy-Passwort	Nur verfügbar, wenn die ausgewählte **Protokoll-Version** `v3` ist, das ausgewählte **Authentifizierungs-Protokoll** `MD5` oder `SHA` und das ausgewählte **Privacy-Protokoll** `3DES` oder `AES` ist: Geben Sie das Passwort ein, das über den ausgewählten Verschlüsselungsalgorithmus zur Verschlüsselung der Kommunikation mit dem SNMP-Dienst verwendet wird.
Zeige Privacy-Passwort	Optional und nur verfügbar, wenn die ausgewählte **Protokoll-Version** `v3` ist, das ausgewählte **Authentifizierungs-Protokoll** `MD5` oder `SHA` und das ausgewählte **Privacy-Protokoll** `3DES` oder `AES` ist: Setzen Sie den Haken in diesem Kontrollkästchen, um das Privacy-Passwort zur Überprüfung anzuzeigen.
Ort	Optional: Geben Sie einen festen Wert ein, den LANCOM R&S®Unified Firewall auf Anfragen an bestimmte Object Identifiers (OIDs) der standardmäßigen Management Information Base (MIB) hin ausgibt: `sysLocation`.
Kontakt	Optional: Geben Sie einen festen Wert ein, den LANCOM R&S®Unified Firewall auf Anfragen an bestimmte Object Identifiers (OIDs) der standardmäßigen Management Information Base (MIB) hin ausgibt: `sysContacts`.

Wenn Sie Änderungen vorgenommen haben, können Sie diese mit den Schaltflächen unten rechts im Bearbeitungsfenster speichern (**Speichern**) oder verwerfen (**Zurücksetzen**). Andernfalls können Sie das Fenster schließen (**Schließen**).

Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

3.4.2.10 Statistiken

Die **Statistiken**-Fenster enthalten Grafiken und Tabellen. Sie können verschiedene Einstellungen an der Darstellung und den Daten dieser Statistiken vornehmen.

Um auf die Statistiken zuzugreifen und die entsprechenden Einstellungen zu konfigurieren, benötigen Sie **Statistiken** -Rechte. Weitere Informationen zu den Webclient-Rechten finden Sie unter *Einstellungen zu Administratoren* auf Seite 34.

Beim Analysieren der Statistiken und beim Konfigurieren der dazugehörigen Einstellungen muss der Administrator Vorschriften zur Datensicherheit einhalten.

Es gibt zwei Möglichkeiten, die einzelnen Statistiken abzurufen:

- Über die Links in der Navigationsleiste zu den detaillierten Statistikfenstern navigieren, z. B. über **Monitoring & Statistiken** > **Statistiken** > **Blockierte Verbindungen**.
- Verwenden Sie den Link **Details** in der oberen rechten Ecke des jeweiligen Grafikfensters in der Übersicht **Statistiken**. Der Link leitet Sie zu einem detaillierten Statistikfenster für diese Grafik weiter. Weitere Informationen finden Sie unter *Übersicht* auf Seite 79.

Arbeiten mit Statistiken

Es gibt zwei verschiedene Arten von Statistiken:

- Zähler werden als Liniendiagramme in den Statistikfenstern **Blockierte Verbindungen** und **Blockierte Inhalte** angezeigt. Die Diagramme enthalten jeweils mehrere Zähler.
- Toplisten geben eine Rangfolge verschiedener Ereignistypen an, die je nach ausgewähltem Zeitraum als Kreisdiagramm oder als Flächendiagramm angezeigt wird. Daten für den Zeitraum `Tag` werden als Kreisdiagramm angezeigt, Daten für die Zeiträume `Monat` und `Jahr` als Flächendiagramm.

Die Statistiken werden jeweils durch eine Tabellenansicht der grafischen Daten ergänzt. Bei Zählern zeigt die Datentabelle immer die gleichen Daten wie das Diagramm an. Jedes Statistikelement stellt eine Spalte in der Datentabelle dar. Bei Toplisten zeigt die Datentabelle die Werte der statistischen Elemente an.

Die Diagramme und Tabellen in den Statistik-Ansichten haben gemeinsame Funktionen, mit denen Sie die Anzeige der Daten anpassen und die Daten herausfiltern können, an denen Sie interessiert sind.

- Unter **Zeitraum** in der Kopfzeile der Statistikfenster können Sie die gewünschte Zeitspanne der anzuzeigenden Daten angeben. Mithilfe der Schaltflächen können Sie zwischen verschiedenen verfügbaren Zeiträumen wechseln. Sie können aus `Tag`, `Monat` und `Jahr` auswählen. Diese Option ist standardmäßig auf `Tag` gesetzt.
- Toplisten enthalten in der Kopfzeile des Fensters normalerweise ein Eingabefeld. Im Eingabefeld **Einträge** können Sie anpassen, wie viele Elemente maximal in der Grafik dargestellt werden. Diese Option ist standardmäßig auf `5` Einträge gesetzt. Sie können entweder eine andere Zahl eingeben oder die Anzahl über die Pfeile im Eingabefeld anpassen.

  Unabhängig vom für die Grafik gesetzten Wert zeigt die Tabelle immer bis zu 1000 Einträge.
- Sie können die Grafiken und Tabellen ein- und ausklappen, indem Sie auf das entsprechende Symbol in der Kopfzeile einer Grafik oder Tabelle klicken, um die Tabelle zu erweitern oder nicht benötigte Details auszublenden. Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28.
- Klicken Sie auf ☰ in der oberen rechten Ecke einer Grafik, um die verschiedenen Exportoptionen (Ansicht drucken, PNG, JPEG, SVG, PDF, CSV und XLS) für die in der Grafik dargestellten Daten zu nutzen.

  Wenn Sie die XLS-Exportoption für Toplisten auswählen, werden nur die von dieser Grafik genutzten Daten unter Berücksichtigung der von Ihnen gewählten maximalen Anzahl an Toplisten-Elementen exportiert.
- Kreis- und Flächendiagramme enthalten eine Legende. Die Legende ist farbkodiert und kann als Filter für die Grafik verwendet werden. Klicken Sie auf Elemente in der Legende unter der Grafik, um sie in der Grafik zu aktivieren oder deaktivieren. Wenn das Klicken keine Reaktion hervorruft und die Legende grau bleibt, ist die Datenerhebung für den zugrundeliegenden Ereignistypen in den Statistikeinstellungen deaktiviert und die Daten daher nicht verfügbar. Weitere Informationen finden Sie unter *Einstellungen zu Statistiken* auf Seite 56.
- Tooltips bieten Details zu spezifischen Punkten der grafischen Statistiken. Bewegen Sie die Maus über die Grafik, um genaue Werte für einen bestimmten Zeitpunkt einzusehen.

In den folgenden Abschnitten finden Sie weitere Informationen zu den in der Statistikübersicht verfügbaren Daten, den einzelnen Statistikfenstern und den dazugehörigen Einstellungen.

3.4.2.10.1 Blockierte Verbindungen

Im Bearbeitungsfenster **Blockierte Verbindungen** können Sie die folgenden Elemente konfigurieren:

Statistikelement (Ereignistyp)	Beschreibung
Regelsatz eingehend (**Blockierter eingehender Verkehr**)	Anzahl durch Eingangsregeln blockierter Verbindungen
Regelsatz ausgehend (**Blockierter weiterzuleitender Verkehr**)	Anzahl der durch Weiterleitungsregeln blockierter Verbindungen
IPS/IDS (**IDPS-Treffer**)	Anzahl der IDS/IPS-Warnmeldungen. Wenn der IDS/IPS-Modus auf „IDS“, „IPS Drop“ oder „IPS Reject“ gesetzt ist, zeigt dieses Statistikelement die Anzahl der verworfenen Pakete an. Weitere Informationen finden Sie unter *IDS / IPS* auf Seite 142.

3.4.2.10.2 Blockierte Inhalte

Im Bearbeitungsfenster **Blockierte Inhalte** können Sie die folgenden Elemente konfigurieren:

Statistikelement (Ereignistyp)	Beschreibung
Virus (Mail) (**Malware entdeckt (Mail)**)	Anzahl der in E-Mails erkannten Viren
Virus (Sonstiges) (**Malware entdeckt (HTTP und FTP)**)	Anzahl der im HTTP- oder FTP-Datenverkehr erkannten Viren
Spam (**Spam entdeckt**)	Anzahl der als Spam erkannten E-Mails
Web-Zugriff (**Web-Zugriff verhindert**)	Vom Contentfilter blockierte Webzugriffe
Appfilter (**Appfilter-Treffer**)	Anzahl der Warnmeldungen über blockierten anwendungsspezifischen Datenverkehr.

3.4.2.10.3 Übersicht

Navigieren Sie zu **Monitoring & Statistiken** > **Statistiken** > **Übersicht**, um eine Zusammenfassung aller verfügbaren statistischen Grafiken einzusehen. Diese kann als Dashboard von **Statistiken** betrachtet werden und soll grundlegende Antworten auf die häufigsten Fragen zu den durch Ihre LANCOM R&S®Unified Firewall erkennbaren Ereignissen geben.

Folgende spezielle Funktionen gelten nur für dieses Fenster (anders als in der Beschreibung der individuellen Statistikfenster in *Statistiken* auf Seite 77):

- Unter **Zeitraum** in der Kopfzeile des Statistikfensters können Sie die gewünschte Zeitspanne für die in allen Grafiken anzuzeigenden Daten angeben.
- Klicken Sie auf den Link **Details** in der oberen rechten Ecke einer einzelnen Grafik, um zum detaillierten Statistikfenster für die jeweilige Grafik weitergeleitet zu werden.
- Die Anzahl der Einträge für Toplist-Grafiken ist auf `5` festgesetzt.

3.4.2.10.4 Meistaufgerufene Domains

Das Fenster **Top aufgerufene Domains** zeigt die häufigsten von den Benutzern des lokalen Netzwerks aufgerufenen Internetseiten an, sofern Sie Ihrer LANCOM R&S®Unified Firewall erlauben, diese Daten zu erheben, indem Sie den Ereignistyp **Web-Zugriff erlaubt** aktivieren. Diese Statistiken dienen dazu, festzustellen, ob die Internetnutzung den Unternehmensrichtlinien und den Zielen der Firma entspricht.

3.4.2.10.5 Meistblockierte Domains

Das Fenster **Top blockierte Domains** zeigt die am häufigsten blockierten Internetseiten an, sofern Sie Ihrer LANCOM R&S®Unified Firewall erlauben, diese Daten zu erheben, indem Sie den Ereignistyp **Web-Zugriff verhindert** aktivieren.

3.4.2.10.6 Höchster Datenverkehr pro Quelle

Das Fenster **Top Traffic pro Quelle** zeigt das Datenvolumen der meistaufgerufen Datenverkehrsquellen an, sofern Sie Ihrer LANCOM R&S®Unified Firewall erlauben, diese Daten zu erheben, indem Sie den Ereignistyp **Beendete Verbindung** aktivieren.

3.4.2.11 Syslog-Server

Mit Ihrer LANCOM R&S®Unified Firewall können mehrere externe Syslog-Server so konfiguriert werden, dass sie von verschiedenen Meldungsquellen erzeugte Ereignisprotokoll-Meldungen für Berichtszwecke weiterleiten.

Syslog-Meldungen werden in der Regel im Klartext (unverschlüsselt) über Port Nummer 514 und entweder über das User Datagram Protocol (UDP) oder das Transmission Control Protocol (TCP) an den Remote-Syslog-Server gesendet.

In den folgenden Abschnitten finden Sie weiterführende Informationen zu externen Syslog-Servern.

3.4.2.11.1 Übersicht Syslog-Server

Navigieren Sie zu **Monitoring & Statistiken** > **Syslog Server**, um die Liste der derzeit im System angelegten Remote-Syslog-Server in der Objektleiste anzuzeigen.

In der erweiterten Ansicht zeigt die Tabelle die Serveradresse des externen Syslog-Servers an, die sich aus der IP-Adresse und dem Port zusammensetzt. Zum Beispiel steht die Serveradresse `192.168.124.5:514` für die IP-Adresse `192.168.124.5` und die Port-Nummer `514`. Außerdem wird der Protokolltyp angezeigt, der für die Übertragung der Textmeldung verwendet wird. Mit den Schaltflächen in der letzten Spalte können Sie die Einstellungen für einen vorhandenen externen Syslog-Server einsehen und anpassen, einen neuen Syslog-Server ausgehend von einer Kopie eines vorhandenen externen Syslog-Servers anlegen oder einen Remote-Syslog-Server aus dem System löschen.

Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28.

3.4.2.11.2 Einstellungen für Syslog-Server

Mit den Einstellungen unter **Syslog Server** können Sie Verbindungsdetails für mehrere Remote-Syslog-Server angeben, um von verschiedenen Meldungsquellen erzeugte Ereignisprotokoll-Meldungen weiterzuleiten.

Unter **Monitoring & Statistiken** > **Syslog Server** können Sie einen neuen entfernten Syslog-Server hinzufügen oder einen vorhandenen bearbeiten.

Im Bearbeitungsfenster **Syslog Server** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Ziel-IP	Geben Sie die IP-Adresse des Servers ein.
Ziel-Port	Geben Sie die zu verwendende Portnummer an, indem Sie einen ganzzahligen Wert eingeben.
Transport-Protokoll	Wählen Sie den zu verwendenden Protokoll-Typ aus der Drop-down-Liste aus.

Die Schaltflächen rechts unten im Bearbeitungsfeld hängen davon ab, ob Sie einen neuen Remote-Syslog-Server hinzufügen oder einen bestehenden Server bearbeiten. Für einen neu konfigurierten Server klicken Sie **Erstellen**, um den Server zur Liste der verfügbaren Remote-Syslog-Server hinzuzufügen oder **Abbrechen**, um Ihre Änderungen zu verwerfen.

Wenn Sie Änderungen vorgenommen haben, können Sie diese mit den Schaltflächen unten rechts im Bearbeitungsfenster speichern (**Speichern**) oder verwerfen (**Zurücksetzen**). Andernfalls können Sie das Fenster schließen (**Schließen**).

Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

3.4.2.12 WireGuard-Status

Unter **Monitoring & Statistiken** > **WireGuard-Status** kann der Status der WireGuard-Verbindungen überwacht werden. Ob eine Verbindung tatsächlich aufgebaut wurde wird bei WireGuard nicht angezeigt.

Spalte	Beschreibung
Remote-Adresse	Die Remote-Adresse dieser WireGuard-Verbindung. ⓘ Nach dieser Spalte kann gefiltert werden.
Keep-Alive	Der eingestellte Keep-Alive-Wert dieser WireGuard-Verbindung.
Gesendet	Über diese Verbindung gesendete Bytes.
Empfangen	Über diese Verbindung empfangene Bytes.
Erlaubte IP-Adressen	Die konfigurierten erlaubten IP-Adressen dieser WireGuard-Verbindung. ⓘ Nach dieser Spalte kann gefiltert werden.

3.4.3 Netzwerk

Mit den Einstellungen unter **Netzwerk** können Sie Ihr Netzwerk organisieren, indem Sie Interfaces, Verbindungen, WLAN, Routing-Regeln und DHCP-Interfaces konfigurieren. Darüber hinaus können Sie den WAN-Zugang Ihrer LANCOM R&S®Unified Firewall einrichten, indem Sie DNS-Einstellungen, DynDNS-Accounts und QoS-Einstellungen konfigurieren.

3.4.3.1 Verbindungen

Mit den **Desktop-Verbindungen**-Einstellungen können Sie die Netzwerk- und PPP-Verbindungen auf Ihrer LANCOM R&S®Unified Firewall konfigurieren.

3.4.3.1.1 Netzwerkverbindungen

Mit den Einstellungen unter **Netzwerk-Verbindungen** können Sie Netzwerkverbindungen konfigurieren. Das System bietet standardmäßige Verbindungen zu allem verfügbaren Ethernet-Interfaces.

In den folgenden Abschnitten finden Sie weiterführende Informationen zu Netzwerkverbindungen.

Übersicht Netzwerkverbindungen

Navigieren Sie zu **Netzwerk** > **Verbindungen** > **Netzwerk-Verbindungen**, um die Liste der Netzwerk-Verbindungen, die derzeit im System angelegt sind, in der Leiste mit der Objektliste anzuzeigen.

In der erweiterten Ansicht wird in der ersten Spalte der Tabelle der **Name** der Netzwerkverbindung angezeigt. Die Spalte **Status** zeigt einen der folgenden Statusindikatoren an.

- Grün – Die Netzwerkverbindung ist aktiv.
- Grau – Die Netzwerkverbindung ist inaktiv.
- Rot – Die Netzwerkverbindung ist getrennt.

Außerdem werden das **Interface**, dem die Netzwerkverbindung zugewiesen ist sowie der **Typ** der Verbindung angezeigt. Mit den Schaltflächen in der letzten Spalte können Sie die Einstellungen für eine vorhandene Netzwerkverbindung einsehen und anpassen, eine neue Verbindung auf der Grundlage einer Kopie einer bestehenden Netzwerkverbindung anlegen oder eine Verbindung aus dem System löschen.

Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28.

Einstellungen für Netzwerkverbindungen

Nutzen Sie die Einstellungen unter **Netzwerk-Verbindungen**, um benutzerdefinierte Netzwerkverbindungen zu konfigurieren.

Unter **Netzwerk** > **Verbindungen** > **Netzwerk-Verbindungen** können Sie eine neue Netzwerkverbindung hinzufügen oder eine vorhandene bearbeiten.

Im Bearbeitungsfenster **Netzwerk-Verbindung** können Sie die folgenden Informationen einsehen und die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
I/0	Ein Schiebeschalter gibt an, ob die Netzwerk-Verbindung derzeit aktiv (**I**) oder inaktiv (**0**) ist. Mit einem Klick auf den Schiebeschalter können Sie den Status der Verbindung ändern. Eine neue Verbindung ist standardmäßig aktiviert.
Name	Geben Sie einen Namen für die Verbindung ein. Wenn Sie dieses Eingabefeld frei lassen, wird der Name automatisch auf der Grundlage des ausgewählten Interfaces und des Verbindungstypen erzeugt.
Interface	Wählen Sie aus der Drop-down-Liste aus, welches Interface Sie der Verbindung zuweisen möchten. Sie können zwischen Ethernet-, VLAN- oder Bridge-Interface auswählen.
Typ	Wählen Sie den Verbindungstyp aus der Drop-down-Liste aus. Diese Option ist standardmäßig auf `Static IPv4` gesetzt, Sie können die Einstellungen jedoch bei Bedarf auf einen der anderen Werte setzen: - **Static IPv4** – In diesem Modus wird eine statische IPv4-Adresse für die Verbindung festgelegt.

Eingabefeld	Beschreibung
	› **DHCPv4** – In diesem Modus werden IPv4-Adressen dynamisch zugewiesen. › **Static IPv6** – In diesem Modus wird eine statische IPv6-Adresse für die Verbindung festgelegt. Diese Verbindungen können nur in IPsec-Verbindungen verwendet werden. › **DHCPv6** – In diesem Modus werden IPv6-Adressen dynamisch zugewiesen. Diese Verbindungen können nur in IPsec-Verbindungen verwendet werden. Sobald Sie auf **Erstellen** klicken, um die Netzwerkverbindung herzustellen, kann der Verbindungstyp nicht mehr geändert werden. Die Elemente im Tab **Netzwerk** hängen vom gewählten Verbindungstyp ab.
Verwendet von	Zeigt an, welche Komponenten die Netzwerkverbindung verwenden.
Status	Zeigt den Status der Netzwerkverbindung an. Der Status kann einer der folgenden sein: › `aktiv` – Die Netzwerkverbindung ist aktiv. › `abgeschaltet` – Die Netzwerkverbindung ist inaktiv. › `unterbrochen` – Die Netzwerkverbindung ist getrennt.

Im Tab **Netzwerk** :

Eingabefeld	Beschreibung
IP-Adressen	Weisen Sie der Netzwerkverbindung eine oder mehrere IP-Adressen zu. Geben Sie eine IP-Adresse in CIDR-Schreibweise ein (IP-Adresse gefolgt von einem Schrägstrich „/“ und der Anzahl der in der Subnetzmaske festgelegten Bits, beispielsweise `192.168.50.1/24`). Klicken Sie auf **Hinzufügen**, um die IP-Adresse zur Liste hinzuzufügen. Sie können einzelne Einträge in der Liste bearbeiten oder löschen, indem Sie auf die entsprechende Schaltfläche neben einem Eintrag klicken. Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28. Wenn Sie eine IP-Adresse bearbeiten, erscheint auf der rechten Seite des Eintrags ein Haken. Sie müssen Ihre Änderung zunächst mit diesem Haken bestätigen, bevor Sie die Einstellungen für die IP Addresse speichern können. Klicken Sie auf ▲ / ▼, um die Reihenfolge der IP-Adressen in der Liste zu ändern. Die erste IP-Adresse in der Liste wird standardmäßig als Quell-IP-Adresse für NAT- und IPsec-Verbindungen verwendet. Falls unter **Typ** eine IPv6-Option eingestellt wurde, dann können hier nur IPv6-Werte eingegeben werden.
Gateway beziehen	Optional und nur verfügbar, wenn der ausgewählte **Typ** der Verbindung `DHCP` ist. Setzen Sie den Haken in diesem Kontrollkästchen, wenn Sie möchten, dass Ihre LANCOM R&S®Unified Firewall ein Gateway für die Verbindung vom DHCP-Server bezieht.
DNS-Server beziehen	Optional und nur verfügbar, wenn der ausgewählte **Typ** der Verbindung `DHCP` ist. Wählen Sie dieses Kontrollkästchen wenn Sie möchten, dass Ihre LANCOM R&S®Unified Firewall einen DNS-Server für die Verbindung bezieht.

Eingabefeld	Beschreibung
Domain beziehen	Optional und nur verfügbar, wenn der ausgewählte **Typ** der Verbindung `DHCP` ist. Aktivieren Sie dieses Kontrollkästchen wenn Sie möchten, dass Ihre LANCOM R&S®Unified Firewall eine Domäne für die Verbindung vom DHCP-Server bezieht.
Via DHCP bezogen	Optional und nur verfügbar, wenn der ausgewählte **Typ** der Verbindung `DHCP` ist. Zeigt eine der folgenden Statusmeldungen an: › Wenn die Verbindung korrekt funktioniert, wird die IP-Adresse angezeigt. › `Verbindung noch nicht gespeichert` – Eine neue Verbindung wird hergestellt. › `Failed` – Die DHCP-Verbindung konnte nicht hergestellt werden.

Im Tab **WAN** :

Eingabefeld	Beschreibung
Standard Gateway setzen	Optional und nur verfügbar, wenn der ausgewählte **Typ** der Verbindung `Static` ist: Setzen Sie den Haken in diesem Kontrollkästchen, um ein Standard-Gateway für die Netzwerkverbindung festzulegen. Wenn Sie `DHCP` als Verbindungstyp auswählen, ist standardmäßig ein Haken gesetzt und das Kästchen ausgegraut, da das Gateway vom DHCP-Server bezogen wird.
Standard-Gateway	Optional und nur verfügbar, wenn der ausgewählte **Typ** der Verbindung `Static` ist: Geben Sie das Standard-Gateway für diese Verbindung ein. Wenn Sie `DHCP` als Verbindungstyp auswählen, ist das Eingabefeld ausgegraut und zeigt das Gateway an, das vom DHCP-Server bezogen wird. Falls unter **Typ** eine IPv6-Option eingestellt wurde, dann können hier nur IPv6-Werte eingegeben werden.
Zeitbeschränkungen	Optional: Setzen Sie den Haken in diesem Kontrollkästchen, um eine Zeitgrenze festzulegen, bis zu der die Verbindung aktiv bleibt. Klicken Sie auf **Bearbeiten**, um das Bearbeitungsfenster **Zeitbeschränkung** zu öffnen, das die folgenden Optionen zur Verfügung stellt: › Mit den Schiebereglern können Sie bestimmte Zeiten und Wochentage einstellen. › **Immer an** – die Verbindung ist immer aktiv. › **Immer aus** – die Verbindung ist immer inaktiv. Mit den Schaltflächen unten rechts im Bearbeitungsfenster können Sie Ihre Änderungen an den Zeiteinschränkungen speichern (**OK**) oder verwerfen (**Abbrechen**). Das Bearbeitungsfenster schließt sich und die gewählte Option wird links von der Schaltfläche **Bearbeiten** angezeigt: `Eingeschränkt`, `Immer an` oder `Immer aus`.
Multi-WAN-Gewichtung	Legen Sie fest, welcher Anteil des Internet-Datenverkehrs über diese Verbindung geroutet wird, indem Sie einen Wert von `1` bis `253` eingeben. Je höher der eingegebene Wert, desto höher der Prozentanteil des über diese Verbindung gerouteten Datenverkehrs. Wird für alle Verbindungen der gleiche Wert eingestellt, wird der Datenverkehr gleichmäßig auf alle Verbindungen verteilt.
Desktop-Objekt	Wählen Sie aus der Drop-down-Liste ein Internetobjekt aus, das in Firewall-Regeln für diese WAN-Verbindung verwendet wird. Weitere Informationen finden Sie unter *Internetobjekte* auf Seite 119.

Im Tab **Failover** :

Eingabefeld	Beschreibung
Heartbeats	Legen Sie fest, wie der Status der Verbindung getestet wird, indem Sie Tests hinzufügen. Die Standardeinstellungen enthalten einen Ping-Test des Google-Servers (8.8.8.8). Klicken Sie auf **Hinzufügen**, um einen weiteren Test zur Liste hinzufügen. Weitere Informationen zur Konfiguration des Erreichbarkeitstests finden Sie unter *Heartbeat-Einstellungen* auf Seite 84. Sie können einzelne Einträge in der Liste bearbeiten oder löschen, indem Sie auf die entsprechende Schaltfläche neben einem Eintrag klicken. Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28. Falls unter **Typ** eine IPv6-Option eingestellt wurde, dann können hier nur IPv6-Werte eingegeben werden.
Als Backup-Verbindung verwenden	Optional: Setzen Sie den Haken in diesem Kontrollkästchen, um die Verbindung als Backup-Internetverbindung zu konfigurieren.
Backup-Verbindungen	Wählen Sie eine beliebige Backup-Verbindung, die Sie der Verbindung zuweisen möchten und geben Sie ihre **Priorität** an. Falls die aktuelle Verbindung versagt, wechselt Ihre LANCOM R&S®Unified Firewall zur verfügbaren Backup-Verbindung mit der höchsten Priorität. Klicken Sie auf **Hinzufügen**, um die Backup-Verbindung zur Liste hinzuzufügen. Sie können einzelne Einträge in der Liste bearbeiten oder löschen, indem Sie auf die entsprechende Schaltfläche neben einem Eintrag klicken. Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28. Wenn Sie eine Backup-Verbindung bearbeiten, erscheint auf der rechten Seite des Eintrags ein Haken. Sie müssen Ihre Änderung zunächst mit diesem Haken bestätigen, bevor Sie die Einstellungen zur Backup-Verbindung speichern können.

Die Schaltflächen rechts unten im Bearbeitungsfeld hängen davon ab, ob Sie eine neue Netzwerkverbindung hinzufügen oder eine bestehende Verbindung bearbeiten. Klicken Sie für eine neu konfigurierte Netzwerkverbindung auf **Erstellen**, um die Verbindung zur Liste der verfügbaren Netzwerkverbindungen hinzuzufügen, oder auf **Abbrechen**, um die Erstellung einer neuen Netzwerkverbindung abzubrechen. Zum Bearbeiten einer vorhandenen Netzwerkverbindung klicken Sie auf **Speichern**, um die neu konfigurierte Verbindung zu speichern, oder auf **Zurücksetzen**, um Ihre Änderungen zu verwerfen. Sie können auf **Schließen** klicken, um das Bearbeitungsfenster zu schließen, solange keine Änderungen darin vorgenommen wurden.

Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

Heartbeat-Einstellungen

Im Bearbeitungsfenster **Heartbeat** können sie automatische Heartbeat-Tests einrichten, mit denen der Status der Verbindung überprüft wird. Sie können in diesem Bearbeitungsfenster die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Typ	Wählen Sie aus der Drop-Down-Liste den Typ des Erreichbarkeitstest ein, den Sie durchführen möchten: › `curl` – Dieser Modus erlaubt die HTTP-Request-Methoden GET und POST. Mit POST können an den angegebenen Endpunkt zu sendende Daten im JSON-Format übergeben werden. › `ping` – Dieser Modus sendet Ping-Signale an das Ziel. › `tcp_probe` – Dieser Modus testet die Kapazität einer TCP-Verbindung.
Timeout	Geben Sie die Zeitüberschreitung für den Test in Sekunden ein.

Eingabefeld	Beschreibung
Anzahl Versuche	Legen Sie die Gesamtanzahl der durchzuführenden Versuche fest.
Anzahl erfolgreicher Versuche	Legen Sie die Zahl der für einen erfolgreichen Heartbeat erforderlichen erfolgreichen Versuche fest.
Argumente	Legen Sie die im Test zu verwendenden Argumente, z. B. IP-Adressen, die gepingt werden, fest.

Wenn Sie im Tab **Failover** eine Backup-Internetverbindung festgelegt haben und der automatische Heartbeat-Test den Status der Verbindung als `disconnected`anzeigt, wechselt LANCOM R&S®Unified Firewall automatisch zur verfügbaren Backup-Verbindung mit der höchsten Priorität.

Mit den Schaltflächen unten im Bearbeitungsfenster rechts können Sie Ihre Änderungen am automatischen Heartbeattest speichern (**OK**) oder den Verbindungstest manuell ausführen (**Testen**). Außerdem können Sie Ihre Änderungen am Test verwerfen (**Abbrechen**), das Bearbeitungsfenster schließen und zum Bearbeitungsfenster **Netzwerk-Verbindung** zurückkehren. Der festgelegte Test wird als Eintrag in der Liste unter **Heartbeats** im Tab **Failover** angezeigt.

3.4.3.1.2 PPP-Verbindungen

Mit den Einstellungen unter **PPP-Verbindungen** können Sie vorhandene Verbindungen, die das Point-to-Point-Protokoll verwenden, konfigurieren und neue hinzufügen.

In den folgenden Abschnitten finden Sie weiterführende Informationen zu PPP-Verbindungen.

Übersicht PPP-Verbindungen

Navigieren Sie zu **Netzwerk** > **Verbindungen** > **PPP-Verbindungen**, um die Liste der derzeit im System angelegten PPP-Verbindungen in der Objektleiste anzuzeigen.

In der erweiterten Ansicht werden in den Tabellenspalten der **Name** und der **Typ** der Verbindung angezeigt und ob sie **Aktiv** ist oder nicht. Mit den Schaltflächen in der letzten Spalte können Sie die Einstellungen für eine vorhandene PPP-Verbindung einsehen und anpassen, eine neue Verbindung auf der Grundlage einer Kopie einer bestehenden PPP-Verbindung anlegen oder eine PPP-Verbindung aus dem System löschen.

Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28.

Einstellungen für PPP-Verbindungen

Unter **Netzwerk** > **Verbindungen** > **PPP-Verbindungen** können Sie eine neue Netzwerkverbindung hinzufügen oder eine vorhandene bearbeiten.

Die Einstellungen unter **PPP-Verbindungen** enthalten die folgenden Elemente:

Eingabefeld	Beschreibung
I/O	Ein Schiebeschalter gibt an, ob die PPP-Verbindung derzeit aktiv (**I**) oder inaktiv (**0**) ist. Mit einem Klick auf den Schiebeschalter können Sie den Status der Verbindung ändern. Neu angelegte PPP-Verbindungen sind standardmäßig aktiviert.
Name	Geben Sie den Namen der Netzwerkverbindung an. Wenn Sie dieses Eingabefeld frei lassen, wird der Name automatisch auf der Grundlage des ausgewählten Interfaces und des Verbindungstypen erzeugt.
Interface	Weisen Sie der Verbindung ein Interface zu. Sie können nur ein PPP-Interface auswählen, das noch nicht für eine andere Verbindung verwendet wird.
Typ	Wählen Sie je nach Ihrem Internet-Provider den Verbindungstyp aus der Drop-down-Liste aus: `PPPoE` oder `PPTP`. Nutzen Sie den PPPoE-Modus, um unter Verwendung des

Eingabefeld	Beschreibung
	Point-to-Point-Protokolls eine Ethernet-Verbindung herzustellen. PPPoE wird in der Regel für die gemeinsame Nutzung einer Breitbandverbindung, zum Beispiel einer einzelnen DSL-Leitung oder eines Kabelmodems, eingesetzt. Nutzen Sie den PPTP-Modus, um unter Verwendung des Point-to-Point-Tunneling-Protokolls eine Verbindung herzustellen. Sobald Sie auf **Erstellen** klicken, um die PPP-Verbindung herzustellen, kann der Verbindungstyp nicht mehr geändert werden. Die Elemente im Tab **Konfiguration** hängen vom gewählten Verbindungstyp ab.
Verwendet von	Zeigt an, welche Komponenten die PPP-Verbindung verwenden.
Status	Zeigt den Status der Verbindung an (`aktiv`, `unterbrochen` oder `abgeschaltet`).

Im Tab **Konfiguration** :

Eingabefeld	Beschreibung
Auth. Methode	Wählen Sie je nach Ihrem Internet-Provider die Authentifizierungsmethode für die Verbindung aus: › `None` › `auto` – Wählt automatisch die Authentifizierungsmethode aus, die am besten zum Internet-Provider passt. › `pap-only` – Passwort-Authentifizierung › `chap-only` – Handshake-Authentifizierung › `ms-chap2` – Handshake-Authentifizierung für Microsoft
Benutzername	Geben Sie den Benutzernamen ein, der für die Verbindung mit Ihrem Internet-Provider benötigt wird.
Kennwort	Geben Sie das Passwort ein, das für die Verbindung mit Ihrem Internet-Provider benötigt wird.
PPTP-Server-IP	Wenn Sie PPTP als Verbindungstyp ausgewählt haben, geben Sie die IP-Adresse des PPTP-Servers ein.
MPPE	Wenn Sie PPTP als Verbindungstyp angegeben haben, wählen Sie die Schlüssellänge für die Microsoft Point-to-Point-Verschlüsselung aus. › `mppe-40` › `mppe-56` › `mppe-128`
Lokale IP	Optional: Geben Sie Ihre lokale IP-Adresse nur ein, wenn dies explizit von Ihrem Internet-Provider verlangt wird.
Remote-IP	Optional: Geben Sie Ihre Remote-IP-Adresse nur ein, wenn dies explizit von Ihrem Internet-Provider verlangt wird.
AC-Hardware-Adresse	Optional: Geben Sie die Hardware-MAC-Adresse des Access Concentrators ein, den Ihr Internet-Provider verwendet. Führen Sie diesen Schritt nur aus, wenn Ihr Internet-Provider dies explizit verlangt.
Trennung erzwingen	Optional: Setzen Sie den Haken in diesem Kontrollkästchen, wenn Sie zu einem angegebenen Zeitpunkt eine Trennung der Verbindung auslösen möchten. Geben Sie den Zeitpunkt im Format `HH:MM:SS` ein.

Eingabefeld	Beschreibung
	Einige Internet-Provider lösen in bestimmten Intervallen (üblicherweise alle 24 Stunden) eine Verbindungstrennung aus. Wenn diese Einstellung aktiv ist, löst Ihre LANCOM R&S®Unified Firewall die Verbindungstrennung zu einem bestimmten Zeitpunkt aus und verhindert damit die automatische Trennung durch den Internet-Provider. So können Sie den Zeitpunkt der Verbindungstrennung selbst bestimmen.

Im Tab **WAN** :

Eingabefeld	Beschreibung
Zeitbeschränkungen	Setzen Sie den Haken in diesem Kontrollkästchen, um eine Zeitgrenze festzulegen, bis zu der die Verbindung aktiv bleibt. Klicken Sie auf **Bearbeiten**, um das Bearbeitungsfenster **Zeitbeschränkungen** zu öffnen, das die folgenden Optionen zur Verfügung stellt: › Mit den Schiebereglern können Sie bestimmte Zeiten und Wochentage einstellen. › **Immer an** – die Verbindung ist immer aktiv. › **Immer aus** – die Verbindung ist immer inaktiv.
Multi-WAN-Gewichtung	Legen Sie fest, welcher Anteil des Internet-Datenverkehrs über diese Verbindung geroutet wird, indem Sie einen Wert von `1` bis `256` eingeben. Je höher der eingegebene Wert, desto höher der Prozentanteil des über diese Verbindung gerouteten Datenverkehrs. Wird für alle Verbindungen der gleiche Wert eingestellt, wird der Datenverkehr gleichmäßig auf alle Verbindungen verteilt.
Desktop-Objekt	Wählen Sie ein Internetobjekt aus, das in Firewall-Regeln für diese Verbindung verwendet wird. Weitere Informationen finden Sie unter *Internetobjekte* auf Seite 119.

Im Tab **Failover** :

Eingabefeld	Beschreibung
Heartbeats	Legen Sie fest, wie der Status der Verbindung getestet wird, indem Sie Ping-Tests hinzufügen. Die Standardeinstellungen enthalten einen Ping-Test des Google-Servers (8.8.8.8). Klicken Sie auf **Hinzufügen**, um einen weiteren Test zur Liste hinzufügen. Weitere Informationen zur Konfiguration des Erreichbarkeitstests finden Sie unter *Heartbeat-Einstellungen* auf Seite 87. Sie können einzelne Einträge in der Liste bearbeiten oder löschen, indem Sie auf die entsprechende Schaltfläche neben einem Eintrag klicken. Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28.
Als Backup-Verbindung verwenden	Setzen Sie den Haken in diesem Kontrollkästchen, um die Verbindung als Backup-Internetverbindung zu konfigurieren.
Backup-Verbindungen	Wählen Sie eine beliebige Backup-Verbindung, die Sie der Verbindung zuweisen möchten und geben Sie ihre **Priorität** an. Falls die aktuelle Verbindung versagt, wechselt Ihre LANCOM R&S®Unified Firewall zur verfügbaren Backup-Verbindung mit der höchsten Priorität. Klicken Sie auf **Hinzufügen**, um die Backup-Verbindung zur Liste hinzuzufügen. Sie können einzelne Einträge in der Liste bearbeiten oder löschen, indem Sie auf die entsprechende Schaltfläche neben einem Eintrag klicken. Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28.

Heartbeat-Einstellungen

Mit den Einstellungen unter **Heartbeats** können Sie automatische Heartbeat-Tests für diese Verbindung konfigurieren. Das Bearbeitungsfenster enthält die folgenden Elemente:

Eingabefeld	Beschreibung
Typ	Wählen Sie aus der Drop-Down-Liste den Typ des Erreichbarkeitstest ein, den Sie durchführen möchten: › `ping` – Dieser Modus sendet Ping-Signale an das Ziel. › `tcp_probe` – Dieser Modus testet die Kapazität einer TCP-Verbindung.
Timeout	Geben Sie die Zeitüberschreitung für den Test in Sekunden ein.
Anzahl Versuche	Legen Sie die Gesamtanzahl der durchzuführenden Versuche fest.
Anzahl erfolgreicher Versuche	Legen Sie die Zahl der für einen erfolgreichen Heartbeat erforderlichen erfolgreichen Versuche fest.
Argumente	Legen Sie die im Test zu verwendenden Argumente, z. B. IP-Adressen, die gepingt werden, fest.

Klicken Sie auf **Testen**, um den Verbindungstest manuell durchzuführen. Klicken Sie auf **OK**, um die Einstellungen zu speichern und zum Bearbeitungsfenster **Netzwerk-Verbindung** zurückzukehren.

Die Schaltflächen rechts unten im Bearbeitungsfeld hängen davon ab, ob Sie eine neue PPP-Verbindung hinzufügen oder eine bestehende Verbindung bearbeiten. Klicken Sie für eine neu konfigurierte Netzwerkverbindung auf **Erstellen**, um die Verbindung zur Liste der verfügbaren PPP-Netzwerkverbindungen hinzuzufügen, oder auf **Abbrechen**, um die Erstellung einer neuen Netzwerkverbindung abzubrechen. Zum Bearbeiten einer vorhandenen PPP-Verbindung klicken Sie auf **Speichern**, um die neu konfigurierte Verbindung zu speichern, oder auf **Zurücksetzen**, um Ihre Änderungen zu verwerfen. Sie können auf **Schließen** klicken, um das Bearbeitungsfenster zu schließen, solange keine Änderungen darin vorgenommen wurden.

Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

3.4.3.1.3 WWAN-Verbindungen

Mit den Einstellungen unter **WWAN-Verbindungen** können Sie Verbindungen, die ein **WWAN-Interface** verwenden, konfigurieren und neue hinzufügen.

In den folgenden Abschnitten finden Sie weiterführende Informationen zu WWAN-Verbindungen.

Übersicht WWAN-Verbindungen

Navigieren Sie zu **Netzwerk** > **Verbindungen** > **WWAN-Verbindungen**, um die Liste der derzeit im System angelegten WWAN-Verbindungen in der Objektleiste anzuzeigen.

In der Ansicht wird zuerst der **Name** der Verbindung angezeigt und ob sie **Aktiv** ist oder nicht. Mit den Schaltflächen in der letzten Spalte können Sie die Einstellungen für eine vorhandene WWAN-Verbindung einsehen und anpassen, eine neue Verbindung auf der Grundlage einer Kopie einer bestehenden WWAN-Verbindung anlegen oder eine WWAN-Verbindung aus dem System löschen.

Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28.

Einstellungen für WWAN-Verbindungen

Unter **Netzwerk** > **Verbindungen** > **WWAN-Verbindungen** können Sie eine neue Netzwerkverbindung hinzufügen oder eine vorhandene bearbeiten.

Die Einstellungen unter **WWAN-Verbindung** enthalten die folgenden Elemente:

Eingabefeld	Beschreibung
I/0	Ein Schiebeschalter gibt an, ob die WWAN-Verbindung derzeit aktiv (**I**) oder inaktiv (**0**) ist. Mit einem Klick auf den Schiebeschalter können Sie den Status der Verbindung ändern. Neu angelegte WWAN-Verbindungen sind standardmäßig aktiviert.
Name	Geben Sie den Namen der Netzwerkverbindung an.
Interface	Weisen Sie der Verbindung ein Interface zu. Sie können nur ein WWAN-Interface auswählen, das noch nicht für eine andere Verbindung verwendet wird.
Status	Zeigt den Status der Verbindung an (`aktiv`, `unterbrochen` oder `abgeschaltet`).
Verbunden mit Heimat-Netz	Zeigt den Roaming-Status der Verbindung an bzw. ob die Verbindung gerade in das Heimat-Netz besteht, oder nicht.

Im Tab **WWAN** :

Eingabefeld	Beschreibung
APN	Steht für Access Point Name, zu Deutsch Zugangspunkt. Dadurch ist der Zugriff auf das Internet im Mobilnetz erst möglich. Das **APN** ist eine Art Adresse, mit dem die LANCOM R&S®Unified Firewall in Kontakt zum Mobilfunknetz steht. Einige gängige APNs der großen ISPs sind direkt auswählbar, wenn man in das leere Eingabefeld klickt. Es kann aber auch eine eigene Angabe gemacht werden.
Benutzername	Geben Sie den Benutzernamen ein, der für die Verbindung mit Ihrem Mobilfunk-Provider benötigt wird.
Passwort	Geben Sie das Passwort ein, das für die Verbindung mit Ihrem Mobilfunk-Provider benötigt wird.
SIM-PIN	Geben Sie die PIN ein, die für den Zugriff auf Ihre SIM-Karte benötigt wird. Um die PIN ggf. zu ändern, benutzen Sie die Schaltfläche **PIN ändern** unten links. Bei eingelegter SIM-Karte wird die eingegebene PIN überprüft, sobald der Dialog gespeichert wird. Wird eine falsche PIN eingegeben, erscheint eine Fehlermeldung unterhalb des Eingabefeldes, die die Anzahl der verbleibenden Versuche angibt. Da unabhängig von der Konfiguration die SIM-Karte jederzeit gewechselt, oder auch erst später eingesetzt werden kann, wird diese Fehlermeldung u. U. auch direkt angezeigt, sobald eine Verbindung zum Bearbeiten geöffnet wird. Wurde die PIN einmal abgelehnt, dann wird das Gerät bei Reboots o. ä. nicht noch einmal probieren, diese PIN zu verwenden, um eine Sperrung der SIM-Karte zu verhindern. Ist die SIM-Karte bereits gesperrt, erscheint unten links im Editor die Schaltfläche **SIM entsperren**. Ein Klick auf diese Schaltfläche öffnet ein Fenster, in dem statt der alten PIN jedoch der PUK (Personal Unblocking Key) und eine neue PIN eingegeben werden müssen.
Roaming erlauben	Erlauben Sie ggf. Roaming.

Im Tab **WAN** :

Eingabefeld	Beschreibung
Zeitbeschränkungen	Setzen Sie den Haken in diesem Kontrollkästchen, um eine Zeitgrenze festzulegen, bis zu der die Verbindung aktiv bleibt. Klicken Sie auf **Bearbeiten**, um das Bearbeitungsfenster **Zeitbeschränkungen** zu öffnen, das die folgenden Optionen zur Verfügung stellt: › Mit den Schiebereglern können Sie bestimmte Zeiten und Wochentage einstellen. › **Immer an** – die Verbindung ist immer aktiv. › **Immer aus** – die Verbindung ist immer inaktiv.

Eingabefeld	Beschreibung
Multi-WAN-Gewichtung	Legen Sie fest, welcher Anteil des Internet-Datenverkehrs über diese Verbindung geroutet wird, indem Sie einen Wert von `1` bis `256` eingeben. Je höher der eingegebene Wert, desto höher der Prozentanteil des über diese Verbindung gerouteten Datenverkehrs. Wird für alle Verbindungen der gleiche Wert eingestellt, wird der Datenverkehr gleichmäßig auf alle Verbindungen verteilt.
Desktop-Objekt	Wählen Sie ein Internetobjekt aus, das in Firewall-Regeln für diese Verbindung verwendet wird. Weitere Informationen finden Sie unter *Internetobjekte* auf Seite 119.

Im Tab **Failover** :

Eingabefeld	Beschreibung
Heartbeats	Legen Sie fest, wie der Status der Verbindung getestet wird, indem Sie Ping-Tests hinzufügen. Die Standardeinstellungen enthalten einen Ping-Test des Google-Servers (8.8.8.8). Klicken Sie auf **Hinzufügen**, um einen weiteren Test zur Liste hinzufügen. Weitere Informationen zur Konfiguration des Erreichbarkeitstests finden Sie unter *Heartbeat-Einstellungen* auf Seite 90. Sie können einzelne Einträge in der Liste bearbeiten oder löschen, indem Sie auf die entsprechende Schaltfläche neben einem Eintrag klicken. Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28.
Als Backup-Verbindung verwenden	Setzen Sie den Haken in diesem Kontrollkästchen, um die Verbindung als Backup-Internetverbindung zu konfigurieren.
Backup-Verbindungen	Wählen Sie eine beliebige Backup-Verbindung, die Sie der Verbindung zuweisen möchten und geben Sie ihre **Priorität** an. Falls die aktuelle Verbindung versagt, wechselt Ihre LANCOM R&S®Unified Firewall zur verfügbaren Backup-Verbindung mit der höchsten Priorität. Klicken Sie auf **Hinzufügen**, um die Backup-Verbindung zur Liste hinzuzufügen. Sie können einzelne Einträge in der Liste bearbeiten oder löschen, indem Sie auf die entsprechende Schaltfläche neben einem Eintrag klicken. Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28.

Heartbeat-Einstellungen

Mit den Einstellungen unter **Heartbeats** können Sie automatische Heartbeat-Tests für diese Verbindung konfigurieren. Das Bearbeitungsfenster enthält die folgenden Elemente:

Eingabefeld	Beschreibung
Typ	Wählen Sie aus der Drop-Down-Liste den Typ des Erreichbarkeitstest ein, den Sie durchführen möchten: › `ping` – Dieser Modus sendet Ping-Signale an das Ziel. › `tcp_probe` – Dieser Modus testet die Kapazität einer TCP-Verbindung.
Timeout	Geben Sie die Zeitüberschreitung für den Test in Sekunden ein.
Anzahl Versuche	Legen Sie die Gesamtanzahl der durchzuführenden Versuche fest.
Anzahl erfolgreicher Versuche	Legen Sie die Zahl der für einen erfolgreichen Heartbeat erforderlichen erfolgreichen Versuche fest.
Argumente	Legen Sie die im Test zu verwendenden Argumente, z. B. IP-Adressen, die gepingt werden, fest.

Klicken Sie auf **Testen**, um den Verbindungstest manuell durchzuführen. Klicken Sie auf **OK**, um die Einstellungen zu speichern und zum Bearbeitungsfenster **WWAN-Verbindung** zurückzukehren.

Die Schaltflächen rechts unten im Bearbeitungsfeld hängen davon ab, ob Sie eine neue WWAN-Verbindung hinzufügen oder eine bestehende Verbindung bearbeiten. Klicken Sie für eine neu konfigurierte Netzwerkverbindung auf **Erstellen**, um die Verbindung zur Liste der verfügbaren WWAN-Netzwerkverbindungen hinzuzufügen, oder auf **Abbrechen**, um die Erstellung einer neuen Netzwerkverbindung abzubrechen. Zum Bearbeiten einer vorhandenen WWAN-Verbindung klicken Sie auf **Speichern**, um die neu konfigurierte Verbindung zu speichern, oder auf **Zurücksetzen**, um Ihre Änderungen zu verwerfen. Sie können auf **Schließen** klicken, um das Bearbeitungsfenster zu schließen, solange keine Änderungen darin vorgenommen wurden.

Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

3.4.3.2 DHCP-Interfaces

Navigieren Sie zu **Netzwerk** > **DHCP-Interfaces**, um die DHCP-Einstellungen für verschiedene Interfaces auf Ihrer LANCOM R&S®Unified Firewall zu konfigurieren.

Eingabefeld	Beschreibung
I/0	Ein Schiebeschalter gibt an, ob der DHCP-Server oder das DHCP-Relay für dieses Interface derzeit aktiv (**I**) oder inaktiv (**0**) ist. Mit einem Klick auf den Schiebeschalter ändern Sie den Status dieser Option.
Modus	Wählen Sie aus, ob Sie für dieses Interface einen DHCP-Server oder ein DHCP-Relay einrichten möchten. Die übrigen Felder auf dem Bildschirm hängen vom gewählten Betriebsmodus ab.
Interface	Wählen Sie das Interface aus, für das Sie Einstellungen vornehmen wollen.

Einstellungen für DHCP-Server

Wenn Sie den DHCP-Server auf Ihrer LANCOM R&S®Unified Firewall betreiben, können Sie Clients im Netzwerk IP-Adressen zuweisen und diesen Clients weitere Konfigurationsparameter (Gateway, DNS-Server, NTP-Server etc.) übertragen. Alternativ ist es möglich, DHCP-Anfragen an einen bereits vorhandenen DHCP-Server in einem anderen Netzwerk zu übertragen.

Konfigurieren Sie für den DHCP-Server eines Interfaces die Einstellungen auf den folgenden Tabs:

Im Tab **Allgemein**:

Eingabefeld	Beschreibung
Netzwerk	Wählen Sie aus der Drop-Down-Liste das Subnetz aus, dessen IP-Adressen vom DHCP-Server verteilt werden. Mit der Auswahl des Subnetzes werden die Eingabefelder **IP-Bereich: Start** und **IP-Bereich: Ende** automatisch mit dem jeweiligen IP-Bereich ausgefüllt.
IP-Bereich: Start	Wenn die vorausgefüllte Start-IP-Adresse nicht Ihren Anforderungen entspricht, können Sie den Eintrag bearbeiten, um den Bereich festzulegen, aus dem IP-Adressen an die Clientcomputer verteilt werden.
IP-Bereich: Ende	Wenn die vorausgefüllte End-IP-Adresse nicht Ihren Anforderungen entspricht, können Sie den Eintrag bearbeiten, um den Bereich festzulegen, aus dem IP-Adressen an die Clientcomputer verteilt werden.
Gateway	Falls die vorausgefüllte Gateway-Adresse, die an den Client weitergegeben wird, nicht Ihren Anforderungen entspricht, können Sie den Eintrag bearbeiten. Die standardmäßige IP-Adresse des Gateways ist normalerweise die IP-Adresse Ihrer LANCOM R&S®Unified Firewall.
Bevorzugter DNS-Server / **Alternativer DNS-Server**	Falls Ihre LANCOM R&S®Unified Firewall keine Namensauflösung durchführt, geben Sie DNS-Server ein, die sich im Netzwerk oder im Internet befinden. Andernfalls bekommen die Clients die IP-Adressen von Ihrer LANCOM R&S®Unified Firewall als DNS-Server zugewiesen.

Eingabefeld	Beschreibung
Lease Time	Geben Sie den Zeitraum, innerhalb dessen ein Computer über eine gültige IP-Adresse verfügt, in Minuten an. Die standardmäßige Nutzungsdauer beträgt `60` Minuten.
Maximale Lease Time	Geben Sie die maximale Nutzungsdauer in Minuten ein.
Bevorzugter NTP-Server / **Alternativer NTP-Server**	Optional: Clients können NTP-Server nutzen, um die exakte Zeit festzustellen. Dies ist besonders für die Benutzerauthentifizierung über Windows-Server wichtig.
WINS-Server	Optional: Wenn Sie einen WINS-Server in Ihrem Netzwerk haben, teilen Sie dies über dieses Eingabefeld den Clients mit.
DNS-Such-Domänen	Geben Sie eine DNS-Suchdomain ein, die der DNS-Dienst nutzt, um Hostnamen aufzulösen, die nicht vollständig qualifizierte Domainnamen sind. Klicken Sie auf ⊕, um die DNS-Suchdomain zur Liste hinzufügen. Sie können einzelne Einträge in der Liste bearbeiten oder löschen, indem Sie auf die entsprechende Schaltfläche neben einem Eintrag klicken. Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28. Wenn Sie einen Eintrag bearbeiten, erscheint auf der rechten Seite des Eintrags ein Haken. Klicken Sie auf den Haken, um Ihre Änderungen zu übernehmen.

Im Tab **Erweitert**:

Eingabefeld	Beschreibung
Authoritative	Wenn aktiv, dann gilt die Firewall als maßgeblicher DHCP-Server, d. h. nur die von der Firewall vergebenen Adressen sind für dieses Netz-Segment gültig. Diese Option ist für Mobilgeräte relevant.
Adress-Konflikte verhindern	Setzen Sie den Haken in diesem Kontrollkästchen, um den DHCP-Server eine IP-Adresse anpingen zu lassen, um sicherzustellen, dass diese noch nicht in Verwendung ist, bevor Sie sie einem neuen Client zuweisen.
TFTP-Server-Adresse	Geben Sie die IP-Adresse zur Boot-Konfigurationsdatei an.
PXE-Dateiname	Geben Sie den Pfad und Dateinamen zur Boot-Konfigurationsdatei an.
Proxy-Konfigurations-Adresse	Geben Sie die URL zur Proxy-Konfiguration für die Konfiguration des Browsers ein.
Routen	Hier können Sie Routen, also die Angabe eines Netzwerks mit dazu gehörigem Gateway, an die Clients übermitteln.

Im Tab **Statische IP-Adressen**:

Eingabefeld	Beschreibung
MAC-Adresse / **IP-Adresse** / **Host-Name**	Legen Sie eine statische IP-Adresse für einen Host im Netzwerk fest, indem Sie die MAC-Adresse und IP-Adresse des Hosts eingeben. Zusätzlich können Sie den Hostnamen eingeben. Klicken Sie auf **Hinzufügen**, um die statische IP-Adresse zur Liste hinzuzufügen. Sie können einzelne Einträge in der Liste bearbeiten oder löschen, indem Sie auf die entsprechende Schaltfläche neben einem Eintrag klicken. Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28. Wenn Sie einen Eintrag bearbeiten, erscheint auf der rechten Seite des Eintrags ein Haken. Klicken Sie auf den Haken, um Ihre Änderungen zu übernehmen.

Eingabefeld	Beschreibung
Aus dem ARP-Cache hinzufügen	Wählen Sie aus der Drop-down-Liste die Adressen aus, die Sie aus dem ARP-Cache hinzufügen möchten.

Im Tab **Herstellerspezifische Optionen**:

Eingabefeld	Beschreibung
Hersteller-Kennung	Hier haben Sie die Möglichkeit herstellerspezifische Optionen (DHCP Option 43) zu konfigurieren. Die Kennung hat eine maximale Länge von 64 Zeichen und darf aus den Zeichen a-z, A-Z, 0-9 und _ bestehen. Dies wird zum Beispiel von der LANCOM Management Cloud genutzt, um LMC-Domain, Projekt-ID und Standort an andere LANCOM Geräte zum Beispiel Access Points zu verteilen.
Optionen	› **Name** Der Name der Option. Dieser hat eine maximale Länge von 64 Zeichen und darf aus den Zeichen a-z, A-Z, 0-9 und _ bestehen. › **Code** Nummer der Option, die an die DHCP-Clients übermittelt werden soll. Die Options-Nummer beschreibt die übermittelte Information, z. B. „43“ für herstellerspezifische Optionen. Eine Liste aller DHCP-Optionen finden Sie im *RFC 2132 – DHCP Options and BOOTP Vendor Extensions* der Internet Engineering Task Force (IETF). › **Wert** In diesem Feld definieren Sie den Inhalt der DHCP-Option. IP-Adressen werden in der üblichen Schreibweise von IPv4-Adressen angegeben, also z. B. als „123.123.123.100“, Integer-Typen werden als normale Dezimalzahlen eingetragen, Strings als einfacher Text. Mehrere Werte in einem Feld werden mit Kommas separiert, also z. B. „123.123.123.100, 123.123.123.200“. Die maximale Länge des Feldes beträgt 64 Zeichen.

Die Schaltflächen rechts unten im Bearbeitungsfeld hängen davon ab, ob Sie ein neues DHCP-Interface hinzufügen oder ein bestehendes bearbeiten. Klicken Sie für ein neues DHCP-Interface auf **Erstellen**, um das DHCP-Interface zur Liste der verfügbaren DHCP-Interfaces hinzuzufügen, oder auf **Abbrechen**, um Ihre Änderungen zu verwerfen. Zum Bearbeiten eines vorhandenen DHCP-Interfaces klicken Sie auf **Speichern**, um die Änderungen zu speichern, oder auf **Zurücksetzen**, um Ihre Änderungen zu verwerfen. Sie können auf **Schließen** klicken, um das Bearbeitungsfenster zu schließen, solange keine Änderungen darin vorgenommen wurden.

DHCP-Relay-Einstellungen

Ein DHCP-Relay leitet eingehende Anfragen an einen DHCP-Server an ein anderes Netzwerk weiter, da DHCP-Anfragen nicht geroutet werden können.

Eingabefeld	Beschreibung
DHCP-Server-IP-Adressen	Geben Sie die IP-Adresse des Servers ein, an den DHCP-Anfragen weitergeleitet werden.

Wenn Sie diese Einstellungen ändern, klicken Sie zum Speichern Ihrer Änderungen auf **Speichern** oder auf **Zurücksetzen**, um sie zu verwerfen. Klicken Sie ansonsten auf **Schließen**, um das Bearbeitungsfenster zu schließen.

Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

3.4.3.3 DNS-Einstellungen

Navigieren Sie zu **Netzwerk** > **DNS-Einstellungen**, um die DNS-Einstellungen auf Ihrer LANCOM R&S®Unified Firewall zu konfigurieren.

Normalerweise werden die DNS-Server-Einstellungen von der WAN-Verbindung vorgegeben. Sie sollten die DNS-Server-Einstellungen nur konfigurieren müssen, wenn Sie sie nicht über die WAN-Verbindung beziehen können.

Weiterführende Informationen finden Sie in den folgenden Abschnitten.

3.4.3.3.1 Allgemeine Einstellungen

Navigieren Sie zu **Netzwerk** > **DNS-Einstellungen** > **Allgemeine Einstellungen**, um die globalen DNS-Einstellungen auf Ihrer LANCOM R&S®Unified Firewall zu konfigurieren.

Normalerweise werden die DNS-Server-Einstellungen von der WAN-Verbindung vorgegeben. Sie sollten die DNS-Server-Einstellungen nur konfigurieren müssen, wenn Sie sie nicht über die WAN-Verbindung beziehen können.

Im Bearbeitungsfenster **Allgemeine Einstellungen** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Bezogenene Server	Hier werden die DNS-Server aufgelistet, die über DHCP- und PPP-Verbindungen o. ä. gelernt wurden.
DNS-Server	Diese Tabelle erlaubt die Konfiguration von 1 bis 2 DNS-Servern pro Zone. Eine Zone ist ein bestimmter DNS-Bereich wie „*.company.intern“. Die Standard-Zone „*“ ist die Zone, in die jede DNS-Adresse fällt, die in keine spezifischere Zone fällt. Die „AUTO“-Einstellung ist nur für die Standard-Zone gültig und kann dort dann nicht zusammen mit manuell eingetragenen IP-Adressen verwendet werden, sondern muss alleine stehen. Wird „AUTO“ eingestellt, dann werden an dieser Stelle die oben aufgelisteten, automatisch gelernten DNS-Server genutzt. Außerdem kann festgelegt werden, über welche Verbindung die eingetragenen Server erreicht werden können. Für den DNS-Server-Eintrag mit „AUTO“ als zuwiesenen Server, werden die **Bezogenene Server** verwendet. Wurde diesem Eintrag eine Verbindung zugewiesen, z. B. dsl, dann werden zwar alle bezogenen Server angezeigt, aber nur die Server verwendet, die über die Verbindung „dsl“ bezogen wurden. Wenn keine Verbindung für den „AUTO“-Eintrag gewählt wird, dann werden alle bezogenen Server verwendet. Die Tabelle kann – mit Ausnahme der Standard-Zone, die immer das letzte Element ist und sich auch nicht löschen lässt – vom Ihnen sortiert werden.
Multicast-DNS-Relay	Aktivieren Sie hier das Multicast-DNS-Relay. Multicast-DNS (mDNS) ist eine Alternative zum herkömmlichen DNS, um Hostnamen in (kleinen) Netzwerken aufzulösen. Dabei wird statt bei einem Server die Namensauflösung anzufragen, eine Anfrage per Multicast an alle durch die Multicast-Adresse erreichbaren Hosts gesendet und verarbeitet. Populäre Implementierungen von mDNS sind Bonjour (Apple) und Avahi (Linux), die das Vernetzen verschiedener Geräte (z.B. Netzwerkdrucker) ermöglichen, ohne vorher irgendwelche Konfigurationsarbeiten durchzuführen.

Wenn Sie diese Einstellungen ändern, klicken Sie zum Speichern Ihrer Änderungen auf **Speichern** oder auf **Zurücksetzen**, um sie zu verwerfen. Klicken Sie ansonsten auf **Schließen**, um das Bearbeitungsfenster zu schließen.

Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

3.4.3.3.2 Netzwerk-spezifische Einstellungen

Navigieren Sie zu **Netzwerk** > **DNS-Einstellungen** > **Netzwerk-spezifische Einstellungen**, um in Abhängigkeit des Quellnetzes von DNS-Anfragen alternative Konfigurationen vorzunehmen.

Im Bearbeitungsfenster **Netzwerk-spezifische Einstellungen** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
I/0	Ein Schiebeschalter gibt an, ob dieser Einstellungssatz derzeit aktiv (**I**) oder inaktiv (**0**) ist. Mit einem Klick auf den Schiebeschalter können Sie den Status ändern. Ein neuer Einstellungssatz ist standardmäßig aktiviert.
Name	Hier können Sie diesen Netzwerk-spezifischen Einstellungen einen Namen geben.
Quell-Netzwerke	Geben Sie hier eine Liste der Subnetze an, für die dieser Eintrag gelten soll. Zwischen unterschiedlichen Einstellungssätzen müssen die Namen eindeutig sein und die Quell-Netzwerke dürfen nicht mehrfach verwendet werden oder sich überschneiden.
DNS-Server	Diese Tabelle erlaubt die Konfiguration von 1 bis 2 DNS-Servern pro Zone. Eine Zone ist ein bestimmter DNS-Bereich wie „*.company.intern“. Anders als in den globalen Einstellungen ist es hier nicht zwingend notwendig, eine Einstellung für die Standard-Zone "*" zu treffen. Trifft eine DNS-Anfrage für einen Namen ein, der nicht innerhalb einer der hier eingestellten Zonen liegt, dann werden zur Namensauflösung die globalen Einstellungen verwendet. Außerdem kann festgelegt werden, über welche Verbindung die eingetragenen Server erreicht werden können. Die „AUTO“-Einstellung kann hier nicht verwendet werden, es müssen immer konkrete DNS-Server-Adressen angegeben werden.
Globale Einstellungen	Die aktuell gültigen globalen Einstellungen werden hier aufgeführt. Die Tabelle kann hier nicht bearbeitet werden und soll nur der Übersicht beim Erstellen von Netz-spezifischen Tabellen dienen.

Wenn Sie diese Einstellungen ändern, klicken Sie zum Speichern Ihrer Änderungen auf **Speichern** oder auf **Zurücksetzen**, um sie zu verwerfen. Klicken Sie ansonsten auf **Schließen**, um das Bearbeitungsfenster zu schließen.

Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

3.4.3.4 DynDNS-Accounts

Um sich aus einem externen Netzwerk, beispielsweise über eine VPN-Verbindung, mit Ihrer LANCOM R&S®Unified Firewall verbinden zu können, muss die IP-Adresse Ihres Geräts im Internet erkannt werden. Durch die Verwendung des dynamischen DNS („DynDNS“) erhält Ihre LANCOM R&S®Unified Firewall einen festen Hostnamen (z. B. `firmenname.dyndns.org`), selbst wenn es selbst keine feste öffentliche IP-Adresse hat. Dies ist möglich, indem die aktuelle IP-Adresse an einen DynDNS-Provider gesendet wird, der sie einem Domain-Namen zuordnet, sodass die Firewall über diesen Domain-Namen zugänglich ist. Falls sich die IP-Adresse zum Beispiel durch eine durch Ihren Internetprovider ausgelöste Verbindungstrennung ändert, wird die IP-Adresse erneut an den DynDNS-Provider gesendet. So wird sichergestellt, dass die dynamische DNS immer auf die aktuelle IP-Adresse verweist.

Um DynDNS auf Ihrer LANCOM R&S®Unified Firewall einzurichten, benötigen Sie einen konfigurierten DynDNS-Account bei einem DynDNS-Provider. Weitere Informationen zum dynamischen DNS und der Registrierung für das dynamische DNS-Verfahren finden Sie zum Beispiel unter *www.dyndns.org*.

Weiterführende Informationen zu DynDNS-Accounts finden Sie in den folgenden Abschnitten.

3.4.3.4.1 Übersicht DynDNS-Accounts

Navigieren Sie zu **Netzwerk** > **DynDNS-Konten**, um die Liste der derzeit im System angelegten DynDNS-Accounts in der Objektleiste anzuzeigen.

In der erweiterten Ansicht zeigen die Tabellenspalten den **Hostname** des DynDNS-Account, den **Server-Typ** des Accounts und den **Status** an. Mithilfe der Schaltflächen in der letzten Spalte können Sie die Einstellungen für einen vorhandenen

DynDNS-Account einsehen und anpassen, einen Account ausgehend von einer Kopie eines vorhandenen DynDNS-Accounts anlegen oder einen Account aus dem System löschen.

Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28.

3.4.3.4.2 Einstellungen zu DynDNS-Accounts

Unter **Netzwerk** > **DynDNS-Konten** können Sie einen neuen, benutzerdefinierten DynDNS-Account für generellen WAN-Zugang hinzufügen, oder einen vorhandenen bearbeiten.

Im Bearbeitungsfenster **DynDNS-Konto** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
I/0	Ein Schiebeschalter gibt an, ob der DynDNS-Account derzeit aktiv (**I**) oder inaktiv (**0**) ist. Mit einem Klick auf den Schiebeschalter können Sie den Status des DynDNS-Accounts ändern. Ein neuer DynDNS-Account ist standardmäßig aktiviert.
Internet-Verbindung	Wählen Sie aus der Drop-Down-Liste die von diesem Account verwendete Internetverbindung aus.
Server-Typ	Wählen Sie aus der Drop-Down-Liste der unterstützten DynDNS Dienste den Typ des zu verwendenden Servers aus.
Hostname	DynDNS-Dienste bieten einen Domain-Nameneintrag unter ihrer Aufsicht an. Folglich trägt ein registrierter Host immer das Suffix des Dienstanbieters (z. B. `IhrName.dynamicdns.org`). Tragen Sie den vollständigen Hostnamen in dieses Eingabefeld ein.
Benutzername	Geben Sie den Benutzernamen ein, mit dem Ihr Account beim DynDNS-Provider angemeldet werden soll.
Kennwort	Geben Sie das Passwort ein, mit dem Ihr Account beim DynDNS-Provider angemeldet werden soll.
Zeige Passwort	Optional: Setzen Sie den Haken in diesem Kontrollkästchen, um das Passwort zu verifizieren.
Benutzerdefinierte Server-Adresse	Optional: Geben Sie die Adresse des Servers ein, falls Sie für Ihren DynDNS-Provider eine abweichende Serveradresse festlegen müssen.
MX Record	Optional: Wenn Sie einen MX-Record einsetzen möchten, geben Sie dessen IP-Adresse oder Hostnamen ein.
Wildcards	Optional: Setzen Sie den Haken in diesem Kontrollkästchen, um die Verwendung von Wildcards in Hostnamen zu aktivieren, wenn Sie Subdomains Ihres DynDNS-Accounts verwenden möchten (z. B. werden mit: `*.IhrName.dynamicdns.org` alle Domains, die auf `yourname.dynamicdns.org` enden, aufgelöst).

Die Schaltflächen rechts unten im Bearbeitungsfeld hängen davon ab, ob Sie einen neuen DynDNS-Account hinzufügen oder einen bestehenden Account bearbeiten. Klicken Sie für einen neu konfigurierten Account auf **Erstellen**, um den Account zur Liste der verfügbaren DynDNS-Accounts hinzuzufügen, oder auf **Abbrechen**, um Ihre Änderungen zu verwerfen. Zum Bearbeiten eines vorhandenen Accounts klicken Sie auf **Speichern**, um den neu konfigurierten Account zu speichern, oder auf **Zurücksetzen**, um Ihre Änderungen zu verwerfen. Sie können auf **Schließen** klicken, um das Bearbeitungsfenster zu schließen, solange keine Änderungen darin vorgenommen wurden.

Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

3.4.3.5 Interfaces

Navigieren Sie zu **Netzwerk** > **Interfaces**, um Ethernet-, VLAN-, Bridge-, PPP- und WireGuard-Interfaces zu konfigurieren. In der Objektleiste erhalten Sie eine Übersicht aller aktuell im System angelegten Interfaces.

3.4.3.5.1 Gebündelte Interfaces

Nutzen Sie die Einstellungen unter **Gebündelte Interfaces**, um mehrere physische Ethernet-Interfaces zu einem logischen gebündelten Interface zu bündeln. Je nach Betriebsmodus bietet ein gebündeltes Interface die folgenden Vorteile:

- Lastverteilung – Ein gebündeltes Interface bietet eine größere Bandbreite, indem alle verbundenen Ethernet-Interfaces parallel zur Datenübertragung genutzt werden können.
- Hochverfügbarkeit – Falls ein Ethernet-Interface ausfällt, können auf den übrigen Ethernet-Interfaces weiterhin Daten empfangen und übertragen werden.

Sie können eine beliebige Anzahl an gebündelten Interfaces hinzufügen, solange Ethernet-Interfaces verfügbar sind, die nicht durch andere Interfaces oder in anderen Netzwerkverbindungen verwendet werden.

In den folgenden Abschnitten finden Sie weitere Informationen zu gebündelten Interfaces.

Übersicht gebündelte Interfaces

Navigieren Sie zu **Netzwerk** > **Interfaces** > **Gebündelte Interfaces**, um die Liste der derzeit im System angelegten gebündelten Interfaces in der Objektleiste anzuzeigen.

In der erweiterten Ansicht wird in der ersten Spalte der Tabelle der **Name** des gebündelten Interfaces angezeigt. Die Spalte **Status** zeigt einen der folgenden Statusindikatoren an.

- Grün – Das gebündelte Interface ist aktiv.
- Grau – Das gebündelte-Interface ist inaktiv.

Außerdem werden die **Ports** (d. h. die Ethernet-Interfaces), die dem gebündelten Interface zugewiesen sind, angezeigt. Mit den Schaltflächen in der letzten Spalte können Sie die Einstellungen für ein vorhandenes gebündeltes Interface ansehen und anpassen oder ein gebündeltes Interface aus dem System löschen.

Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28.

Einstellungen für gebündelte Interfaces

Nutzen Sie die Einstellungen unter **Gebündelte Interfaces**, um benutzerdefinierte, gebündelte Interfaces zu konfigurieren.

Unter **Netzwerk** > **Interfaces** > **Gebündelte Interfaces** können Sie ein neues gebündeltes Interface hinzufügen oder ein vorhandenes gebündeltes Interface bearbeiten.

Im Bearbeitungsfenster **Gebündeltes Interface** können Sie die folgenden Informationen einsehen und die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
I/0	Ein Schiebeschalter gibt an, ob das gebündelte Interface aktiv (**I**) oder inaktiv (**0**) ist. Mit einem Klick auf den Schiebeschalter können Sie den Status des gebündelten Interfaces ändern. Neu angelegte gebündelte Interfaces sind standardmäßig aktiviert.
Name	Zeigt den Namen des gebündelten Interfaces an. Der Name wird automatisch generiert. Gebündelte Interfaces werden in der Reihenfolge ihrer Erstellung nummeriert, angefangen mit `bond0`.
Hardware-Adresse	Zeigt die Hardwareadresse (MAC-Adresse) des gebündelten Interfaces an.
Verwendet von	Zeigt die Netzwerkkomponenten (z. B. Verbindungen, andere Interfaces, etc.) an, die das gebündelte Interface verwenden.
Modus	Wählen Sie aus der Drop-Down-Liste den Betriebsmodus des gebündelten Interfaces aus und legen Sie fest, wie die Interfaces verbunden werden sollen. Die Option ist standardmäßig auf `IEEE 802.1AX (LACP, Direktverbindung)` gesetzt, Sie können die Einstellungen jedoch je nach Bedarf auf einen der anderen Werte setzen:

Eingabefeld	Beschreibung
	› `Balance – Round-Robin (Trunk, Direktverbindung)` – Dieser Modus bietet Lastverteilung und Hochverfügbarkeit. Pakete werden nacheinander vom ersten verfügbaren verbundenen Ethernet-Interface bis zum letzten übertragen, daraufhin wird wieder mit dem ersten verbundenen Ethernet-Interface begonnen. › `Active-Backup (Bridge)` – Dieser Modus bietet nur Hochverfügbarkeit. Daten werden nur vom aktiven Ethernet-Interface (d. h. dem ersten Ethernet-Interface auf der Liste) übertragen und empfangen, solange dieses nicht ausfällt. Fällt das erste Ethernet-Interface aus, wird das nächste Ethernet-Interface auf der Liste zum Übertragen und Empfangen der Daten genutzt. Ist das ursprüngliche Interface wieder verfügbar, verbleibt die Verbindung weiterhin auf dem Interface, welches die Kommunikation übernommen hat. › `Balance – XOR (Trunk, Direktverbindung)` – Dieser Modus bietet Lastverteilung und Hochverfügbarkeit. Pakete werden auf allen Ethernet-Interfaces übertragen. Ein einfacher Algorithmus (Layer2+3 XOR) wird angewandt, um festzulegen, welches Ethernet-Interface zur Datenübertragung genutzt wird. › `Broadcast (Trunk, Direktverbindung)` – Dieser Modus bietet nur Hochverfügbarkeit. Daten werden auf allen Ethernet-Interfaces gleichzeitig übertragen und empfangen. › `IEEE 802.1AX (LACP, Direktverbindung)` – Dieser Modus bietet Lastverteilung und Hochverfügbarkeit nach der LACP-Norm (Link Aggregation Control Protocol). Pakete werden auf allen Ethernet-Interfaces übertragen. Ein einfacher Algorithmus (Layer2+3 XOR) wird angewandt, um festzulegen, welches Ethernet-Interface zur Datenübertragung genutzt wird. › `Balance – TLB (Bridge)` – Dieser Modus bietet Lastverteilung und Hochverfügbarkeit. Zusätzlich zum einfachen Auswahlalgorithmus (Layer2+3 XOR) wird die aktuelle Last des Ethernet-Interfaces in die Entscheidung, welches Ethernet-Interface zur Datenübertragung genutzt wird, miteinbezogen. › `Balance – ALB (Bridge)` – Dieser Modus bietet Lastverteilung und Hochverfügbarkeit. Daten werden über ARP-Aushandlung empfangen. Zusätzlich zum einfachen Auswahlalgorithmus (Layer2+3 XOR) wird die aktuelle Last des Ethernet-Interfaces in die Entscheidung, welches Ethernet-Interface zur Datenübertragung genutzt wird, miteinbezogen.
Ports	Fügen Sie die Interfaces hinzu, die Sie zu einem logischen Link verbinden möchten, indem Sie in das Eingabefeld klicken. Sie können beliebig viele verfügbare Ethernet-Interfaces auswählen. Sie können nur Ethernet-Interfaces auswählen, die nicht von anderen Interfaces oder in anderen Netzwerkverbindungen verwendet werden. Die ausgewählten Ethernet-Interfaces werden in einer Tabelle unten im Bearbeitungsfenster angezeigt. Um ein Element aus dem Eingabefeld zu entfernen, klicken Sie auf ✖ auf der linken Seite des Eintrags.
MTU	Legen Sie die maximale Paketgröße in Bytes fest. Die maximale Übertragungseinheit kann jede ganze Zahl zwischen `64` und `16384` sein.

Die Schaltflächen rechts unten im Bearbeitungsfeld hängen davon ab, ob Sie ein neues gebündeltes Interface hinzufügen oder ein bestehendes bearbeiten. Klicken Sie für ein neu konfiguriertes gebündeltes Interface auf **Erstellen**, um das gebündelte Interface zur Liste der verfügbaren gebündelten Interfaces hinzuzufügen, oder auf **Abbrechen**, um Ihre Änderungen zu verwerfen. Zum Bearbeiten eines vorhandenen gebündelten Interfaces klicken Sie auf **Speichern**, um das neu konfigurierte gebündelte Interface zu speichern, oder auf **Zurücksetzen**, um Ihre Änderungen zu verwerfen. Sie können auf **Schließen** klicken, um das Bearbeitungsfenster zu schließen, solange keine Änderungen darin vorgenommen wurden.

Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

3.4.3.5.2 Bridge-Interfaces

Nutzen Sie die Einstellungen unter **Bridge Interfaces**, um zwei Interfaces und deren Netzwerke auf Layer 2 zu verbinden, sodass sie eine gemeinsame Broadcast-Domäne ergeben.

In den folgenden Abschnitten finden Sie weitere Informationen zu Bridge-Interfaces.

Übersicht Bridge-Interfaces

Navigieren Sie zu **Netzwerk** > **Interfaces** > **Bridge Interfaces**, um die Liste der derzeit im System angelegten Bridge-Interfaces in der Objektleiste anzuzeigen.

In der erweiterten Ansicht wird in der ersten Spalte der Tabelle der **Name** des Bridge-Interfaces angezeigt. Die Spalte **Status** zeigt einen der folgenden Statusindikatoren an.

- Grün – Das Bridge-Interface ist aktiviert.
- Orange – Das Bridge-Interface ist deaktiviert.

Außerdem werden die **Ports**, die dem Bridge-Interface zugewiesen sind, angezeigt. Mit den Schaltflächen in der letzten Spalte können Sie die Einstellungen für ein vorhandenes Bridge-Interface einsehen und anpassen, ein neues Bridge-Interface ausgehend von einer Kopie eines vorhandenen Bridge-Interfaces anlegen, oder ein Bridge-Interface aus dem System löschen.

Sollen mehrere VLANs in einem Bridge-Interface verwendet werden, ist es erforderlich, die VLANs zuerst mit den Ethernet-Ports in VLAN-Interfaces zusammenzufassen. Die VLAN-Interfaces können anschließend in einem Bridge-Interface hinterlegt werden.

Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28.

Einstellungen zu Bridge-Interfaces

Nutzen Sie die Einstellungen unter **Bridge Interfaces**, um benutzerdefinierte Bridge-Interfaces zu konfigurieren.

Unter **Netzwerk** > **Interfaces** > **Bridge Interfaces** können Sie ein neues Bridge-Interface hinzufügen, oder ein vorhandenes bearbeiten.

Im Bearbeitungsfenster **Bridge Interface** können Sie die folgenden Informationen einsehen und die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
I/0	Ein Schiebeschalter gibt an, ob das Bridge-Interface aktiv (**I**) oder inaktiv (**0**) ist. Mit einem Klick auf den Schiebeschalter können Sie den Status des Bridge-Interfaces ändern. Neu angelegte Bridge-Interfaces sind standardmäßig aktiviert.
Name	Zeigt den Namen des Bridge-Interfaces an. Der Name wird automatisch generiert. Bridges werden in der Reihenfolge ihrer Erstellung nummeriert, angefangen mit `br0`.
Hardware-Adresse	Zeigt die Hardwareadresse (MAC-Adresse) des Bridge-Interfaces an.
Verwendet von	Zeigt die Netzwerkkomponenten (z. B. Verbindungen, andere Interfaces etc.) an, die das Bridge-Interface verwenden.
Ports	Fügen Sie die Ports hinzu, die das Bridge-Interface zusammenschließt, indem Sie in das Eingabefeld klicken. Sie können beliebig viele VLAN-Interfaces oder andere Bridge-Interfaces auswählen. Um ein Element aus dem Eingabefeld zu entfernen, klicken Sie auf ✖ auf der linken Seite des Eintrags. Die ausgewählten Ports werden in einer Tabelle unten im Bearbeitungsfenster angezeigt.

Eingabefeld	Beschreibung
	Bridges können nicht mit Interfaces erstellt werden, die bereits als Teil einer anderen Bridge verwendet werden.
MTU	Legen Sie die maximale Paketgröße in Bytes fest. Die maximale Übertragungseinheit kann jede ganze Zahl zwischen `64` und `16384` sein.
Spanning Tree Protocol	Optional: Setzen Sie den Haken in diesem Kontrollkästchen, um das Spanning Tree Protocol zu aktivieren. Dieses ist standardmäßig deaktiviert.
Priorität	Nur verfügbar, wenn **Spanning Tree Protocol** aktiviert ist: Legen Sie die Priorität der Bridge fest. Geben Sie ein Vielfaches von `4096` im Bereich von `4096` bis `61440` ein.
Hello-Intervall	Nur verfügbar, wenn **Spanning Tree Protocol** aktiviert ist: Legen Sie das Hello-Intervall in Sekunden fest. Geben Sie eine beliebige ganze Zahl zwischen `1` und `10` ein.
Ports	Diese Tabelle zeigt die für das Bridge-Interface ausgewählten Ports an. Wenn **Spanning Tree Protocol** aktiviert ist, können Sie mit den Schaltflächen auf der rechten Seite jedes Eintrags die **Priorität** und **Kosten** des jeweiligen Ports festlegen, oder den Port aus dem Bridge-Interface entfernen.

Die Schaltflächen rechts unten im Bearbeitungsfeld hängen davon ab, ob Sie ein neues Interface hinzufügen oder ein bestehendes bearbeiten. Klicken Sie für ein neu konfiguriertes Bridge-Interface auf **Erstellen**, um es zur Liste der verfügbaren Bridge-Interfaces hinzuzufügen, oder auf **Abbrechen**, um Ihre Änderungen zu verwerfen. Zum Bearbeiten eines vorhandenen Bridge-Interfaces klicken Sie auf **Speichern**, um das neu konfigurierte Bridge-Interface zu speichern, oder auf **Zurücksetzen**, um Ihre Änderungen zu verwerfen. Sie können auf **Schließen** klicken, um das Bearbeitungsfenster zu schließen, solange keine Änderungen darin vorgenommen wurden.

Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

3.4.3.5.3 Ethernet-Interfaces

Die physischen **Ethernet-Interfaces** erhalten die folgenden standardmäßigen IP-Adressen: `192.168.X.254/24` (`X` steht für die Nummer der Interfaces, die IP-Adresse von eth0 ist also `192.168.0.254`).

In den folgenden Abschnitten finden Sie detailliertere Informationen zu Ethernet-Interfaces.

Übersicht Ethernet-Interfaces

Navigieren Sie zu **Netzwerk** > **Interfaces** > **Ethernet-Interfaces**, um die Liste der derzeit im System angelegten Ethernet-Interfaces in der Objektleiste anzuzeigen.

In der erweiterten Ansicht wird in der ersten Spalte der Tabelle der **Name** des Ethernet-Interfaces angezeigt. Die Spalte **Status** zeigt einen der folgenden Statusindikatoren an.

- Grün – Das Ethernet-Interface ist aktiv.
- Grau – Das Ethernet-Interface ist inaktiv.

Außerdem wird die **Geschwindigkeit** des Ethernet-Interfaces angezeigt. Mit der Schaltfläche in der letzten Spalte können Sie die Einstellungen für ein vorhandenes Ethernet-Interface einsehen und bearbeiten.

Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28.

Einstellungen zu Ethernet-Interfaces

Unter **Netzwerk** > **Interfaces** > **Ethernet-Interfaces** können Sie weiterführende Informationen zu den verfügbaren Ethernet-Interfaces anzeigen und die entsprechenden Einstellungen anpassen.

Im Bearbeitungsfenster **Ethernet-Interface** können Sie die folgenden Informationen einsehen und die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Name	Zeigt den Namen des Ethernet-Interfaces an, z. B. `eth0`.
Beschreibung	Zeigt eine kurze Beschreibung des Ethernet-Interfaces an.
Hardware-Adresse	Zeigt die Hardwareadresse (MAC-Adresse) des Ethernet-Interfaces an.
Verwendet von	Zeigt die Verbindung an, die zurzeit das Ethernet-Interface verwendet.
Status	Zeigt den Status des Ethernet-Interfaces an. Der Status kann einer der folgenden sein: › `aktiv` – Das Ethernet-Interface ist aktiviert. › `abgeschaltet` – Das Ethernet-Interface ist deaktiviert.
Geschwindigkeit	Gibt die Geschwindigkeit (z. B. in Gbit/s) des Ethernet-Interfaces an.
Duplex	Zeigt den Duplex-Modus des Ethernet-Interfaces an, z. B. `full`.
Typ	Zeigt den mit dem Interface verbundenen Kabeltyp an, z. B. `twisted pair`.
I/0	Ein Schiebeschalter gibt an, ob der Ethernet-Interface-Link aktiv (**I**) oder inaktiv (**0**) ist. Mit einem Klick auf den Schiebeschalter können Sie den Status des Ethernet-Interface-Links ändern.
MTU	Legen Sie die maximale Paketgröße in Bytes fest. Die maximale Übertragungseinheit kann jede ganze Zahl zwischen `64` und `16384` sein.

Wenn Sie diese Einstellungen ändern, klicken Sie zum Speichern Ihrer Änderungen auf **Speichern** oder auf **Zurücksetzen**, um sie zu verwerfen. Klicken Sie ansonsten auf **Schließen**, um das Bearbeitungsfenster zu schließen.

Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

3.4.3.5.4 PPP-Interfaces

Mit den Einstellungen unter **PPP-Interfaces** können Sie Interfaces unter Verwendung des Point-to-Point-Protokolls erstellen.

In den folgenden Abschnitten finden Sie detailliertere Informationen zu PPP-Interfaces.

Übersicht PPP-Interfaces

Navigieren Sie zu **Netzwerk** > **Interfaces** > **PPP-Interfaces**, um die Liste der derzeit im System angelegten PPP-Interfaces in der Objektleiste anzuzeigen.

In der erweiterten Ansicht wird in der ersten Tabellenspalte der **Name** des PPP-Interfaces angezeigt. Die Spalte **Status** zeigt einen der folgenden Statusindikatoren an.

› Grün – das PPP-Interface ist aktiviert.

› Orange – das PPP-Interface ist deaktiviert.

Außerdem wird das **Haupt-Interface** angezeigt, zu dem das PPP-Interface gehört. Mit den Schaltflächen in der letzten Spalte können Sie die Einstellungen für ein vorhandenes PPP-Interface einsehen und anpassen, ein neues PPP-Interface ausgehend von einer Kopie eines vorhandenen PPP Interfaces anlegen, oder ein PPP-Interface aus dem System löschen.

Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28.

Einstellungen zu PPP-Interfaces

Nutzen Sie die Einstellungen unter **PPP-Interfaces**, um benutzerdefinierte PPP-Interfaces zu konfigurieren.

Unter **Netzwerk** > **Interfaces** > **PPP-Interfaces** können Sie ein neues PPP-Interface hinzufügen, oder ein bestehendes bearbeiten.

Im Bearbeitungsfenster **PPP-Interfaces** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
I/0	Ein Schiebeschalter gibt an, ob das PPP-Interface aktiv (**I**) oder inaktiv (**0**) ist. Mit einem Klick auf den Schiebeschalter können Sie den Status des PPP-Interfaces ändern. Neu angelegte PPP-Interfaces sind standardmäßig aktiviert.
Haupt-Interface	Wählen Sie aus der Drop-Down-Liste das Ethernet-, VLAN- oder Bridge-Interface aus, das dem PPP-Interface als Gegenstelle zugeordnet wird.
LCP Echo-Intervall	Legen Sie das Intervall in Sekunden fest, in dem Ihre LANCOM R&S®Unified Firewall Echo-Anfragen an die Gegenstelle sendet, indem Sie einen ganzzahligen Wert von `1` bis `1800` eingeben.
LCP Echo-Fehlerzahl	Legen Sie die Zahl der unbeantworteten LCP-Echo-Anfragen fest, nach denen die Gegenstelle als nicht erreichbar betrachtet wird, indem Sie einen ganzzahligen Wert von `0` bis `64`eingeben. Wenn Sie `0`eingeben, werden unbeantwortete Anfragen ignoriert.
MTU	Legen Sie die maximale Paketgröße in Bytes fest. Die maximale Übertragungseinheit kann jede ganze Zahl zwischen `64` und `16384` sein.
MRU	Geben Sie die maximale Empfangseinheit an, indem Sie einen ganzzahligen Wert zwischen `128` und `16384` eingeben.

Die Schaltflächen rechts unten im Bearbeitungsfeld hängen davon ab, ob Sie ein neues PPP-Interface hinzufügen oder ein bestehendes bearbeiten. Klicken Sie für ein neu konfiguriertes PPP-Interface auf **Erstellen**, um es zur Liste der verfügbaren PPP-Interfaces hinzuzufügen, oder auf **Abbrechen**, um Ihre Änderungen zu verwerfen. Zum Bearbeiten eines vorhandenen PPP-Interfaces klicken Sie auf **Speichern**, um das neu konfigurierte Interface zu speichern, oder auf **Zurücksetzen**, um Ihre Änderungen zu verwerfen. Sie können auf **Schließen** klicken, um das Bearbeitungsfenster zu schließen, solange keine Änderungen darin vorgenommen wurden.

Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

3.4.3.5.5 VLAN-Interfaces

Mit den Einstellungen unter **VLAN-Interfaces** können Sie dem Datenverkehr eines bestimmten Interfaces benutzerdefinierte Tags zuweisen.

Dadurch können Sie „virtual interfaces" anlegen, die es Ihnen ermöglichen, mehrere logische Netzwerkzonen auf ein physisches Interface zu legen. Wenn ein VLAN-Tag einem Netzwerk-Interface zugeordnet wird, wird der Tag an alle ausgehenden Pakete angefügt, die über dieses virtuelle Interface versandt werden und von denjenigen eingehenden Paketen entfernt, die über dieses VLAN empfangen werden. Mit jedem Netzwerk-Interface können mehrere VLANs verknüpft werden. Pakete mit verschiedenen Tags können verarbeitet und den entsprechenden Interfaces zugeordnet werden.

In den folgenden Abschnitten finden Sie detailliertere Informationen zu VLAN-Interfaces.

Übersicht VLAN-Interfaces

Navigieren Sie zu **Netzwerk** > **Interfaces** > **VLAN-Interfaces**, um die Liste der derzeit im System angelegten VLAN-Interfaces in der Objektleiste anzuzeigen.

In der erweiterten Ansicht wird in der ersten Tabellenspalte der **Name** des VLAN-Interfaces angezeigt. Die Spalte **Status** zeigt einen der folgenden Statusindikatoren an.

- Grün – das VLAN-Interface ist aktiviert.
- Orange – das VLAN-Interface ist deaktiviert.

Außerdem werden das zum VLAN gehörige **Haupt-Interface** und der **VLAN-Tag** angezeigt. Mithilfe der Schaltflächen in der letzten Spalte können Sie die Einstellungen für ein vorhandenes VLAN einsehen und anpassen, ein neues VLAN-Interface ausgehend von einer Kopie eines vorhandenen anlegen, oder ein VLAN-Interface aus dem System löschen.

Sollen mehrere VLANs in einem Bridge-Interface verwendet werden, ist es erforderlich, die VLANs zuerst mit den Ethernet-Ports in VLAN-Interfaces zusammenzufassen. Die VLAN-Interfaces können anschließend in einem Bridge-Interface hinterlegt werden.

Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28.

Einstellungen zu VLAN-Interfaces

Mit den Einstellungen unter **VLAN-Interfaces** können Sie benutzerdefinierte Tags für das Virtual Local Area Network (virtuelles lokales Netzwerk) konfigurieren, die dem gesamten Traffic an einem bestimmten Interface hinzugefügt werden.

Unter **Netzwerk** > **Interfaces** > **VLAN-Interfaces** können Sie ein neues VLAN-Interface hinzufügen oder ein vorhandenes bearbeiten.

Im Bearbeitungsfenster **VLAN-Interface** können Sie die folgenden Informationen einsehen und die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
I/0	Ein Schiebeschalter gibt an, ob das VLAN-Interface aktiv (**I**) oder inaktiv (**0**) ist. Mit einem Klick auf den Schiebeschalter können Sie den Status des VLAN-Interfaces ändern. Neu angelegte VLAN-Interfaces sind standardmäßig aktiviert.
Name	Zeigt den Namen des VLAN-Interfaces an. Der Name wird automatisch generiert und enthält den **VLAN-Tag** und das zugrundeliegende **Haupt-Interface**.
Hardware-Adresse	Nur für bearbeitete VLAN-Interfaces: Zeigt die Hardwareadresse (MAC-Adresse) des zugrundeliegenden **Haupt-Interface** an.
Verwendet von	Zeigt die Netzwerkkomponenten (z. B. Verbindungen, andere Interfaces etc.) an, die das VLAN-Interface verwenden.
Haupt-Interface	Nur für bearbeitete VLAN-Interfaces: Wählen Sie aus der Drop-Down-Liste das Ethernet- oder Bridge-Interface aus, mit dem das VLAN-Interface verknüpft ist. Nur für bearbeitete VLAN-Interfaces: Zeigt das Ethernet- oder Bridge-Interface an, mit dem das VLAN-Interface verknüpft ist.
VLAN-Tag	Geben Sie den Textinhalt des VLAN-Tag ein. Der Tag kann jeden ganzzahligen Wert zwischen `1` und `4094` enthalten.
MTU	Legen Sie die maximale Paketgröße in Bytes fest. Die maximale Übertragungseinheit ist auf die maximale Übertragungseinheit des zugrundeliegenden Master-Interfaces beschränkt. Aufgrund einer Beschränkung des Systemkerns ist die maximale Übertragungseinheit auf die maximale Übertragungseinheit des zugrundeliegenden Interfaces beschränkt.

Die Schaltflächen rechts unten im Bearbeitungsfeld hängen davon ab, ob Sie ein neues VLAN-Interface hinzufügen oder ein bestehendes VLAN bearbeiten. Klicken Sie für ein neu konfiguriertes VLAN-Interface auf **Erstellen**, um es zur Liste der verfügbaren VLAN-Interfaces hinzuzufügen, oder auf **Abbrechen**, um Ihre Änderungen zu verwerfen. Zum Bearbeiten eines vorhandenen VLAN-Interfaces klicken Sie auf **Speichern**, um das neu konfigurierte VLAN-Interface zu speichern, oder auf **Zurücksetzen**, um Ihre Änderungen zu verwerfen. Sie können auf **Schließen** klicken, um das Bearbeitungsfenster zu schließen, solange keine Änderungen darin vorgenommen wurden.

Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

3.4.3.5.6 WireGuard-Interfaces

Mit den Einstellungen unter **WireGuard-Interfaces** können Sie per WireGuard gesicherte Interfaces einrichten.

In den folgenden Abschnitten finden Sie detailliertere Informationen zu WireGuard-Interfaces.

Einstellungen zu WireGuard-Interfaces

Unter **Netzwerk** > **Interfaces** > **WireGuard-Interfaces** können Sie ein neues WireGuard-Interface hinzufügen oder ein vorhandenes bearbeiten.

Im Bearbeitungsfenster **WireGuard-Interface** können Sie die folgenden Informationen einsehen und die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
I/0	Ein Schiebeschalter gibt an, ob das WireGuard-Interface aktiv (**I**) oder inaktiv (**0**) ist. Mit einem Klick auf den Schiebeschalter können Sie den Status des WireGuard-Interfaces ändern. Neu angelegte WireGuard-Interfaces sind standardmäßig aktiviert.
Name	Zeigt den Namen des WireGuard-Interfaces an. Der Name wird automatisch nach dem Schema wg<*x*> generiert.
Verwendet von	Zeigt die Netzwerkkomponenten (z. B. Verbindungen, andere Interfaces etc.) an, die das WireGuard-Interface verwenden.
Status	Zeigt den aktuellen Status des WireGuard-Interfaces an.
MTU	Legen Sie die maximale Paketgröße in Bytes fest.

Die Schaltflächen rechts unten im Bearbeitungsfeld hängen davon ab, ob Sie ein neues WireGuard-Interface hinzufügen oder ein bestehendes WireGuard-Interface bearbeiten. Klicken Sie für ein neu konfiguriertes WireGuard-Interface auf **Erstellen**, um es zur Liste der verfügbaren WireGuard-Interfaces hinzuzufügen, oder auf **Abbrechen**, um Ihre Änderungen zu verwerfen. Zum Bearbeiten eines vorhandenen WireGuard-Interfaces klicken Sie auf **Speichern**, um das neu konfigurierte WireGuard-Interface zu speichern, oder auf **Zurücksetzen**, um Ihre Änderungen zu verwerfen. Sie können auf **Schließen** klicken, um das Bearbeitungsfenster zu schließen, solange keine Änderungen darin vorgenommen wurden.

Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

3.4.3.5.7 WWAN-Interfaces

Mit den Einstellungen unter **WWAN-Interfaces** können Sie ein ggf. vorhandenes WWAN-Interface wie z. B. eine Mobilfunkverbindung aktivieren bzw. deaktivieren.

In den folgenden Abschnitten finden Sie detailliertere Informationen zu WWAN-Interfaces.

Übersicht WWAN-Interfaces

Navigieren Sie zu **Netzwerk** > **Interfaces** > **WWAN-Interfaces**, um die Liste der derzeit im System angelegten WWAN-Interfaces in der Objektleiste anzuzeigen.

In der ersten Tabellenspalte wird der **Name** des WWAN-Interfaces angezeigt. Die nächste Spalte zeigt die aktuelle Signalstärke an.

Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28.

Einstellungen zu WWAN-Interfaces

Unter **Netzwerk** > **Interfaces** > **WWAN-Interfaces** können Sie ein WWAN-Interface aktivieren bzw. deaktivieren und Informationen zum Interface einsehen.

Im Bearbeitungsfenster **WWAN-Interface** können Sie die folgenden Informationen einsehen und die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
I/0	Ein Schiebeschalter gibt an, ob das WWAN-Interface aktiv (**I**) oder inaktiv (**0**) ist. Mit einem Klick auf den Schiebeschalter können Sie den Status des WWAN-Interfaces ändern.
Name	Zeigt den Namen des WWAN-Interfaces an.
IMEI	Die International Mobile Equipment Identity (IMEI) ist eine eindeutige 15-stellige Seriennummer, anhand derer Mobiltelefone bzw. vergleichbare Geräte weltweit eindeutig identifiziert werden können.
Verwendet von	Verbindung, die dieses Interface verwendet.
Status	Status der Verbindung.
Signal	Signalstärke der Verbindung.
Funk-Bänder	Verwendete Funk-Bänder.
RSSI	Received Signal Strength Indicator
RSRP	Reference Signal Received Power
RSRQ	Reference Signal Received Quality
SNR	Signal to Noise Ratio
MTU	Die Maximum Transmission Unit (MTU) beschreibt die maximale Größe der Nutzdaten, die in einem einzelnen Datenpaket übertragen werden können.
Verbunden mit Heimat-Netz	Zeigt den Roaming-Status der Verbindung an bzw. ob die Verbindung gerade in das Heimat-Netz besteht, oder nicht.

Klicken Sie auf **Netzwerk-Scan**, um eine Liste der unterschiedlichen Funkzellen abrufen, deren Signale empfangen werden können. Das erzeugen dieser Liste kann einige Minuten in Anspruch nehmen. Je mehr Daten über das Modul zum Zeitpunkt des Scans übertragen werden, desto langsamer ist der Scan. Ein Scan lässt sich nicht abbrechen und während des Scans ist keine Interaktion mit dem Webclient der Firewall möglich. Vor Beginn des Scans erscheint noch eine entsprechende Warnung mit Möglichkeit zum Abbruch.

Zum Bearbeiten eines vorhandenen WWAN-Interfaces klicken Sie auf **Speichern**, um das neu konfigurierte WWAN-Interface zu speichern, oder auf **Zurücksetzen**, um Ihre Änderungen zu verwerfen. Sie können auf **Schließen** klicken, um das Bearbeitungsfenster zu schließen, solange keine Änderungen darin vorgenommen wurden.

Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

3.4.3.6 Traffic Shaping

Unter **Netzwerk** > **Traffic Shaping** können Sie Einstellungen zu Ihrem IP-Traffic vornehmen. Dabei wird ein weitergehenderer Ansatz verfolgt, als nur Quality-of-Service-Werte zuzuweisen. Hier definieren Sie Traffic-Gruppen, über die Regeln für diese Traffic-Gruppe an diversen Stellen in Ihrer LANCOM R&S®Unified Firewall angewendet werden:

- Über eine Desktop-Verbindung: Dies gilt für den gesamten verschlüsselten Tunnel-Traffic, wobei einzelne Trafficarten innerhalb des Tunnels nicht berücksichtigt werden. Die Zuordnung zu einer Gruppe kann für die ganze Verbindung oder auch nur für einzelne Regeln der Verbindung erfolgen.
- Über einen IPsec-Tunnel: Dies betrifft den verschlüsselten Datenverkehr über diesen Tunnel, ohne Berücksichtigung evtl. verschiedenartiger unverschlüsselter Daten innerhalb des Tunnels.
- Über ein App-Routing-Profil: Betrifft den Traffic, der einer der im Profil eingestellten Applikationen und einer Desktop-Verbindung entspricht, auf der dieses Profil verwendet wird.

Die Gruppen können in Regeln verwendet werden, um zu bestimmen, wie ihnen entsprechender Datenverkehr priorisiert werden soll und welche Bandbreiten-Limits und -Garantien gelten. Dazu werden diese Regeln jeweils pro Interface in **Shaping-Konfigurationen** zusammengefasst. Eine solche Shaping-Konfiguration

- gilt für ein bestimmtes WAN-Interface oder den inneren Traffic zu einem Routen-basierten IPsec-Tunnel,

- legt fest, welche Bandbreiten (Upload / Download) über das gewählte Interface oder den gewählten Tunnel insgesamt zur Verfügung stehen und
- hält, separat für Upload und Download, je eine Liste von anzuwendenden Shaping-Regeln. Dies ist für eine Traffic-Gruppe die Priorität, garantierte Bandbreite und maximale Bandbreite. Für eingehende Regeln können diese Einstellungen auch für ein Netzwerk-Interface statt für eine Traffic-Gruppe vorgenommen werden.

An allen Stellen, an denen Traffic einer Gruppe zugeordnet werden kann (Desktop-Verbindung, IPsec-Tunnel oder App-Routing-Profil), kann optional auch ein DSCP-Wert (Quality of Service) für ausgehende Pakete festgelegt werden. Damit kann anderen Geräten entlang der Paket-Route innerhalb sowie auch außerhalb des Netzwerks der LANCOM R&S®Unified Firewall ein Anhaltspunkt zur Paket-Priorisierung mitgeteilt werden. Wird keine Angabe gemacht, dann bleibt der entsprechende IP-Paket-Header unberührt und behält seinen alten Wert.

3.4.3.6.1 Shaping-Konfigurationen

Navigieren Sie zu **Netzwerk** > **Traffic Shaping** > **Shaping-Konfigurationen**, um Ihre Shaping-Konfigurationen zu verwalten. In einer solchen Konfiguration können für ein WAN-Interface oder den Traffic innerhalb eines IPsec-Tunnels die nötigen Rahmenparameter sowie einzelne Shaping-Regeln für eingehenden und ausgehenden Datenverkehr festgelegt werden. Die Shaping-Regeln legen fest, wie der Traffic, der zu den verschiedenen Traffic-Gruppen gehört, für das angegebene Interface bzw. den Tunnel und die jeweilige Richtung priorisiert werden soll.

Traffic, der keiner der eingehenden Regeln entspricht, hat die niedrigste Priorität und es wird keine Bandbreite garantiert. Die Summe der garantierten Bandbreiten aller Regeln einer Übertragungsrichtung darf die maximale Interface-Bandbreite für diese Übertragungsrichtung nicht überschreiten. Dasselbe gilt für die in einer Regel festgelegte maximale Bandbreite.

Im Bearbeitungsfenster **Shaping-Konfiguration** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
I/0	Ein Schiebeschalter gibt an, ob diese Shaping-Konfiguration derzeit aktiv (**I**) oder inaktiv (**0**) ist. Mit einem Klick auf den Schiebeschalter ändern Sie den Status. ⓘ Pro Interface bzw. Tunnel kann es nur eine aktive Shaping-Konfiguration geben.
Interface	Wählen Sie ein Interface aus.
Maximale Download-Bandbreite	Geben Sie die maximale Download-Bandbreite des gewählten Interfaces an. Diese Angabe wird benötigt, um die Regeln für eingehenden Datenverkehr korrekt anzuwenden. ⓘ An der rechten Seite des Bandbreiten-Eingabefeldes wird die aktuell gültige Einheit bzw. Größenordnung für die Eingabe angezeigt (GBit/s, MBit/s, KBit/s). Mit einem Klick auf die gegenwärtig eingestellte Größenordnung lässt sich ein Menü öffnen, um diese anzupassen. Außerdem wechselt durch Tippen von „g“, „m“ oder „k“ im Eingabefeld die Größenorndung ebenfalls auf Giga, Mega oder Kilo.
Maximale Upload-Bandbreite	Geben Sie die maximale Upload-Bandbreite des gewählten Interfaces an. Diese Angabe wird benötigt, um die Regeln für ausgehenden Datenverkehr korrekt anzuwenden. ⓘ An der rechten Seite des Bandbreiten-Eingabefeldes wird die aktuell gültige Einheit bzw. Größenordnung für die Eingabe angezeigt (GBit/s, MBit/s, KBit/s). Mit einem Klick auf die gegenwärtig eingestellte Größenordnung lässt sich ein Menü öffnen, um diese anzupassen. Außerdem wechselt durch Tippen von „g“, „m“ oder „k“ im Eingabefeld die Größenorndung ebenfalls auf Giga, Mega oder Kilo.
Eingehende Regeln – Definieren Sie hier den Regelsatz für eingehenden Datenverkehr. Eine einzelne Regel ordnet dem Datenverkehr der ausgewählten Traffic-Gruppe eine Priorität und ein Bandbreiten-Kontingent zu. Dieses besteht aus der einer Traffic-Gruppe garantierten Bandbreite und der Bandbreite, die sie maximal in Anspruch nehmen darf.	
Traffic-Gruppe / Interface	Wählen Sie die Traffic-Gruppe oder das Interface aus, für die diese Regel gelten soll. Auswählbare Interface-Typen sind Ethernet, VLAN, Bridge und Bond.
Priorität	Eine kleine Zahl (1) entspricht einer hohen Priorität, eine hohe Zahl (7) einer niedrigen.

Eingabefeld	Beschreibung
	Mehrere Regeln können die gleiche Priorität haben. In diesem Fall wird die Übertragungskapazität „fair“ aufgeteilt.
Garantierte Bandbreite	Garantierte Bandbreite für diese Traffic-Gruppe. An der rechten Seite des Bandbreiten-Eingabefeldes wird die aktuell gültige Einheit bzw. Größenordnung für die Eingabe angezeigt (GBit/s, MBit/s, KBit/s). Mit einem Klick auf die gegenwärtig eingestellte Größenordnung lässt sich ein Menü öffnen, um diese anzupassen. Außerdem wechselt durch Tippen von „g“, „m“ oder „k“ im Eingabefeld die Größenorndung ebenfalls auf Giga, Mega oder Kilo.
Maximale Bandbreite	Maximale Bandbreite für diese Traffic-Gruppe. An der rechten Seite des Bandbreiten-Eingabefeldes wird die aktuell gültige Einheit bzw. Größenordnung für die Eingabe angezeigt (GBit/s, MBit/s, KBit/s). Mit einem Klick auf die gegenwärtig eingestellte Größenordnung lässt sich ein Menü öffnen, um diese anzupassen. Außerdem wechselt durch Tippen von „g“, „m“ oder „k“ im Eingabefeld die Größenorndung ebenfalls auf Giga, Mega oder Kilo.
Ausgehende Regeln – Definieren Sie hier den Regelsatz für ausgehenden Datenverkehr	
Traffic-Gruppe / Interface	Wählen Sie die Traffic-Gruppe oder das Interface aus, für die diese Regel gelten soll. Auswählbare Interface-Typen sind Ethernet, VLAN, Bridge und Bond.
Priorität	Eine kleine Zahl (1) entspricht einer hohen Priorität, eine hohe Zahl (7) einer niedrigen. Pro Interface kann nur eine Shaping-Konfiguration zur gleichen Zeit aktiv sein. Traffic, der keiner der ausgehenden Regeln entspricht, hat die niedrigste Priorität und es wird keine Bandbreite garantiert. Die Summe der garantierten Bandbreiten aller Regeln einer Übertragungsrichtung darf die maximale Interface-Bandbreite für diese Übertragungsrichtung nicht überschreiten. Dasselbe gilt für die in einer Regel festgelegten maximalen Bandbreite. Mehrere Regeln können die gleiche Priorität haben. In diesem Fall wird die Übertragungskapazität „fair“ aufgeteilt.
Garantierte Bandbreite	Garantierte Bandbreite für diese Traffic-Gruppe. An der rechten Seite des Bandbreiten-Eingabefeldes wird die aktuell gültige Einheit bzw. Größenordnung für die Eingabe angezeigt (GBit/s, MBit/s, KBit/s). Mit einem Klick auf die gegenwärtig eingestellte Größenordnung lässt sich ein Menü öffnen, um diese anzupassen. Außerdem wechselt durch Tippen von „g“, „m“ oder „k“ im Eingabefeld die Größenorndung ebenfalls auf Giga, Mega oder Kilo.
Maximale Bandbreite	Maximale Bandbreite für diese Traffic-Gruppe. An der rechten Seite des Bandbreiten-Eingabefeldes wird die aktuell gültige Einheit bzw. Größenordnung für die Eingabe angezeigt (GBit/s, MBit/s, KBit/s). Mit einem Klick auf die gegenwärtig eingestellte Größenordnung lässt sich ein Menü öffnen, um diese anzupassen. Außerdem wechselt durch Tippen von „g“, „m“ oder „k“ im Eingabefeld die Größenorndung ebenfalls auf Giga, Mega oder Kilo.

Wenn Sie diese Einstellungen ändern, klicken Sie zum Speichern Ihrer Änderungen auf **Speichern** oder auf **Zurücksetzen**, um sie zu verwerfen. Klicken Sie ansonsten auf **Schließen**, um das Bearbeitungsfenster zu schließen.

3.4.3.6.2 Traffic-Gruppen

Navigieren Sie zu **Netzwerk** > **Traffic Shaping** > **Traffic-Gruppen**, um die Liste der derzeit im System angelegten Traffic-Gruppen anzuzeigen und zu verwalten. Diesen Traffic-Gruppen kann Datenverkehr auf unterschiedlichen Wegen zugeordnet werden (Desktop-Verbindung, IPsec-Verbindung, App-Routing-Profil, DSCP-Wert).

Mit den Schaltflächen in der letzten Spalte können Sie die Einstellungen für eine vorhandene Traffic-Gruppe ansehen und anpassen oder eine Traffic-Gruppe aus dem System löschen. Klicken Sie auf die Schaltfläche ⊕, um eine neue Traffic-Gruppe anzulegen. Es öffnet sich ein Bearbeitungsfenster, in dem Sie die Einstellungen für eine Traffic-Gruppe anpassen können.

Im Bearbeitungsfenster **Traffic-Gruppe** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Name	Der Name dieser Traffic-Gruppe. Sie können bis zu 7 Traffic-Gruppen anlegen.
DSCP eingehend	Wählen Sie einen optionalen DSCP-Wert für eingehenden Datenverkehr aus der Liste aus. Datenverkehr, der außerhalb der Unified Firewall entsprechend markiert wurde, wird in der Unified Firewall der aktuellen Traffic-Gruppe zugeordnet. Die Liste enthält die Bezeichnungen aus den relevanten RFCs (z. B. „AF41“) und der Gruppe (z. B. „Multimedia Conferencing“). Zusätzlich wird der Wert ebenfalls in seiner numerischen Repräsentation zu verschiedenen Basen (binär, hexadezimal und dezimal) angezeigt. Die Liste können Sie entsprechend dieser Darstellungen durchsuchen, so dass Sie unabhängig von der individuell bevorzugten Darstellung schnell den gewünschten Wert finden.

Wenn Sie diese Einstellungen ändern, klicken Sie zum Speichern Ihrer Änderungen auf **Speichern** oder auf **Zurücksetzen**, um sie zu verwerfen. Klicken Sie ansonsten auf **Schließen**, um das Bearbeitungsfenster zu schließen.

Traffic-Gruppen-Zuordnung und DSCP-Werte für ausgehenden Datenverkehr

An unterschiedlichen Stellen lässt sich Datenverkehr einer Traffic-Gruppe zuordnen, sowie ein DSCP-Wert festlegen, mit dem entsprechende Pakete vor dem Weitersenden durch LANCOM R&S®Unified Firewall versehen werden. Beide Angaben sind stets optional. Die Angabe einer **Traffic-Gruppe** erlaubt es, den entsprechenden Datenverkehr mit Hilfe einer Shaping-Konfiguration zu priorisieren. Der Wert im Feld **DSCP ausgehend** erlaubt es anderen Geräten im Netzwerk, die ensprechenden Pakete ebenfalls zu klassifizieren und – bei entsprechender Konfiguration – wunschgemäß zu behandeln.

Desktop-Verbindungen

Die Einstellungen betreffen den Datenverkehr, welcher der bearbeiteten Desktop-Verbindung entspricht. Die Einstellungsmöglichkeiten bei Desktop-Verbindungen verhalten sich wie diejenigen für NAT-Einstellungen: Sie lassen sich sowohl für die gesamte Desktop-Verbindung als auch für einzelne Regeln innerhalb dieser Verbindung vornehmen. In beiden Fällen werden die Einstellungen über den Tab **Traffic-Shaping** (entweder auf Verbindungs- oder auf Regelebene) vorgenommen. In der Regelliste lässt sich in der zweiten Spalte (TS) anhand der Checkboxes sehen und anpassen, ob die Einstellungen auf Verbindungs-Ebene genutzt werden sollen, oder nicht.

Im Tab **Traffic-Shaping** können Sie die Einstellungen des Traffic Shaping für den Datenverkehr auf der gewählten Verbindung konfigurieren:

Eingabefeld	Beschreibung
Traffic-Gruppe	Wählen Sie optional den Namen einer Traffic-Gruppe aus. Dadurch werden die für diese Gruppe definierten Regeln für den Datenverkehr auf dieser Verbindung angewendet. Siehe auch *Traffic Shaping* auf Seite 105. ⓘ Falls es sich um einen Routen-basierten IPsec-Tunnel handelt, kann der Datenverkehr innerhalb eines Tunnels mit Hilfe einer eigenen Shaping-Konfiguration priorisiert werden.
DSCP ausgehend	Wählen Sie einen optionalen DSCP-Wert für ausgehenden Datenverkehr aus der Liste aus. Die Liste enthält die Bezeichnungen aus den relevanten RFCs (z. B. „CS0“) und der Gruppe (z. B. „Standard“). Zusätzlich wird der Wert ebenfalls in seiner numerischen Repräsentation zu verschiedenen Basen (binär, hexadezimal und dezimal) angezeigt. Die Liste kann entsprechend dieser Darstellungen durchsucht werden, so dass Sie unabhängig von der individuell bevorzugten Darstellung schnell den gewünschten Wert finden.

Diese Einstellungen für die Verbindung lassen sich dann in einer Firewall-Regel verwenden oder dort durch servicespezifische Einstellungen überschreiben.

Im Tab zu den Einstellungen unter **Traffic-Shaping** stehen die folgenden Optionen zur Verfügung:

Eingabefeld	Beschreibung
Traffic-Shaping	Wählen Sie aus den folgenden Optionen: › **Verbindungs-Einstellungen verwenden** – Mit dieser Einstellung werden die auf Verbindungsebene vorgenommenen Traffic-Shaping-Einstellungen übernommen. Siehe *Einstellungen für Desktopverbindungen* auf Seite 115. › **Servicespezifische-Einstellungen verwenden** – Über diese Einstellung können sie die Traffic-Shaping-Einstellungen pro Service einstellen. Dazu werden die im Folgenden beschriebenen Einstellungen eingeblendet.
Traffic-Gruppe	Wählen Sie optional den Namen einer Traffic-Gruppe aus. Dadurch werden die für diese Gruppe definierten Regeln für den Datenverkehr auf dieser Verbindung angewendet. Siehe auch *Traffic Shaping* auf Seite 105. Falls es sich um einen Routen-basierten IPsec-Tunnel handelt, kann der Datenverkehr innerhalb eines Tunnels mit Hilfe einer eigenen Shaping-Konfiguration priorisiert werden.
DSCP ausgehend	Wählen Sie einen optionalen DSCP-Wert für ausgehenden Datenverkehr aus der Liste aus. Die Liste enthält die Bezeichnungen aus den relevanten RFCs (z. B. „CS0“) und der Gruppe (z. B. „Standard“). Zusätzlich wird der Wert ebenfalls in seiner numerischen Repräsentation zu verschiedenen Basen (binär, hexadezimal und dezimal) angezeigt. Die Liste kann entsprechend dieser Darstellungen durchsucht werden, so dass Sie unabhängig von der individuell bevorzugten Darstellung schnell den gewünschten Wert finden.

IPsec-Verbindungen und -Templates

Unter **VPN** > **IPsec** > **Verbindungen** bzw. **VPN** > **IPsec** > **Vorlagen** können Sie die Traffic-Shaping-Regeln für IPsec-Verbindungen bzw. IPsec-Verbindungsvorlagen anwenden.

Im Tab **Traffic-Shaping** können Sie die folgenden Felder konfigurieren:

Eingabefeld	Beschreibung
Traffic-Gruppe	Wählen Sie optional den Namen einer Traffic-Gruppe aus. Dadurch werden die für diese Gruppe definierten Regeln für den Datenverkehr auf dieser Verbindung angewendet. Siehe auch *Traffic Shaping* auf Seite 105. Falls es sich um einen Routen-basierten IPsec-Tunnel handelt, kann der Datenverkehr innerhalb eines Tunnels mit Hilfe einer eigenen Shaping-Konfiguration priorisiert werden.
DSCP ausgehend	Wählen Sie einen optionalen DSCP-Wert für ausgehenden Datenverkehr aus der Liste aus. Die Liste enthält die Bezeichnungen aus den relevanten RFCs (z. B. „CS0“) und der Gruppe (z. B. „Standard“). Zusätzlich wird der Wert ebenfalls in seiner numerischen Repräsentation zu verschiedenen Basen (binär, hexadezimal und dezimal) angezeigt. Die Liste kann entsprechend dieser Darstellungen durchsucht werden, so dass Sie unabhängig von der individuell bevorzugten Darstellung schnell den gewünschten Wert finden.

App-Routing-Profile

Hier finden Sie die Einstellungen nicht in einem eigenen Tab, sondern direkt auf oberster Ebene des Editors eines App-Routing-Profils unter **UTM** > **Application-Management** > **Routing-Profile**.

Eingabefeld	Beschreibung
Traffic-Gruppe	Wählen Sie optional den Namen einer Traffic-Gruppe aus. Dadurch werden die für diese Gruppe definierten Regeln für den Datenverkehr angewendet, der vom Application Filter den im Routing-Profil ausgewählten Regeln zugeordnet wird. Dafür muss der Datenverkehr zunächst auch der Desktop-Verbindung entsprechen, in der das bearbeitete App-Routing-Profil verwendet wird. Siehe auch *Traffic Shaping* auf Seite 105.
DSCP ausgehend	Wählen Sie einen optionalen DSCP-Wert für ausgehenden Datenverkehr aus der Liste aus. Die Liste enthält die Bezeichnungen aus den relevanten RFCs (z. B. „CS0“) und der Gruppe (z. B. „Standard“). Zusätzlich wird der Wert ebenfalls in seiner numerischen Repräsentation zu verschiedenen Basen (binär, hexadezimal und dezimal) angezeigt. Die Liste kann entsprechend dieser Darstellungen durchsucht werden, so dass Sie unabhängig von der individuell bevorzugten Darstellung schnell den gewünschten Wert finden.

3.4.3.7 Routing

Nutzen Sie die Einstellungen unter **Routing**, um das Border Gateway Protocol (BGP), Routingtabellen und Routing-Regeln zu konfigurieren.

Über die Routingeinstellungen können Sie benutzerdefinierte Routen anlegen, die genutzt werden, um Computer in einem bestimmten Zielnetzwerk zu erreichen.

Routen zwischen Netzwerkobjekten werden automatisch erstellt und verborgen. Normalerweise müssen Sie keine Routen erstellen, es sei denn, Sie haben einen übergeordneten Router, der spezielle Routen erfordert. Um den Datenverkehr zwischen den Netzwerkobjekten zu beeinflussen, erstellen Sie wie unter *Einstellungen für Firewall-Regeln* auf Seite 30beschrieben eine Firewall-Regel.

3.4.3.7.1 BGP

Das Border Gateway Protocol (BGP) ist ein dynamisches Path-Vector-Routing-Protokoll, mit dessen Hilfe Routing-Informationen zwischen autonomen Systemen (AS) ausgetauscht werden.

BGP wird dabei typischerweise für das Übermitteln von Routing-Informationen zwischen verschiedenen AS im Internet (eBGP) oder für das Übermitteln von aus eBGP gelernten Informationen innerhalb eines AS (iBGP) eingesetzt.

Einstellungen für BGP

Unter **Netzwerk** > **Routing** > **BGP** können Sie die BGP-Einstellungen der Firewall konfigurieren.

Im Bearbeitungsfenster **BGP** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
I/0	Ein Schiebeschalter gibt an, ob Routing über BGP aktiv (**I**) oder inaktiv (**0**) ist. Mit einem Klick auf den Schiebeschalter können Sie den Status ändern.
Eigener Name	Der eigene Name wird angezeigt.
Domain	Die eigene Domain wird angezeigt.
AS-Nummer	Geben Sie hier die eigene AS-Nummer an.
Nachbarn	› **Name** – Geben Sie den Namen des BGP-Nachbarn an. › **Adresse** – Geben Sie die IP-Adresse des BGP-Nachbarn an. › **AS-Nummer** – Geben Sie die AS-Nummer des BGP-Nachbarn an. › **Passwort** – Geben Sie das Passwort / den Shared Key zur Authentifizierung mit dem BGP-Nachbarn an. Klicken Sie rechts auf ⊕, um Ihren Eintrag zur Liste der BGP-Nachbarn hinzuzufügen.

Eingabefeld	Beschreibung
Multihop-Peers	Stellen Sie die max. Anzahl an Hops ein, über die ein Peer erreicht werden kann. Mögliche Werte: 0 bis 255 (bei 0 werden nur direkt verbundene Peers berücksichtigt).
Verbundene Routen weiter verteilen	Geben Sie hier an, ob die auf der Firewall konfigurierten Netzwerke an alle BGP-Nachbarn verteilt werden sollen.
Statische Routen weiter verteilen	Geben Sie hier an, ob die unten konfigurierten Netzwerke an alle BGP-Nachbarn verteilt werden sollen.
Routen	Geben Sie hier die Netzwerke an, die über BGP weitergegeben (announced) werden sollen. Klicken Sie rechts auf ⊕, um Ihren Eintrag zur Liste der Routen hinzuzufügen.
Ziel-Routing-Tabelle	Routing-Tabelle, in die die gelernten Routing-Einträge geschrieben werden sollen. Mögliche Werte: 254 (Haupttabelle) oder 512 bis 65535 (benutzerdefinierte Tabellen)

Wenn Sie diese Einstellungen ändern, klicken Sie zum Speichern Ihrer Änderungen auf **Speichern** oder auf **Zurücksetzen**, um sie zu verwerfen. Klicken Sie ansonsten auf **Schließen**, um das Bearbeitungsfenster zu schließen.

3.4.3.7.2 Routing-Regeln

Routing-Regeln legen fest, welche Pakete von welcher Routingtabelle verwaltet werden. Dies ermöglicht ein differenzierteres Routing, da Routing-Regeln mehr Felder des IP-Headers in die Routingentscheidung einbeziehen, während Routingtabellen nur die Ziel-IP-Adresse beachten.

Übersicht Routing-Regeln

Navigieren Sie zu **Netzwerk** > **Routing** > **Routing-Regeln**, um die Liste der Routing-Regeln anzuzeigen, die derzeit im System angelegt sind.

Über die Plus-Schaltfläche ⊕ über den Filtereinstellungen können Sie neue Routing-Regeln anlegen.

Mit den **Filtereinstellungen** können Sie die Ergebnisse eingrenzen und nur Einträge anzeigen, die einen bestimmten Suchbegriff enthalten. Sie können Inhalte filtern, indem Sie die gewünschten Optionen aus der Drop-down-Liste auswählen und / oder einen Suchbefehl im jeweiligen Eingabefeld eingeben. Klicken Sie auf **Anwenden**, um die gewählten Filteroptionen anzuwenden. Die Liste der Routing-Regeln zeigt nun Ihre Filterergebnisse an. Klicken Sie auf **Zurücksetzen**, um die gewählten Filteroptionen wieder zu entfernen und eine ungefilterte Ansicht der Liste der Routing-Regeln anzuzeigen.

Die Tabellenspalten der Liste der Routing-Regeln zeigen die Priorität der jeweiligen Routing-Regel an, die Selektoren, mit denen definiert werden kann, welcher Traffic geroutet wird und ob es sich um eine Systemregel handelt oder nicht. Mit den Schaltflächen in der letzten Spalte können Sie die Einstellungen für eine vorhandene Routing-Regel einsehen und anpassen oder eine Regel aus dem System löschen.

Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28.

ⓘ Vom System vorgesehene Routing-Regeln können nicht angepasst oder gelöscht werden.

Klicken Sie auf ✖ in der rechten oberen Ecke des Fensters, um das Fenster **Routing-Regeln** zu schließen.

Einstellungen für Routing-Regeln

Unter **Netzwerk** > **Routing** > **Routing-Regeln** können Sie eine neue Routing-Regel hinzufügen oder eine vorhandene bearbeiten.

Im Bearbeitungsfenster **Routing-Regel** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Priorität	Bestimmen Sie die Priorität einer benutzerdefinierten Routing-Regel, indem Sie einen ganzzahligen Wert zwischen `64` und `32767` eingeben.

Eingabefeld	Beschreibung
	Die Regeln werden nach aufsteigender Priorität geordnet. Das System beginnt also, angefangen mit der Systemregel mit der Priorität `0`, die Liste der Regeln zu durchlaufen, bis es auf eine Regel stößt, deren Selektoren komplett mit dem Paket übereinstimmen. Die für diese Regel bestimmte Aktion wird dann ausgeführt.
Quell-Subnetz	Optional: Geben Sie die IP-Adresse des Quell-Subnetzes in CIDR-Schreibweise ein (IP-Adresse gefolgt von einem Schrägstrich „/" und der Anzahl der in der Subnetzmaske festgelegten Bits, beispielsweise `192.168.50.0/24`).
Ziel-Subnetz	Optional: Geben Sie die IP-Adresse des Ziel-Subnetzes in CIDR-Schreibweise ein (IP-Adresse gefolgt von einem Schrägstrich „/" und der Anzahl der in der Subnetzmaske festgelegten Bits, beispielsweise `192.168.50.0/24`).
Eingangs-Interface	Optional: Wählen Sie eines der auf Ihrer LANCOM R&S®Unified Firewall definierten Interfaces als Eingabe-Interface aus.
Ausgangs-Interface	Optional: Wählen Sie eines der auf Ihrer LANCOM R&S®Unified Firewall definierten Interfaces als Ausgabe-Interface aus.
TOS	Optional: Geben Sie den Type of Service-Wert an, indem Sie eine Hexadezimalzahl zwischen `0` und `FF` eingeben.
Aktion	Bestimmen Sie eine Aktion für die Regel: › **Goto** – Geben Sie die **Priorität** einer anderen Routing-Regel ein. Wenn ein Paket mit den Selektoren in der Regel übereinstimmt, springt es zu der Regel mit der angegebenen Goto-Priorität. › **Tabelle** – Geben Sie die Nummer einer Routingtabelle ein. Wenn ein Paket mit den Selektoren in der Regel übereinstimmt, durchläuft es die angegebene Routingtabelle. Wenn eine der Routen in der Tabelle mit dem Paket übereinstimmt, wird es entsprechend geroutet. Wenn nicht, durchläuft das Paket weiter die Liste der Routing-Regeln. Der hier eingegebene Parameter wird in der Tabellenspalte **Aktions-Parameter** der Liste der Routing-Regeln angezeigt (weitere Informationen hierzu finden Sie unter *Übersicht Routing-Regeln* auf Seite 111).

Wenn Sie keinen der Selektoren bestimmen, stimmt der gesamte Datenverkehr mit der Regel überein.

Die Schaltflächen rechts unten im Bearbeitungsfeld hängen davon ab, ob Sie eine neue Routing-Regel hinzufügen oder eine bestehende Regel bearbeiten. Klicken Sie für eine neu konfigurierte Routing-Regel auf **Erstellen**, um die Regel zur Liste der verfügbaren Routing-Regeln hinzuzufügen, oder auf **Abbrechen**, um die Erstellung einer neuen Regel abzubrechen. Zum Bearbeiten einer vorhandenen Regel klicken Sie auf **Speichern**, um die neu konfigurierte Regel zu speichern, oder auf **Zurücksetzen**, um Ihre Änderungen zu verwerfen. Sie können auf **Schließen** klicken, um das Bearbeitungsfenster zu schließen, solange keine Änderungen darin vorgenommen wurden.

3.4.3.7.3 Routingtabellen

Routingtabellen routen Pakete nach ihrer Ziel-IP-Adresse durch das Netzwerk.

In den folgenden Abschnitten finden Sie weiterführende Informationen zu Routingtabellen.

Übersicht Routingtabellen

Navigieren Sie zu **Netzwerk** > **Routing** > **Routing-Tabellen**, um die Liste der derzeit im System angelegten Routingtabellen in der Leiste mit der Objektliste anzuzeigen.

Entfernen Sie den Haken vor **Nur konfigurierbare Tabellen zeigen**, um alle Tabellen im System anzuzeigen. Wenn Sie den Haken gesetzt lassen, werden nur diejenigen Tabellen angezeigt, die bearbeitet werden können.

Die folgenden Tabellen sind im System vorhanden:

- Tabelle 254 ist die primäre Routingtabelle. Zu dieser Tabelle können Sie benutzerdefinierte Routen hinzufügen. Die Einträge werden dann für alle bestehenden Routingtabellen übernommen.
- Tabelle 255 enthält lokale Routen für alle konfigurierten Interfaces.
- Tabellen 1 bis 63 sind für die Verwaltung der Internetverbindungen reserviert.
- Tabellen 64 bis 250 sind für Routen mit Quelladresse reserviert und erscheinen während der Einrichtung der Routen mit ihrer Quell-IP-Adresse.
- Tabelle 293 ist für den transparenten Proxy reserviert.

In der erweiterten Ansicht zeigen die Tabellenspalten den Namen der Routingtabelle an. Mit den Schaltflächen in der letzten Spalte können Sie die Einstellungen für eine vorhandene Routingtabelle einsehen und anpassen oder eine Tabelle aus dem System löschen.

Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28.

Einstellungen für Routingtabellen

Unter **Routing-Tabellen** können Sie eine neue Routingtabelle hinzufügen, oder vorhandene Routingtabellen bearbeiten.

Im Bearbeitungsfenster **Routing-Tabelle** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Tabellen-Nummer	Geben Sie eine Identifikationsnummer für die Routingtabelle ein. Benutzerdefinierte Tabellen erhalten die ID `512` oder eine höhere Zahl. Für benutzerdefinierte Routingtabellen müssen Routing-Regeln konfiguriert werden, andernfalls werden diese Tabellen nicht verwendet (siehe *Routing-Regeln* auf Seite 111).
Routen	Diese Tabelle zeigt die benutzerdefinierten Routen in der Routingtabelle an. Klicken Sie auf **Hinzufügen**, um das Fenster **Route bearbeiten** zu öffnen und eine neue Route zu definieren. Sie können einzelne Einträge in der Liste bearbeiten oder löschen, indem Sie auf die entsprechende Schaltfläche neben einem Eintrag klicken.

Im Bearbeitungsfenster **Route bearbeiten** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Ziel	Geben Sie die IP-Adresse des Ziel-Subnetzes in CIDR- Schreibweise ein (IP-Adresse gefolgt von einem Schrägstrich „/" und der Anzahl der in der Subnetzmaske festgelegten Bits, beispielsweise 192.168.50.0/24).
Interface	Wählen Sie ein Interface für die Route.
Gateway	Geben Sie eine IP-Adresse als Gateway für diese Route ein. Datenverkehr von der Quellzone zum Zielnetzwerk wird über dieses Gateway geleitet (anstelle des Standard-Gateways).
Typ	Wählen Sie den Addresstyp aus der Drop-Down-Liste.
Bevorzugte Quelle	Nur Pakete mit der gewählten Senderadresse werden geroutet.
Metrik	Bestimmen Sie die Kosten für die Route. Der hier eingegebene Wert betrifft Routingprotokolle. Eine höherer Wert in der Metrik bedeutet, dass die Route als kostenungünstig betrachtet und mit weniger Wahrscheinlichkeit gewählt wird.

Klicken Sie auf **OK**, um die Routingeinstellungen zu speichern und zum Fenster **Routing-Tabelle** zurückzukehren.

Die Schaltflächen rechts unten im Bearbeitungsfeld hängen davon ab, ob Sie eine neue Routingtabelle hinzufügen oder eine bestehende Tabelle bearbeiten. Klicken Sie für eine neu konfigurierte Routingtabelle auf **Erstellen**, um die Tabelle zur Liste der verfügbaren Routingtabellen hinzuzufügen, oder auf **Abbrechen**, um Ihre Änderungen zu verwerfen. Zum Bearbeiten einer vorhandenen Tabelle klicken Sie auf **Speichern**, um die neu konfigurierte Tabelle zu speichern, oder

auf **Zurücksetzen**, um Ihre Änderungen zu verwerfen. Sie können auf **Schließen** klicken, um das Bearbeitungsfenster zu schließen, solange keine Änderungen darin vorgenommen wurden.

3.4.3.7.4 LLDP

Das LLDP (Link Layer Discovery Protocol) wird verwendet, um Informationen wie z. B. Interface MAC-Adressen oder System-Beschreibungen mit direkt verbundenen Nachbar-Geräten auszutauschen. Es operiert dabei auf Layer 2. Jedes Interface sendet und empfängt Informationen separat. So sendet das lokale Interface eth1 nur Informationen über sich selbst an Nachbarn, mit denen das lokale Gerät auf diesem Interface verbunden ist. Beim Empfangen verhält es sich genau so. Informationen werden ausschließlich mit unmittelbaren Nachbarn ausgetauscht und können verwendet werden, um beispielsweise beim Verkabeln von Geräten zu unterstützen.

In den folgenden Abschnitten finden Sie weiterführende Informationen zu LLDP.

Einstellungen für LLDP

Unter **Netzwerk** > **LLDP** > **LLDP-Einstellungen** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
I/**0**	Ein Schiebeschalter gibt an, ob die LLDP-Einstellungen derzeit aktiv (**I**), oder inaktiv (**0**) sind. Mit einem Klick auf den Schiebeschalter können Sie den Status ändern.
Interface	Aktivieren Sie für jedes vorhandene Interface, ob LLDP-Daten separat gesendet oder empfangen werden sollen. Im Tabellenheader können Sie dies auch für alle Interfaces gleichzeitig einstellen. Beachten Sie, dass beim Senden verschiedene Informationen über die Firewall gesendet werden: Seriennummer, Vendor-ID, Hardware-Typ, Version und Management-IP der Firewall.

Die Schaltflächen rechts unten im Bearbeitungsfeld hängen davon ab, ob Sie Änderungen vorgenommen haben. Um die Änderungen zu übernehmen, klicken Sie auf **Speichern**, um die Änderungen zu speichern, oder auf **Zurücksetzen**, um Ihre Änderungen zu verwerfen. Sie können auf **Schließen** klicken, um das Bearbeitungsfenster zu schließen, solange keine Änderungen darin vorgenommen wurden.

3.4.4 Desktop

Die Einstellungen unter **Desktop** zeigen eine Liste aller verfügbaren Dienste und der im System definierten Firewall-Regeln an.

3.4.4.1 Desktopverbindungen

Navigieren Sie zu **Desktop** > **Desktop-Verbindungen**, um die Verbindungen zwischen verschiedenen Desktop-Objekten, die im System definiert sind, anzuzeigen und zu bearbeiten.

3.4.4.1.1 Übersicht Desktopverbindungen

In der erweiterten Ansicht zeigen die Tabellenspalten die einzelnen Knoten der Desktopverbindung an. Mithilfe der Schaltflächen in der letzten Spalte können Sie die Einstellungen für eine vorhandene Desktopverbindung einsehen und anpassen, eine neue Desktopverbindung ausgehend von einer Kopie einer bestehenden Desktopverbindung anlegen, oder eine Verbindung aus dem System löschen.

Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28.

Kopierte Desktopverbindungen werden stets zwischen denselben Knoten eingerichtet wie das Original.

3.4.4.1.2 Einstellungen für Desktopverbindungen

Wenn Sie eine Desktopverbindung bearbeiten, öffnet sich das **Verbindung** Fenster . Unter **Beschreibung** können Sie zusätzliche Informationen zur Desktopverbindung für die interne Verwendung eingeben.

Im Tab **Regeln** können Sie den Regelsatz für die gewählte Verbindung anpassen. Weitere Informationen zur Erstellung von Firewall-Regeln finden Sie unter *Einstellungen für Firewall-Regeln* auf Seite 30. Zusätzlich zu den dort beschriebenen Einstellungen können Sie in der ersten Spalte über den Haken bei **NAT der Verbind.** steuern, ob Sie entweder die im Folgenden beschriebenen Einstellungen der Verbindung auf dem Reiter **NAT** oder Service-spezifische Einstellungen verwenden. Letztere finden Sie auf dem Reiter **Erweitert** bei den Firewall-Regeln. Siehe auch *Erstellen einer Firewall-Regel* auf Seite 31.

Im Tab **NAT** können Sie für ganze Netzwerke SNAT- und DNAT-Einstellungen konfigurieren. Die Einstellungen entsprechen dabei den Einstellungen für einzelne Services mit Ausnahme des Ziel-Ports, der bei den NAT-Einstellungen der Verbindung entfällt.

Eingabefeld	Beschreibung
NAT / Masquerading	Geben Sie für NAT / Masquerading die gewünschte Richtung an (**Bidirektional**, **Links-nach-rechts** oder **Rechts-nach-links**) oder deaktivieren Sie (**Aus**) die Funktion für diese Regel, indem Sie die entsprechende Optionsschaltfläche auswählen. Die Standardeinstellung hängt von den für die Verbindung ausgewählten Quell- und Zielobjekten ab.
NAT-Quell-IP	Optional: Wenn Sie mehrere ausgehende IP-Adressen haben, geben Sie die IP-Adresse an, die für Source-NAT verwendet werden soll. Wenn Sie keine IP-Adresse angeben, wählt das System automatisch die Haupt-IP-Adresse des ausgehenden Interface aus. Wenn ein verbundenes Objekt ein Netzwerk ist, können Sie hier auch ein Netzwerk eintragen unter der Voraussetzung, dass das eingetragene Netz dieselbe Größe hat wie das Netzwerk des Objektes.
DNAT aktivieren	Ist ein einzelnes Host- oder Netzwerk-Objekt das Ziel, können Sie den Haken in diesem Kontrollkästchen setzen, um DNAT zu aktivieren.
Externe IP-Adresse	Optional: Geben Sie die Ziel-IP-Adresse des zu bearbeitenden Datenverkehrs an. DNAT wird nur auf diesen Datenverkehr angewandt. Diese IP-Adresse muss eine der IP-Adressen der Firewall sein. Wenn ein verbundenes Objekt ein Netzwerk ist, können Sie hier auch ein Netzwerk eintragen unter der Voraussetzung, dass das eingetragene Netz dieselbe Größe hat wie das Netzwerk des Objektes.
Ziel-IP-Adresse	Optional: Geben Sie die Ziel-IP-Adresse des zu bearbeitenden Datenverkehrs an.

Im Tab **URL- / Content-Filter** können Sie den URL- und den Contentfilter für die gewählte Verbindung konfigurieren:

Eingabefeld	Beschreibung
Standardmäßig alles blockieren	Jegliche Anfragen werden geblockt, soweit die Anfrage nicht von einer aktivierten Whitelist explizit freigegeben ist. Contentfilter und Blacklisteinträge haben keine Funktion und werden daher ausgegraut.
Web-Filter-Modus	Sie haben die Auswahl zwischen den folgenden Modi: › **Proxy** – Standardmodus für den **URL- / Content-Filter**. › **DNS** – **URL- / Content-Filter** auf Basis von DNS betreiben. Dies bedeutet, dass DNS-Abfragen, die über den DNS-Server der LANCOM R&S®Unified Firewall laufen, klassifiziert werden und gemäß ihrer Kategorien oder konfigurierter Black- und Whitelists gefiltert werden. Dabei werden die gleichen Profile genutzt wie beim **URL- / Content-Filter** über den HTTP- / HTTPS-Proxy. Für die Verwendung des DNS-Filters auch bei HTTPS-Verbindungen ist keine Installation von Zertifikaten auf den Client-Geräten notwendig. Dadurch kommt es aber auch zu folgenden Einschränkungen:

Eingabefeld	Beschreibung
	› Gefiltert wird auf der Domain, nicht auf der URL. › Es wird keine Blockpage angezeigt und es ist nicht möglich, den Override-Modus zu nutzen. › Gefiltert wird nur, wenn die DNS Anfrage durch die Firewall geht. › **Proxy und DNS** – Eine Kombination der obigen Modi.
Name	Zeigt den Namen des URL- und des Contentfilters an.
URL-Filter Black/White	Fügen Sie die URLs der jeweiligen Filter zur Blacklist oder zur Whitelist hinzu, indem Sie auf die betreffenden Kontrollkästchen klicken.
Content-Filter	Um Contentfilter auszuwählen, setzen Sie den Haken in den jeweiligen Kontrollkästchen.
Zeitsteuerung	Zeigt an, ob der Filter stets aktiv, stets inaktiv oder nach einem gewählten Zeitplan aktiv ist. Klicken Sie auf den Eintrag, um den Zeitplan zu bearbeiten.

Im Tab **Traffic-Shaping** können Sie die Einstellungen des Traffic Shaping für den Datenverkehr auf der gewählten Verbindung konfigurieren:

Eingabefeld	Beschreibung
Traffic-Gruppe	Wählen Sie optional den Namen einer Traffic-Gruppe aus. Dadurch werden die für diese Gruppe definierten Regeln für den Datenverkehr auf dieser Verbindung angewendet. Siehe auch *Traffic Shaping* auf Seite 105. Falls es sich um einen Routen-basierten IPsec-Tunnel handelt, kann der Datenverkehr innerhalb eines Tunnels mit Hilfe einer eigenen Shaping-Konfiguration priorisiert werden.
DSCP ausgehend	Wählen Sie einen optionalen DSCP-Wert für ausgehenden Datenverkehr aus der Liste aus. Die Liste enthält die Bezeichnungen aus den relevanten RFCs (z. B. „CS0“) und der Gruppe (z. B. „Standard“). Zusätzlich wird der Wert ebenfalls in seiner numerischen Repräsentation zu verschiedenen Basen (binär, hexadezimal und dezimal) angezeigt. Die Liste kann entsprechend dieser Darstellungen durchsucht werden, so dass Sie unabhängig von der individuell bevorzugten Darstellung schnell den gewünschten Wert finden.

Wenn Sie Anwendungsfilter (siehe *Application-Management* auf Seite 137) erstellt haben, können Sie diese für die gewählte Desktopverbindung aktivieren oder deaktivieren. Im Tab **Application Filter** können Sie den **Modus** des Anwendungsfilters auf **Blacklist** oder **Whitelists** setzen, oder den Application-Filter für jedes gewählte Profil deaktivieren, indem Sie die entsprechende Optionsschaltfläche auswählen. Im Tab **Application Based Routing** können Sie konfigurierte ***Routing-Profile*** hinzufügen.

Wenn Sie diese Einstellungen ändern, klicken Sie zum Speichern Ihrer Änderungen auf **Speichern** oder auf **Zurücksetzen**, um sie zu verwerfen. Klicken Sie ansonsten auf **Schließen**, um das Bearbeitungsfenster zu schließen.

Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

Weitere Informationen zu URL-, Content- und Application-Filtern finden Sie unter *URL- / Contentfilter* auf Seite 149 und *Application-Management* auf Seite 137.

3.4.4.2 Desktop-Objekte

Mit den Einstellungen unter **Desktop-Objekte** können Sie Ihr Netzwerk durch das Erstellen einzelner Objekte und Objektgruppen für Hosts, Benutzer, VPN- und IP-Bereiche organisieren. Die erstellten Objekte werden als Knoten auf dem Desktop angezeigt und können als Quelle und / oder Ziel einer Verbindung eingesetzt werden, um Firewall-Regeln anzuwenden.

In der Objektleiste erhalten Sie eine nach Typen gruppierte Übersicht aller aktuell im System definierten Desktop-Objekte. Wenn Sie auf einen Eintrag in der Objektleiste klicken, werden das entsprechende Desktop-Objekt und alle Verbindungen, die diesen Dienst verwenden, auf dem Desktop hervorgehoben.

Um ein Desktop-Objekt zu erstellen, klicken Sie auf die ⊕ Schaltfläche oben im jeweiligen Abschnitt der Objektliste. Alternativ können Sie auch auf das Symbol für das Desktop-Objekt in der Symbolleiste oben auf dem Desktop klicken.

Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28.

Die nachfolgenden Abschnitte enthalten weitere Informationen zu den verschiedenen Typen von Desktop-Objekten.

3.4.4.2.1 Host- / Netzwerkgruppen

Erstellen Sie Desktop-Objekte für Host- und Netzwerkgruppen, die zur Erstellung von Verbindungen zwischen mehreren Hosts, Netzwerken oder anderen Desktop-Objekten (z. B. VPN-Objekten) verwendet werden können. Host- und Netzwerkgruppen können bei der Anwendung von Firewall-Regeln und Webfiltern für mehrere Computer als Quellen bzw. Ziele dienen.

Übersicht Host- / Netzwerkgruppen

Navigieren Sie zu **Desktop** > **Desktop-Objekte** > **Host-/Netzwerk-Gruppen**, um die Liste der Host- und Netzwerkgruppenobjekte, die derzeit im System angelegt sind, in der Leiste mit der Objektliste anzuzeigen.

In der erweiterten Ansicht wird in der Tabelle der **Name** des Host- oder Netzwerkgruppenobjekts angezeigt. Anhand der Schaltflächen in der letzten Spalte können Sie die Einstellungen für ein vorhandenes Host- oder Netzwerkgruppenobjekt einsehen und anpassen, ein neues Gruppenobjekt ausgehend von einer Kopie eines vorhandenen Host- oder Netzwerkgruppenobjekts anlegen oder ein Gruppenobjekt aus dem System löschen.

Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28.

Einstellungen für Host- / Netzwerkgruppen

Mit den **Host- / Netzwerk-Gruppe**-Einstellungen können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Name	Geben Sie einen Namen für das Host- / Netzwerkgruppenobjekt an.
Beschreibung	Optional: Geben Sie weitere Informationen zum Host- / Netzwerkgruppenobjekt für die interne Verwendung ein.
Tags	Optional: Wählen Sie aus der Drop-down-Liste die Desktop-Tags aus, die Sie dem Host- oder Netzwerkgruppenobjekt zuweisen möchten. Weitere Informationen finden Sie unter *Desktop-Tags* auf Seite 129.
Farbe	Wählen Sie die Farbe aus, die für dieses Objekt auf dem Desktop verwendet werden soll.
Von IDS/IPS-Überprüfung ausnehmen	Nimmt dieses Gruppenobjekt von der IDS/IPS-Überprüfung aus.
Von Anti-Virus-Überprüfung ausnehmen	Nimmt dieses Gruppenobjekt von der Anti-Virus-Überprüfung aus.
Hosts / Netzwerke	Geben Sie die Hosts oder Netzwerke an, die Sie zum Host- oder Netzwerkgruppenobjekt hinzufügen möchten. Wählen Sie einen Namen, ein **Interface**, die IP-Adresse des Hosts oder des Netzwerks und bestimmen Sie, ob ein Login erlaubt ist. Alternativ wählen Sie unter **Desktop-Objekt / Name** ein bereits erstelltes Host- oder Netzwerk-Objekt. Änderungen an diesen referenzierten Desktop-Objekten werden beim Aktivieren der Regeln damit auch für diese Hostgruppe automatisch übernommen. Eine Bearbeitung des bereits existierenden Host- oder Netzwerk-Objekts aus diesem Dialog heraus ist erst möglich, sobald es der List hinzugefügt wurde. Im Infobereich werden referenzierte Objekte mit einem ⚙ markiert, sie sind somit auch von dort direkt zu bearbeiten. Klicken Sie auf **Hinzufügen**, um einen Host oder ein Netzwerk zur Liste hinzuzufügen. Sie können einzelne Einträge in den Listen bearbeiten oder löschen, indem Sie auf die entsprechende Schaltfläche neben einem Eintrag klicken. Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28.

Eingabefeld	Beschreibung
	Wenn Sie einen Eintrag bearbeiten, erscheint auf der rechten Seite des Eintrags ein Haken. Klicken Sie auf den Haken, um Ihre Änderungen zu übernehmen.
	Ist ein Gruppenmitglied implizit von der Prüfung durch ein UTM-Feature ausgenommen, so erscheint rechts neben der IP-Adresse ein -Symbol. Ein Klick hierauf öffnet dann ein kleines Popover mit einer Erklärung sowie einer Liste der UTM-Features, von denen das Gruppenmitglied ausgenommen ist, und von welchen übergeordneten Objekten diese Einstellung geerbt wurde.

Die Schaltflächen rechts unten im Bearbeitungsfeld hängen davon ab, ob Sie ein neues Host- oder Netzwerkgruppenobjekt hinzufügen oder ein bestehendes Objekt bearbeiten. Klicken Sie für ein neu konfiguriertes Objekt auf **Erstellen**, um es zur Liste der verfügbaren Host- und Netzwerkgruppen hinzuzufügen, oder auf **Abbrechen**, um Ihre Änderungen zu verwerfen. Zum Bearbeiten eines vorhandenen Objekts klicken Sie auf **Speichern**, um das neu konfigurierte Objekt zu speichern, oder auf **Zurücksetzen**, um Ihre Änderungen zu verwerfen. Sie können auf **Schließen** klicken, um das Bearbeitungsfenster zu schließen, solange keine Änderungen darin vorgenommen wurden.

Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

3.4.4.2.2 Hosts

Erstellen Sie ein Hostobjekt, das zur Erstellung von Verbindungen zwischen dem Host und weiteren Desktop-Objekten (z. B. VPN-Objekten) verwendet werden kann. Einem Host (z. B. einem Drucker oder einem VoIP-Telefon) kann eine eigene IP-Adresse zugewiesen werden, sodass die Firewall-Regeln speziell darauf angewendet werden können. Weitere Informationen zur Erstellung von Firewall-Regeln finden Sie unter *Einstellungen für Firewall-Regeln* auf Seite 30.

Übersicht Hosts

Navigieren Sie zu **Desktop** > **Desktop-Objekte** > **Hosts**, um die Liste der im System angelegten Hostobjekte in der Leiste mit der Objektliste anzuzeigen.

In der erweiterten Ansicht wird in den Tabellenspalten der **Name** und die **IP** des Hostobjekts angezeigt und mit welchem Interface er verbunden ist. Mithilfe der Schaltflächen in der letzten Spalte können Sie die Einstellungen für ein vorhandenes Hostobjekt einsehen und anpassen, ein neues Objekt ausgehend von einer Kopie eines vorhandenen Netzwerkobjekts anlegen, oder ein Objekt aus dem System löschen.

Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28.

Hosteinstellungen

Im Bearbeitungsfenster **Host** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Name	Geben Sie einen Namen für das Hostobjekt an.
Beschreibung	Optional: Geben Sie weitere Informationen zum Hostobjekt für die interne Verwendung ein.
Tags	Optional: Wählen Sie aus der Drop-down-Liste die Desktop-Tags aus, die Sie dem Hostobjekt zuweisen möchten. Weitere Informationen finden Sie unter *Desktop-Tags* auf Seite 129.
Farbe	Wählen Sie die Farbe aus, die für dieses Objekt auf dem Desktop verwendet werden soll.
Anmeldung erlauben	Aktivieren Sie dieses Kontrollkästchen, um Benutzern zu erlauben, sich mit der IP Adresse dieses Hostobjekts auf Ihrer LANCOM R&S®Unified Firewall einzuloggen. Durch diese Einstellung können benutzerspezifische Firewall-Regeln auf den aktuell eingeloggten Benutzer angewendet werden.
Icon	Wählen Sie ein Symbol, mit dem der Host auf dem Display dargestellt wird.
Interface	Wählen Sie ein Interface, mit dem der Host verbunden ist.

Eingabefeld	Beschreibung
Host	Geben Sie die IP-Adresse des Hostobjekts ein.
Von IDS/IPS-Überprüfung ausnehmen	Nimmt dieses Hostobjekt von der IDS/IPS-Überprüfung aus. Ein Objekt kann auch bereits implizit von der Prüfung ausgeschlossen sein. Das ist der Fall, wenn es in einem Netzbereich liegt, der bereits durch ein übergeordnetes Objekt explizit von der Prüfung ausgenommen wurde. In diesem Fall erscheint ein entsprechedner Hinweis unterhalb der Checkbox, der auch die Namen der Objekte aufführt, von denen die Einstellung „geerbt" wurde.
Von Anti-Virus-Überprüfung ausnehmen	Nimmt dieses Hostobjekt von der Anti-Virus-Überprüfung aus. Ein Objekt kann auch bereits implizit von der Prüfung ausgeschlossen sein. Das ist der Fall, wenn es in einem Netzbereich liegt, der bereits durch ein übergeordnetes Objekt explizit von der Prüfung ausgenommen wurde. In diesem Fall erscheint ein entsprechedner Hinweis unterhalb der Checkbox, der auch die Namen der Objekte aufführt, von denen die Einstellung „geerbt" wurde.

Die Schaltflächen rechts unten im Bearbeitungsfeld sind davon abhängig, ob Sie ein neues Host-Objekt hinzufügen oder ein bestehendes Objekt bearbeiten. Klicken Sie für ein neu konfiguriertes Objekt auf **Erstellen**, um es zur Liste der verfügbaren Objekte hinzuzufügen, oder auf **Abbrechen**, um Ihre Änderungen zu verwerfen. Zum Bearbeiten eines vorhandenen Objekts klicken Sie auf **Speichern**, um das neu konfigurierte Objekt zu speichern, oder auf **Zurücksetzen**, um Ihre Änderungen zu verwerfen. Sie können auf **Schließen** klicken, um das Bearbeitungsfenster zu schließen, solange keine Änderungen darin vorgenommen wurden.

Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

3.4.4.2.3 Internetobjekte

Erstellen Sie Internetobjekte für Ihre Internetverbindungen. Internetobjekte werden verwendet, um Verbindungen zwischen anderen Desktop-Objekten (z. B. VPN-Objekten) und dem Internet herzustellen.

Übersicht Internetobjekte

Navigieren Sie zu **Desktop** > **Desktop-Objekte** > **Internet-Objekte**, um die Liste der im System angelegten Internetobjekte in der Leiste mit der Objektliste anzuzeigen.

In der erweiterten Ansicht zeigt die Tabelle den **Objekt-Name** des Internetobjekts an. Mithilfe der Schaltflächen in der letzten Spalte können Sie die Einstellungen für ein vorhandenes Internetobjekt einsehen und anpassen, ein neues Objekt ausgehend von einer Kopie eines vorhandenen Internetobjekts anlegen, oder ein Objekt aus dem System löschen.

Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28.

Einstellungen für Internetobjekte

Im Bearbeitungsfenster **Internet-Objekt** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Objekt-Name	Geben Sie einen Namen für das Internetobjekt an.
Beschreibung	Optional: Geben Sie weitere Informationen zum Internetobjekt für die interne Verwendung ein.
Tags	Optional: Wählen Sie aus der Drop-down-Liste die Desktop-Tags aus, die Sie dem Internetobjekt zuweisen möchten. Weitere Informationen finden Sie unter *Desktop-Tags* auf Seite 129.
Farbe	Wählen Sie die Farbe aus, die für dieses Objekt auf dem Desktop verwendet werden soll.
Verbindungen	Wählen Sie die Internetverbindung(en) aus, zu denen dieses Objekt gehört. Weitere Informationen finden Sie unter *Einstellungen für Netzwerkverbindungen* auf Seite 81.

Die Schaltflächen rechts unten im Bearbeitungsfeld hängen davon ab, ob Sie ein neues Internetobjekt hinzufügen oder ein bestehendes Objekt bearbeiten. Klicken Sie für ein neu konfiguriertes Objekt auf **Erstellen**, um es zur Liste der verfügbaren Internetobjekte hinzuzufügen, oder auf **Abbrechen**, um Ihre Änderungen zu verwerfen. Zum Bearbeiten eines vorhandenen Objekts klicken Sie auf **Speichern**, um das neu konfigurierte Objekt zu speichern, oder auf **Zurücksetzen**, um Ihre Änderungen zu verwerfen. Sie können auf **Schließen** klicken, um das Bearbeitungsfenster zu schließen, solange keine Änderungen darin vorgenommen wurden.

Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

Weitere Informationen zur Erstellung von Internetobjekten finden Sie unter *Internetzugang aktivieren* auf Seite 16.

3.4.4.2.4 IP-Bereiche

Erstellen Sie ein Objekt für einen IP-Adressenbereich, um Hosts nach ihrer Start- und End-IP-Adresse zu gruppieren. Wenn ein DHCP-Server für das gewählte Interface konfiguriert ist, können Sie auch den Adressbereich des DHCP-Servers verwenden.

Übersicht IP-Bereiche

Navigieren Sie zu **Desktop** > **Desktop-Objekte** > **IP-Bereiche**, um die Liste der im System angelegten IP-Bereichsobjekte in der Leiste mit der Objektliste anzuzeigen.

In der erweiterten Ansicht zeigen die Tabellenspalten den **Objekt-Name** des IP-Bereichsobjekts an, mit welchem **Interface** er verbunden ist sowie seine **Start-IP** und **End-IP**. Mithilfe der Schaltflächen in der letzten Spalte können Sie die Einstellungen für ein vorhandenes IP-Bereichsobjekt einsehen und anpassen, ein neues Objekt ausgehend von einer Kopie eines vorhandenen IP-Bereichsobjekts anlegen oder ein Objekt aus dem System löschen.

Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28.

Einstellungen für IP-Bereiche

Mit den **IP-Bereich**-Einstellungen können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Name	Geben Sie einen Namen für das IP-Bereichsobjekt an.
Beschreibung	Optional: Geben Sie weitere Informationen zum IP-Bereichsobjekt für die interne Verwendung ein.
Tags	Optional: Wählen Sie aus der Drop-down-Liste die Desktop-Tags aus, die Sie dem IP-Bereichsobjekt zuweisen möchten. Weitere Informationen finden Sie unter *Desktop-Tags* auf Seite 129.
Farbe	Wählen Sie die Farbe aus, die für dieses Objekt auf dem Desktop verwendet werden soll.
Anmeldung erlauben	Aktivieren Sie dieses Kontrollkästchen, um Benutzern zu erlauben, sich mit dem IP-Bereich dieses Objekts auf Ihrer LANCOM R&S®Unified Firewall einzuloggen. Durch diese Einstellung können benutzerspezifische Firewall-Regeln auf den aktuell eingeloggten Benutzer angewendet werden.
Interface	Wählen Sie ein Interface, um es dem IP-Bereichsobjekt zuzuweisen. Wählen Sie `any`, wenn Sie das Objekt nicht einem bestimmten Interface zuweisen möchten. Mit dieser Einstellung akzeptieren alle Interfaces Pakete aus dem IP-Bereich dieses Objekts.
Start-IP	Geben Sie die Start-IP-Adresse des IP-Bereichs an.
End-IP	Geben Sie die End-IP-Adresse des IP-Bereichs an.

Wenn Sie den IP-Adressbereich des DHCP-Servers des gewählten Interface verwenden möchten, klicken Sie auf die Schaltfläche **DHCP-IP-Bereich verwenden** unten links im Bearbeitungsfenster.

Die Schaltflächen rechts unten im Bearbeitungsfeld sind davon abhängig, ob Sie ein neues IP-Bereichsobjekt hinzufügen oder ein bestehendes Objekt bearbeiten. Klicken Sie für ein neu konfiguriertes Objekt auf **Erstellen**, um es zur Liste der

verfügbaren IP-Bereichsobjekte hinzuzufügen, oder auf **Abbrechen**, um Ihre Änderungen zu verwerfen. Zum Bearbeiten eines vorhandenen Objekts klicken Sie auf **Speichern**, um das neu konfigurierte Objekt zu speichern, oder auf **Zurücksetzen**, um Ihre Änderungen zu verwerfen. Sie können auf **Schließen** klicken, um das Bearbeitungsfenster zu schließen, solange keine Änderungen darin vorgenommen wurden.

Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

3.4.4.2.5 Netzwerke

Erstellen Sie ein Netzwerkobjekt, das zur Erstellung von Verbindungen zwischen dem Netzwerk und weiteren Desktop-Objekten (z. B. VPN-Objekten) verwendet werden kann.

Übersicht Netzwerke

Navigieren Sie zu **Desktop** > **Desktop-Objekte** > **Netzwerke**, um die Liste der derzeit im System angelegten Netzwerk-Objekte in der Objektleiste anzuzeigen.

In der erweiterten Ansicht wird in den Tabellenspalten der **Name** und die **IP** des Netzwerkobjekts angezeigt und mit welchem **Interface** es verbunden ist. Mithilfe der Schaltflächen in der letzten Spalte können Sie die Einstellungen für ein vorhandenes Netzwerkobjekt einsehen und anpassen, ein neues Objekt ausgehend von einer Kopie eines vorhandenen Netzwerkobjekts anlegen oder ein Objekt aus dem System löschen.

Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28.

Netzwerkeinstellungen

Im Bearbeitungsfenster **Netzwerk** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Name	Geben Sie einen Namen für das Netzwerkobjekt an.
Beschreibung	Optional: Geben Sie weitere Informationen zum Netzwerkobjekt für die interne Verwendung ein.
Tags	Optional: Wählen Sie aus der Drop-down-Liste die Desktop-Tags aus, die Sie dem Netzwerkobjekt zuweisen möchten. Weitere Informationen finden Sie unter *Desktop-Tags* auf Seite 129.
Farbe	Wählen Sie die Farbe aus, die für dieses Objekt auf dem Desktop verwendet werden soll.
Anmeldung erlauben	Aktivieren Sie dieses Kontrollkästchen, um Benutzern zu erlauben, sich mit der IP-Adresse dieses Netzwerkobjekts auf Ihrer LANCOM R&S®Unified Firewall einzuloggen. Durch diese Einstellung können benutzerspezifische Firewall-Regeln auf den aktuell eingeloggten Benutzer angewendet werden.
Interface	Wählen Sie das Interface aus, mit dem das Netzwerk verbunden ist.
Netzwerk-IP	Geben Sie die IP-Adresse des Netzwerks in CIDR-Schreibweise ein (IP-Adresse gefolgt von einem Schrägstrich „/" und der Anzahl der in der Subnetzmaske festgelegten Bits, beispielsweise `192.168.50.0/24`).
Von IDS/IPS-Überprüfung ausnehmen	Nimmt dieses Netzwerkobjekt von der IDS/IPS-Überprüfung aus. ⓘ Ein Objekt kann auch bereits implizit von der Prüfung ausgeschlossen sein. Das ist der Fall, wenn es in einem Netzbereich liegt, der bereits durch ein übergeordnetes Objekt explizit von der Prüfung ausgenommen wurde. In diesem Fall erscheint ein entsprechedner Hinweis unterhalb der Checkbox, der auch die Namen der Objekte aufführt, von denen die Einstellung „geerbt" wurde.
Von Anti-Virus-Überprüfung ausnehmen	Nimmt dieses Netzwerkobjekt von der Anti-Virus-Überprüfung aus. ⓘ Ein Objekt kann auch bereits implizit von der Prüfung ausgeschlossen sein. Das ist der Fall, wenn es in einem Netzbereich liegt, der bereits durch ein übergeordnetes

Eingabefeld	Beschreibung
	Objekt explizit von der Prüfung ausgenommen wurde. In diesem Fall erscheint ein entsprechedner Hinweis unterhalb der Checkbox, der auch die Namen der Objekte aufführt, von denen die Einstellung „geerbt“ wurde.

Die Schaltflächen rechts unten im Bearbeitungsfeld sind davon abhängig, ob Sie ein neues Netzwerkobjekt hinzufügen oder ein bestehendes Objekt bearbeiten. Klicken Sie für ein neu konfiguriertes Objekt auf **Erstellen**, um es zur Liste der verfügbaren Netzwerkobjekte hinzuzufügen, oder auf **Abbrechen**, um Ihre Änderungen zu verwerfen. Zum Bearbeiten eines vorhandenen Netzwerks klicken Sie auf **Speichern**, um das neu konfigurierte Netzwerk zu speichern, oder auf **Zurücksetzen**, um Ihre Änderungen zu verwerfen. Sie können auf **Schließen** klicken, um das Bearbeitungsfenster zu schließen, solange keine Änderungen darin vorgenommen wurden.

Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

3.4.4.2.6 Benutzergruppen

Erstellen Sie Desktop-Objekte für Benutzer, die zum Einsehen aller Benutzer auf dem Desktop und zur Erstellung von Verbindungen zwischen mehreren Benutzern oder anderen Desktop-Objekten (z. B. VPN-Objekten) verwendet werden können.

Übersicht Benutzergruppen

Navigieren Sie zu **Desktop** > **Desktop-Objekte** > **Benutzergruppen**, um die Liste der derzeit im System angelegten Benutzergruppenobjekte in der Objektleiste anzuzeigen.

In der erweiterten Ansicht wird in der Tabelle der **Name** des Benutzergruppenobjekts angezeigt. Mithilfe der Schaltflächen in der letzten Spalte können Sie die Einstellungen für ein vorhandenes Benutzergruppenobjekt einsehen und anpassen, ein neues Objekt ausgehend von einer Kopie eines vorhandenen Benutzergruppenobjekts anlegen oder ein Objekt aus dem System löschen.

Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28.

Einstellungen für Benutzergruppen

Im Bearbeitungsfenster **Benutzergruppe** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Name	Geben Sie einen Namen für das Benutzergruppenobjekt an.
Beschreibung	Optional: Geben Sie weitere Informationen zum Benutzergruppenobjekt für die interne Verwendung ein.
Tags	Optional: Wählen Sie aus der Drop-down-Liste die Desktop-Tags aus, die Sie dem Benutzergruppenobjekt zuweisen möchten. Weitere Informationen finden Sie unter *Desktop-Tags* auf Seite 129.
Farbe	Wählen Sie die Farbe aus, die für dieses Objekt auf dem Desktop verwendet werden soll.
Benutzer	Wählen Sie die Benutzer, die Sie zur Gruppe hinzufügen möchten. Um einen einzelnen Benutzer hinzuzufügen, klicken Sie auf ⊕. ⓘ Benutzer können mehreren Gruppen angehören.

Die Schaltflächen rechts unten im Bearbeitungsfeld sind davon abhängig, ob Sie eine neue Benutzergruppe hinzufügen oder eine bestehende Gruppe bearbeiten. Klicken Sie für eine neu konfigurierte Gruppe auf **Erstellen**, um sie zur Liste der verfügbaren Benutzergruppen hinzuzufügen, oder auf **Abbrechen**, um Ihre Änderungen zu verwerfen. Zum Bearbeiten einer vorhandenen Gruppe klicken Sie auf **Speichern**, um die neu konfigurierte Gruppe zu speichern, oder auf

Zurücksetzen, um Ihre Änderungen zu verwerfen. Sie können auf **Schließen** klicken, um das Bearbeitungsfenster zu schließen, solange keine Änderungen darin vorgenommen wurden.

Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

3.4.4.2.7 Benutzer

Erstellen Sie Desktop-Objekte für Benutzer, die zum Einsehen aller Benutzer auf dem Desktop und zur Erstellung von Verbindungen zwischen mehreren Benutzern und anderen Desktop-Objekten (z. B. VPN-Objekten) verwendet werden können.

Mit dem Menü **Desktop** > **Desktop-Objekte** > **Benutzer** können nur Desktop-Objekte für Benutzer erstellt werden, die bereits im System angelegt sind. Weitere Informationen zum Hinzufügen und Verwalten von Benutzern finden Sie unter *Benutzerauthentifizierung* auf Seite 164.

Übersicht Benutzer

Navigieren Sie zu **Desktop** > **Desktop-Objekte** > **Benutzer**, um die Liste der derzeit im System angelegten Benutzerobjekte in der Objektleiste anzuzeigen.

In der erweiterten Ansicht werden in den Tabellenspalten der **Name** des Benutzerobjekts und der damit verbundene **Benutzername** angezeigt. Mithilfe der Schaltflächen in der letzten Spalte können Sie die Einstellungen für ein vorhandenes Benutzerobjekt einsehen und anpassen, ein neues Objekt ausgehend von einer Kopie eines vorhandenen Benutzerobjekts anlegen, oder ein Objekt aus dem System löschen.

Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28.

Benutzereinstellungen

Im Bearbeitungsfenster **Benutzer** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Objekt-Name	Geben Sie einen Namen für das Benutzerobjekt an.
Beschreibung	Optional: Geben Sie weitere Informationen zum Benutzerobjekt für die interne Verwendung ein.
Tags	Optional: Wählen Sie aus der Drop-down-Liste die Desktop-Tags aus, die Sie dem Benutzerobjekt zuweisen möchten. Weitere Informationen finden Sie unter *Desktop-Tags* auf Seite 129.
Farbe	Wählen Sie die Farbe aus, die für dieses Objekt auf dem Desktop verwendet werden soll.
Benutzername	Wählen Sie den Benutzer aus, der für dieses Objekt verwendet werden soll. Benutzer können mehreren Benutzerobjekten zugewiesen werden.

Die Schaltflächen rechts unten im Bearbeitungsfeld hängen davon ab, ob Sie ein neues Benutzerobjekt hinzufügen oder ein bestehendes Objekt bearbeiten. Klicken Sie für ein neu konfiguriertes Objekt auf **Erstellen**, um es zur Liste der verfügbaren Benutzerobjekte hinzuzufügen, oder auf **Abbrechen**, um Ihre Änderungen zu verwerfen. Zum Bearbeiten eines vorhandenen Objekts klicken Sie auf **Speichern**, um das neu konfigurierte Objekt zu speichern, oder auf **Zurücksetzen**, um Ihre Änderungen zu verwerfen. Sie können auf **Schließen** klicken, um das Bearbeitungsfenster zu schließen, solange keine Änderungen darin vorgenommen wurden.

Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

3.4.4.2.8 VPN-Gruppen

Erstellen Sie VPN-Gruppenobjekte, die zur Erstellung von Verbindungen zwischen mehreren VPN-Verbindungen oder anderen Desktop-Objekten (z. B. VPN-Objekten) verwendet werden können, indem ein gemeinsamer Regelsatz auf mehrere VPN-Verbindungen angewandt wird.

Übersicht VPN-Gruppen

Navigieren Sie zu **Desktop** > **Desktop-Objekte** > **VPN-Gruppen**, um die Liste der VPN-Gruppenobjekte, die derzeit im System angelegt sind, in der Leiste mit der Objektliste anzuzeigen.

In der erweiterten Ansicht wird in der Tabelle der **Name** des VPN-Gruppenobjekts angezeigt. Mithilfe der Schaltflächen in der letzten Spalte können Sie die Einstellungen für ein vorhandenes VPN-Benutzergruppenobjekt einsehen und anpassen, ein neues Objekt ausgehend von einer Kopie eines vorhandenen VPN-Benutzergruppenobjekts anlegen, oder ein Objekt aus dem System löschen.

Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28.

Einstellungen für VPN-Gruppen

Mit den **VPN-Gruppe**-Einstellungen können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung	
Name	Geben Sie einen Namen für das VPN-Gruppenobjekt an.	
Beschreibung	Optional: Geben Sie weitere Informationen zum VPN-Gruppenobjekt für die interne Verwendung ein.	
Tags	Optional: Wählen Sie aus der Drop-down-Liste die Desktop-Tags aus, die Sie dem VPN-Gruppenobjekt zuweisen möchten. Weitere Informationen finden Sie unter *Desktop-Tags* auf Seite 129.	
Farbe	Wählen Sie die Farbe aus, die für dieses Objekt auf dem Desktop verwendet werden soll.	
VPN-Verbindungen	Um VPN-Verbindungen zur VPN-Gruppe hinzuzufügen, klicken Sie auf ⊕. Es öffnet sich sich ein Fenster, in dem Sie die VPN-Verbindung auswählen bzw. bearbeiten.	
	Verbindungstyp	Wählen Sie den Typ der VPN-Verbindung aus, indem Sie die entsprechende Optionsschaltfläche auswählen.
	IPsec-Verbindung / **VPN-SSL-Verbindung**	Dieses Feld hängt vom gewählten Verbindungstyp ab. Wählen Sie aus der Drop-down-Liste die VPN-Verbindung aus, die Sie der VPN-Gruppe zuweisen möchten.
	Remote Netzwerke	Falls Sie eine IPsec-Verbindung ausgewählt haben, dann können Sie entweder alle konfigurierten remote Netzwerke verwenden oder die zu verwendenden remote Netzwerke explizit hinzufügen.
	ⓘ VPN-Verbindungen können mehreren VPN-Gruppen zugewiesen werden.	

Die Schaltflächen rechts unten im Bearbeitungsfeld sind davon abhängig, ob Sie ein neues VPN-Gruppenobjekt hinzufügen oder ein bestehendes Objekt bearbeiten. Klicken Sie für ein neu konfiguriertes Objekt auf **Erstellen**, um es zur Liste der verfügbaren VPN-Gruppenobjekte hinzuzufügen, oder auf **Abbrechen**, um Ihre Änderungen zu verwerfen. Zum Bearbeiten eines vorhandenen Objekts klicken Sie auf **Speichern**, um das neu konfigurierte Objekt zu speichern, oder auf **Zurücksetzen**, um Ihre Änderungen zu verwerfen. Sie können auf **Schließen** klicken, um das Bearbeitungsfenster zu schließen, solange keine Änderungen darin vorgenommen wurden.

Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

3.4.4.2.9 VPN-Hosts

Erstellen Sie ein VPN-Netzwerkobjekt, das zur Konfiguration von Firewall-Regeln für Client-to-Site VPN-Verbindungen verwendet werden kann.

Übersicht VPN-Hosts

Navigieren Sie zu **Desktop** > **Desktop-Objekte** > **VPN-Hosts**, um die Liste der VPN-Hostobjekte, die derzeit im System angelegt sind, in der Leiste mit der Objektliste anzuzeigen.

In der erweiterten Ansicht werden in den Tabellenspalten der **Name** des VPN-Hostobjekts, der **Typ** der VPN-Verbindung und die VPN-Verbindung angezeigt, zu der der VPN-Host gehört, an. Mithilfe der Schaltflächen in der letzten Spalte können Sie die Einstellungen für ein vorhandenes VPN-Hostobjekt einsehen und anpassen, ein neues Objekt ausgehend von einer Kopie eines vorhandenen VPN-Hostobjekts anlegen oder ein Objekt aus dem System löschen.

Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28.

Einstellungen für VPN-Hosts

Im Bearbeitungsfenster **VPN-Host** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Name	Geben Sie einen Namen für das VPN-Hostobjekt an.
Beschreibung	Optional: Geben Sie weitere Informationen zum VPN-Hostobjekt für die interne Verwendung ein.
Tags	Optional: Wählen Sie aus der Drop-down-Liste die Desktop-Tags aus, die Sie dem VPN-Hostobjekt zuweisen möchten. Weitere Informationen finden Sie unter *Desktop-Tags* auf Seite 129.
Farbe	Wählen Sie die Farbe aus, die für dieses Objekt auf dem Desktop verwendet werden soll.
Icon	Wählen Sie ein Symbol aus, mit dem das VPN-Hostobjekt auf dem Display dargestellt wird.
Verbindungstyp	Wählen Sie den Typ der VPN-Verbindung aus, indem Sie die entsprechende Optionsschaltfläche auswählen.
IPsec-Verbindung / **VPN-SSL-Verbindung**	Dieses Feld hängt vom gewählten VPN-Verbindungstyp ab. Wählen Sie aus der Drop-down-Liste die Verbindung aus, die Sie dem VPN-Hostobjekt zuweisen möchten.

Die Schaltflächen rechts unten im Bearbeitungsfeld hängen davon ab, ob Sie ein neues VPN-Hostobjekt hinzufügen oder ein bestehendes Objekt bearbeiten. Klicken Sie für ein neu konfiguriertes Objekt auf **Erstellen**, um es zur Liste der verfügbaren VPN-Hostobjekte hinzuzufügen, oder auf **Abbrechen**, um Ihre Änderungen zu verwerfen. Zum Bearbeiten eines vorhandenen Objekts klicken Sie auf **Speichern**, um das neu konfigurierte Objekt zu speichern, oder auf **Zurücksetzen**, um Ihre Änderungen zu verwerfen. Sie können auf **Schließen** klicken, um das Bearbeitungsfenster zu schließen, solange keine Änderungen darin vorgenommen wurden.

Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

3.4.4.2.10 VPN-Netzwerke

Erstellen Sie ein VPN-Netzwerkobjekt, das zur Konfiguration von Firewall-Regeln für Site-to-Site VPN-Verbindungen verwendet werden kann.

Übersicht VPN-Netzwerke

Navigieren Sie zu **Desktop** > **Desktop-Objekte** > **VPN-Netzwerke**, um die Liste der VPN- Netzwerkobjekte, die derzeit im System angelegt sind, in der Leiste mit der Objektliste anzuzeigen.

In der erweiterten Ansicht wird in den Tabellenspalten der **Name** des VPN-Netzwerkobjekts, der **Typ** der VPN-Verbindung und die VPN-Verbindung angezeigt, zu der das VPN-Netzwerk gehört, an. Mithilfe der Schaltflächen in der letzten Spalte

können Sie die Einstellungen für ein vorhandenes VPN-Netzwerkobjekt einsehen und anpassen, ein neues Objekt ausgehend von einer Kopie eines vorhandenen VPN-Netzwerkobjekts anlegen oder ein Objekt aus dem System löschen.

Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28.

Einstellungen für VPN-Netzwerke

Im Bearbeitungsfenster **VPN-Netzwerk** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Name	Geben Sie einen Namen für das VPN-Netzwerkobjekt an.
Beschreibung	Optional: Geben Sie weitere Informationen zum VPN-Netzwerkobjekt für die interne Verwendung ein.
Tags	Optional: Wählen Sie aus der Drop-down-Liste die Desktop-Tags aus, die Sie dem VPN-Netzwerkobjekt zuweisen möchten. Weitere Informationen finden Sie unter *Desktop-Tags* auf Seite 129.
Farbe	Wählen Sie die Farbe aus, die für dieses Objekt auf dem Desktop verwendet werden soll.
Verbindungstyp	Wählen Sie den Typ der VPN-Verbindung aus, indem Sie die entsprechende Optionsschaltfläche auswählen.
IPsec-Verbindung / **VPN-SSL-Verbindung**	Dieses Feld hängt vom gewählten Verbindungstyp ab. Wählen Sie aus der Drop-down-Liste die VPN-Verbindung aus, die Sie dem VPN-Netzwerkobjekt zuweisen möchten.
Remote Netzwerke	Falls Sie eine IPsec-Verbindung ausgewählt haben, dann können Sie entweder alle konfigurierten remote Netzwerke verwenden oder die zu verwendenden remote Netzwerke explizit hinzufügen.

Die Schaltflächen rechts unten im Bearbeitungsfeld hängen davon ab, ob Sie ein neues VPN-Netzwerkobjekt hinzufügen oder ein bestehendes Objekt bearbeiten. Klicken Sie für ein neu konfiguriertes Objekt auf **Erstellen**, um es zur Liste der verfügbaren VPN-Netzwerkobjekte hinzuzufügen, oder auf **Abbrechen**, um Ihre Änderungen zu verwerfen. Zum Bearbeiten eines vorhandenen Objekts klicken Sie auf **Speichern**, um das neu konfigurierte Objekt zu speichern, oder auf **Zurücksetzen**, um Ihre Änderungen zu verwerfen. Sie können auf **Schließen** klicken, um das Bearbeitungsfenster zu schließen, solange keine Änderungen darin vorgenommen wurden.

Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

3.4.4.2.11 VPN-Benutzergruppen

Erstellen Sie Desktop-Objekte für VPN-Benutzergruppen, die zur Erstellung von Verbindungen zwischen mehreren Benutzern oder anderen Desktop-Objekten verwendet werden können, indem ein gemeinsamer Regelsatz auf mehrere VPN-Benutzer angewandt wird. VPN-Benutzergruppen werden am VPN-Knoten auf dem Desktop angezeigt.

Übersicht VPN-Benutzergruppen

Navigieren Sie zu **Desktop** > **Desktop-Objekte** > **VPN-Benutzergruppen**, um die Liste der derzeit im System angelegten VPN-Benutzergruppenobjekte in der Objektleiste anzuzeigen.

In der erweiterten Ansicht wird in der Tabelle der **Name** des VPN-Benutzergruppenobjekts angezeigt. Mithilfe der Schaltflächen in der letzten Spalte können Sie die Einstellungen für ein vorhandenes VPN-Benutzergruppenobjekt einsehen und anpassen, ein neues Objekt ausgehend von einer Kopie eines vorhandenen VPN-Benutzergruppenobjekts anlegen, oder ein Objekt aus dem System löschen.

Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28.

Einstellungen für VPN-Benutzergruppen

Im Bearbeitungsfenster **VPN-Benutzergruppe** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Name	Geben Sie einen Namen für die VPN-Benutzergruppe an.
Beschreibung	Optional: Geben Sie weitere Informationen zur VPN-Benutzergruppe für die interne Verwendung ein.
Tags	Optional: Wählen Sie aus der Drop-down-Liste die Desktop-Tags aus, die Sie der VPN-Benutzergruppe zuweisen möchten. Weitere Informationen finden Sie unter *Desktop-Tags* auf Seite 129.
Farbe	Wählen Sie die Farbe aus, die für dieses Objekt auf dem Desktop verwendet werden soll.
Benutzer	Wählen Sie die Benutzer aus, die Sie zur Gruppe hinzufügen möchten. Um einen einzelnen Benutzer hinzuzufügen, klicken Sie auf ⊕. Benutzer können mehreren VPN-Benutzergruppen angehören.

Die Schaltflächen rechts unten im Bearbeitungsfeld hängen davon ab, ob Sie eine neue VPN-Benutzergruppe hinzufügen oder eine bestehende Gruppe bearbeiten. Klicken Sie für eine neu konfigurierte Gruppe auf **Erstellen**, um sie zur Liste der verfügbaren VPN-Benutzergruppen hinzuzufügen, oder auf **Abbrechen**, um Ihre Änderungen zu verwerfen. Zum Bearbeiten einer vorhandenen Gruppe klicken Sie auf **Speichern**, um die neu konfigurierte Gruppe zu speichern, oder auf **Zurücksetzen**, um Ihre Änderungen zu verwerfen. Sie können auf **Schließen** klicken, um das Bearbeitungsfenster zu schließen, solange keine Änderungen darin vorgenommen wurden.

Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

3.4.4.2.12 VPN-Benutzer

Erstellen Sie Desktop-Objekte für Benutzer, die in VPN-Verbindungen verwendet werden können. Die VPN-Benutzer werden am VPN-Knoten auf dem Desktop angezeigt.

Mit dem Menü **Desktop** > **Desktop-Objekte** > **VPN-Benutzer** können nur Desktop-Objekte für Benutzer erstellt werden, die bereits im System angelegt sind. Weitere Informationen zum Hinzufügen und Verwalten von Benutzern finden Sie unter *Benutzerauthentifizierung* auf Seite 164.

Übersicht VPN-Benutzer

Navigieren Sie zu **Desktop** > **Desktop-Objekte** > **VPN-Benutzer**, um die Liste der derzeit im System angelegten VPN-Benutzerobjekte in der Objektleiste anzuzeigen.

In der erweiterten Ansicht werden in den Tabellenspalten der **Objekt-Name** des VPN Benutzerobjekts und zusätzlich ein **Benutzername** angezeigt. Mithilfe der Schaltflächen in der letzten Spalte können Sie die Einstellungen für ein vorhandenes VPN-Benutzerobjekt einsehen und anpassen, ein neues Objekt ausgehend von einer Kopie eines vorhandenen VPN-Benutzerobjekts anlegen, oder ein Objekt aus dem System löschen.

Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28.

Einstellungen für VPN-Benutzer

Mit den **VPN-Benutzer**-Einstellungen können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Objekt-Name	Geben Sie einen Namen für das VPN-Benutzerobjekt an.
Beschreibung	Optional: Geben Sie weitere Informationen zum VPN-Benutzerobjekt für die interne Verwendung ein.

Eingabefeld	Beschreibung
Tags	Optional: Wählen Sie aus der Drop-down-Liste die Desktop-Tags aus, die Sie dem VPN-Benutzerobjekt zuweisen möchten. Weitere Informationen finden Sie unter *Desktop-Tags* auf Seite 129.
Farbe	Wählen Sie die Farbe aus, die für dieses Objekt auf dem Desktop verwendet werden soll.
Benutzername	Wählen Sie den Benutzer aus, der für dieses VPN-Benutzerobjekt verwendet werden soll. Benutzer können mehreren Benutzerobjekten zugewiesen werden.

Die Schaltflächen rechts unten im Bearbeitungsfeld hängen davon ab, ob Sie ein neues VPN-Benutzerobjekt hinzufügen oder ein bestehendes Objekt bearbeiten. Klicken Sie für ein neu konfiguriertes Objekt auf **Erstellen**, um es zur Liste der verfügbaren VPN- Benutzerobjekte hinzuzufügen, oder auf **Abbrechen**, um Ihre Änderungen zu verwerfen. Zum Bearbeiten eines vorhandenen Objekts klicken Sie auf **Speichern**, um das neu konfigurierte Objekt zu speichern, oder auf **Zurücksetzen**, um Ihre Änderungen zu verwerfen. Sie können auf **Schließen** klicken, um das Bearbeitungsfenster zu schließen, solange keine Änderungen darin vorgenommen wurden.

Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

3.4.4.2.13 LTA-Benutzergruppen

Erstellen Sie Desktop-Objekte für LTA-Benutzergruppen (LANCOM Trusted Access). Normalerweise werden diese hier nur angezeigt, da diese über die LANCOM Management Cloud verwaltet werden.

LANCOM Trusted Access ist die vertrauenswürdige Network Access Security-Lösung fur Unternehmensnetzwerke. Er ermöglicht einen sicheren und skalierenden Zugriff auf Unternehmensanwendungen für Mitarbeitende im Büro, zu Hause oder unterwegs und schützt damit modernes hybrides Arbeiten von überall und jederzeit. Die LANCOM Trusted Access-Lösung passt sich an steigende Sicherheitsanforderungen in Ihrer Organisation an und ermöglicht sowohl Cloud-managed VPN-Client-Vernetzung für den Zugriff auf ganze Netze als auch den Umstieg auf eine Zero-Trust-Sicherheitsarchitektur für eine umfassende Netzwerksicherheit. Dabei erhalten Benutzer auf Basis granularer Zugriffsrechte ausschließlich Zugangsberechtigung auf Anwendungen, die ihnen zugewiesen wurden (Zero-Trust-Prinzip). Bestehende Systeme zur Verwaltung von Benutzern und Benutzergruppen (Active Directory) lassen sich vollständig in die LANCOM Management Cloud (LMC) integrieren. Für kleinere Netzwerke bietet die LMC alternativ eine interne Benutzerverwaltung. LANCOM Trusted Access 100% DSGVO-konform und skaliert für Kleinunternehmen genauso wie für sehr große Netzwerke mit mehreren tausend Benutzern.

Übersicht LTA-Gruppen

Navigieren Sie zu **Desktop** > **Desktop-Objekte** > **LTA-Gruppen**, um die Liste der derzeit im System angelegten LTA-Benutzergruppenobjekte in der Objektleiste anzuzeigen.

Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28.

Einstellungen für LTA-Gruppen

Im Bearbeitungsfenster **LTA-Gruppe** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Name	Geben Sie einen Namen für die LTA-Gruppe an.
Beschreibung	Optional: Geben Sie weitere Informationen zur LTA-Gruppe für die interne Verwendung ein.
Gruppen-ID	Die Gruppen-ID, die im Zertifikat des Benutzers verwendet wird.
Tags	Optional: Wählen Sie aus der Drop-down-Liste die Desktop-Tags aus, die Sie der LTA-Gruppe zuweisen möchten. Weitere Informationen finden Sie unter *Desktop-Tags* auf Seite 129.
Farbe	Wählen Sie die Farbe aus, die für dieses Objekt auf dem Desktop verwendet werden soll.

Die Schaltflächen rechts unten im Bearbeitungsfeld hängen davon ab, ob Sie eine neue LTA-Gruppe hinzufügen oder eine bestehende Gruppe bearbeiten. Klicken Sie für eine neu konfigurierte Gruppe auf **Erstellen**, um sie zur Liste der verfügbaren LTA-Gruppen hinzuzufügen, oder auf **Abbrechen**, um Ihre Änderungen zu verwerfen. Zum Bearbeiten einer vorhandenen Gruppe klicken Sie auf **Speichern**, um die neu konfigurierte Gruppe zu speichern, oder auf **Zurücksetzen**, um Ihre Änderungen zu verwerfen. Sie können auf **Schließen** klicken, um das Bearbeitungsfenster zu schließen, solange keine Änderungen darin vorgenommen wurden.

Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

3.4.4.3 Desktopregeln

Mit den **Desktop-Regeln**-Einstellungen können Sie die Regeln zur Verwaltung des Netzwerksverkehrs anzeigen und bearbeiten. Weiterführende Informationen zur Erstellung von Firewall-Regeln finden Sie unter *Einstellungen für Firewall-Regeln* auf Seite 30.

Navigieren Sie zu **Desktop** > **Desktop-Regeln**, um die Liste der im System angelegten Regeln anzuzeigen.

Mit den **Filtereinstellungen** können Sie die Liste der Regeln eingrenzen und nur Regeln anzeigen, die einen bestimmten Suchbegriff enthalten. Sie können Inhalte filtern, indem Sie die gewünschten Optionen aus der Drop-down-Liste auswählen und / oder eine Sucheingabe im jeweiligen Eingabefeld eingeben. Klicken Sie auf **Anwenden**, um die gewählten Filteroptionen anzuwenden. Die Liste der Firewall-Regeln zeigt nun Ihre Filterergebnisse an. Klicken Sie auf **Zurücksetzen**, um die gewählten Filteroptionen wieder zu entfernen und eine ungefilterte Ansicht der Liste der Regeln anzuzeigen.

Die Tabellenspalten der Liste der Regeln enthalten die folgenden Informationen:

Spalte	Beschreibung
Objekt A	Diese Spalte zeigt das Quellobjekt der Verbindung an.
Richtung	Diese Spalte zeigt die Richtung an, in die die Regel angewandt wird.
Objekt B	Diese Spalte zeigt das Zielobjekt der Verbindung an.
Dienst	Diese Spalte zeigt den Namen des Dienstes der Regel an.

Mit den Schaltflächen in der letzten Spalte können Sie die Einstellungen für eine vorhandene Verbindung einsehen und bearbeiten. Klicken Sie auf ✎, um den Dialog **Verbindung** zu öffnen. Weiterführende Informationen zur Erstellung von Firewall-Regeln und zum Bearbeiten von Verbindungen finden Sie unter *Einstellungen für Firewall-Regeln* auf Seite 30 und *Desktopverbindungen* auf Seite 114.

Um das Fenster **Desktop-Regeln** zu schließen und zum Desktop zurückzukehren, klicken Sie auf ✖ in der oberen rechten Ecke des Fensters.

3.4.4.4 Desktop-Tags

Unter **Desktop-Tags** können Sie eine Liste von Tags anlegen, die Sie beliebigen Desktopobjekten zuordnen können, mit Ausnahme des **Firewall**-Rootknotens und der Hauptknoten (z. B. **Intranet**). Mit diesen Tags können Sie eine gefilterte Desktopansicht anzeigen, um sich nach Ihren Bedürfnissen eine Übersicht Ihres konfigurierten Netzwerks zu erstellen. Weitere Informationen finden Sie unter *Desktop* auf Seite 25.

Wenn Sie ein Backup einer LCOS FX-Version vor 10.0 wiederherstellen, werden die Ebenen und Regionen, die in dieser Version erstellt wurden, in Tags umgewandelt. Alle Desktop-Objekte, die auf einer Ebene oder Region liegen, werden mit den umgewandelten Tags markiert.

3.4.4.4.1 Übersicht Desktop-Tags

Navigieren Sie zu **Desktop** > **Desktop-Tags**, um die Liste der im System angelegten Desktop-Tags in der Leiste mit der Objektliste anzuzeigen.

In der erweiterten Ansicht wird in der ersten Spalte der Tabelle der **Name** des Desktop-Tags angezeigt. Mithilfe der Schaltflächen in der letzten Spalte können Sie die Einstellungen für einen vorhandenen Desktop-Tag einsehen und

anpassen, einen neuen Tag auf der Grundlage einer Kopie eines bestehenden Desktop-Tags anlegen oder einen Tag aus dem System löschen.

Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28.

Wenn Sie auf einen Eintrag in der Objektleiste klicken, werden das entsprechende Desktop-Objekt und alle Verbindungen, die diesen Dienst verwenden, auf dem Desktop hervorgehoben. Wenn Sie auf den Knoten eines Desktop-Objekts klicken, während die Objektleiste mit den **Desktop-Tags** offen ist, werden die diesem Desktop-Objekt zugewiesenen Desktop-Tags darin hervorgehoben.

3.4.4.4.2 Einstellungen für Desktop-Tags

Unter **Desktop** > **Desktop-Tags** können Sie einen neuen Desktop-Tag hinzufügen, oder einen vorhandenen bearbeiten.

Im Bearbeitungsfenster **Desktop-Tag** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Name	Geben Sie einen Namen für den Desktop-Tag ein.

Die Schaltflächen rechts unten im Bearbeitungsfeld hängen davon ab, ob Sie einen neuen Desktop-Tag hinzufügen oder einen bestehenden Tag bearbeiten. Klicken Sie für einen neu konfigurierten Desktop-Tag auf **Erstellen**, um ihn zur Liste der verfügbaren Desktop-Tags hinzuzufügen, oder auf **Abbrechen**, um Ihre Änderungen zu verwerfen. Zum Bearbeiten eines vorhandenen Desktop-Tags klicken Sie auf **Speichern**, um den neu konfigurierten Tag zu speichern, oder auf **Zurücksetzen**, um Ihre Änderungen zu verwerfen. Sie können auf **Schließen** klicken, um das Bearbeitungsfenster zu schließen, solange keine Änderungen darin vorgenommen wurden.

Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

3.4.4.5 Dienste

Navigieren Sie zu **Desktop** > **Dienste**, um die Liste der im System angelegten Dienste und Dienstgruppen in der Objektleiste anzuzeigen. Dienste sind Protokolle oder Kombinationen aus Protokollen und Ports, falls die Protokolle Ports wie z. B. TCP und UDP verwenden. Wenn Sie auf einen Eintrag in der Objektleiste klicken, werden das entsprechende Desktop-Objekt und alle Verbindungen, die diesen Dienst verwenden, auf dem Desktop hervorgehoben. Wenn Sie auf ein Objekt auf dem Desktop klicken, werden in der Liste diejenigen Dienste hervorgehoben, die von diesem Objekt verwendet werden.

Um einen benutzerdefinierten Dienst oder eine Dienstgruppe zu erstellen, klicken Sie auf die Schaltfläche ⊕ oben im entsprechenden Abschnitt der Objektleiste.

Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28.

Die nachfolgenden Abschnitte enthalten weitere Informationen zu den verschiedenen Typen von Diensten und Dienstgruppen.

3.4.4.5.1 Vordefinierte Dienste

Navigieren Sie zu **Desktop** > **Dienste** > **Vordefinierte Dienste**, um die Liste der derzeit im System angelegten vordefinierten Dienste in der Objektleiste anzuzeigen.

In der erweiterten Ansicht wird in den Tabellenspalten der **Name** des jeweiligen Dienstes angezeigt, ob der Dienst in einer Verbindung verwendet wird (grün), oder nicht (orange), und – soweit verfügbar – die **Ports** und Protokolle, die der Dienst verwendet.

Die voreingestellten Dienste stehen zur Verwendung in benutzerdefinierten Firewall-Regeln zur Verfügung (siehe *Erstellen einer Firewall-Regel* auf Seite 31).

3.4.4.5.2 Dienstgruppen

Mit den **Dienst-Gruppen**-Einstellungen können Sie vordefinierte und benutzerdefinierte Dienste in eine Dienstgruppe einordnen. Somit können Sie ähnliche Regelsätze auf verschiedene Verbindungen anwenden, ohne jeden Dienst einzeln hinzufügen zu müssen.

Übersicht Dienstgruppen

Navigieren Sie zu **Desktop** > **Dienste** > **Dienst-Gruppen**, um die Liste der im System angelegten Dienstgruppen in der Leiste mit der Objektliste anzuzeigen.

In der erweiterten Ansicht werden in der Tabelle der **Name** der Dienstgruppe und die Anzahl der **Dienste** in der Gruppe angezeigt. Anhand der Schaltflächen in der letzten Spalte können Sie die Einstellungen für eine vorhandene Dienstgruppe einsehen und anpassen, eine neue Gruppe ausgehend von einer Kopie einer vorhandenen Dienstgruppe anlegen oder eine Dienstgruppe aus dem System löschen.

Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28.

Einstellungen für Dienstgruppen

Nutzen Sie die Einstellungen unter **Dienst-Gruppen**, um Dienstgruppen zu konfigurieren.

Unter **Desktop** > **Dienste** > **Dienst-Gruppen** können Sie eine neue Dienstgruppe hinzufügen oder eine vorhandene bearbeiten.

Im Fenster **Dienst-Gruppe** können Sie die folgenden Informationen einsehen und die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Name	Geben Sie einen Namen für die Dienstgruppe ein.
Dienste	Zusammen mit dem **Dienst-Gruppe**-Fenster öffnet sich rechts im Browserfenster eine Leiste mit einer Dienstauswahlliste, die alle aktuell im System angelegten Dienste enthält. Die Leiste ist in Kategorien von Diensten mit einer jeweils ähnlichen Funktion eingeteilt. Die Kategorien können mit einem Klick auf das entsprechende Symbol ein- und ausgeklappt werden. Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28. Mithilfe des **Filter**-Eingabefelds oben in der Leiste mit der Liste der Dienste können Sie schnell und einfach einen bestimmten Dienst finden. Während Sie Ihre Suche in das Eingabefeld eintippen, werden nur diejenigen Dienste angezeigt, die die eingegebenen Zeichen enthalten. Klicken Sie im Eingabefeld auf ⊗, um die Sucheingabe zu löschen und zur ungefilterten Listenansicht zurückzukehren. Um einen einzelnen Dienst zur Dienstgruppe hinzuzufügen, klicken Sie auf ⊕ vor dem jeweiligen Dienst in der Leiste mit der Dienstauswahlliste. Um alle Dienste einer Kategorie gleichzeitig hinzuzufügen, klicken Sie auf die Schaltfläche ⊕ direkt unter dem Titel der jeweiligen Kategorie. Die Dienste erscheinen zusammen mit den ihnen zugeordneten Ports und / oder Protokollen als Einträge in der Liste. Um einen Dienst aus der Gruppe zu entfernen, klicken Sie neben dem Eintrag auf 🗑. ⓘ Mit der Schaltfläche **Dienste löschen** unten links im Fenster löschen Sie alle Dienste in der Gruppe gleichzeitig.

Die Schaltflächen rechts unten im Bearbeitungsfeld hängen davon ab, ob Sie eine neue Dienstgruppe hinzufügen oder eine bestehende Gruppe bearbeiten. Klicken Sie für eine neu konfigurierte Dienstgruppe auf **Erstellen**, um die Gruppe zur Liste der verfügbaren Dienstgruppen hinzuzufügen, oder auf **Abbrechen**, um die Erstellung einer neuen Dienstgruppe abzubrechen. Zum Bearbeiten einer vorhandenen Dienstgruppe klicken Sie auf **Speichern**, um die neu konfigurierte Gruppe zu speichern, oder auf **Zurücksetzen**, um Ihre Änderungen zu verwerfen. Sie können auf **Schließen** klicken, um das Bearbeitungsfenster zu schließen, solange keine Änderungen darin vorgenommen wurden.

Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

Die hier definierten Dienstgruppen stehen zur Verwendung in benutzerdefinierten Firewall-Regeln zur Verfügung (weiterführende Informationen finden Sie unter *Erstellen einer Firewall-Regel* auf Seite 31).

3.4.4.5.3 Benutzerdefinierte Dienste

Wenn Sie einen Port oder ein Protokoll benötigen, das nicht von einem der vordefinierten Dienste (siehe *Vordefinierte Dienste* auf Seite 130) abgedeckt ist, können Sie einen benutzerdefinierten Dienst erstellen, der auf eine Verbindung angewandt werden kann.

Navigieren Sie zu **Desktop** > **Dienste** > **Benutzerdef. Dienste**, um die Liste der im System angelegten benutzerdefinierten Dienste in der Objektliste anzuzeigen.

Übersicht benutzerdefinierte Dienste

In der erweiterten Ansicht wird in den Tabellenspalten der **Name** des jeweiligen Dienstes angezeigt, ob der Dienst in einer Verbindung verwendet wird (grün), oder nicht (orange) und (soweit verfügbar) die **Ports** und Protokolle, die der Dienst verwendet. Anhand der Schaltflächen in der letzten Spalte können Sie die Einstellungen für einen benutzerdefinierten Dienst einsehen und anpassen, einen neuen Dienst ausgehend von einer Kopie eines vorhandenen benutzerdefinierten Dienstes anlegen, oder einen benutzerdefinierten Dienst aus dem System löschen.

Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28.

Einstellungen für benutzerdefinierte Dienste

Unter **Desktop** > **Dienste** > **Benutzerdef. Dienste** können Sie einen neuen benutzerdefinierten Dienst hinzufügen oder einen vorhandenen benutzerdefinierten Dienst bearbeiten.

Im Bearbeitungsfenster **Benutzerdefinierte Dienste** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Name	Geben Sie einen Namen für den benutzerdefinierten Dienst ein.
Ports / Protokolle	Um den benutzerdefinierten Dienst zu erweitern, sodass er auf Verkehr zu bestimmten Protokollen und / oder Ports oder Portbereichen angewandt wird, klicken Sie auf **Hinzufügen**. Das Fenster **Dienst bearbeiten** öffnet sich. Mithilfe dieses Fensters können Sie die Ports und Protokolle definieren, die verwendet werden sollen: › Der **Quell-Port** kann optional für die Protokolle TCP bzw. UDP beschränkt werden. Wenn Sie die Option **Quell-Port beschränken** auswählen, dann können Sie für TCP bzw. UDP einzelne Ports oder Bereiche angeben, um den Dienst auf Verkehr anzuwenden, der von einem Quellport übertragen wird. Verwenden Sie die Eingabefelder **Quell-Port von** und **Bis**, um Werte einzugeben. Als Eingabewert ist jede ganze Zahl zwischen `1` und `65535` möglich. **Quell-Port von** und **Bis** ergeben zusammen einen Portbereich. Um einen einzelnen Port einzugeben, geben Sie in beide Felder denselben Wert ein oder lassen Sie **Bis** frei. › Geben Sie für die Protokolle TCP bzw. UDP einzelne Ports oder Bereiche an, um den Dienst auf Verkehr anzuwenden, der von dort zu einem bestimmten Zielport übertragen wird. Verwenden Sie die Eingabefelder **Ziel-Port von** und **Bis**, um Werte einzugeben. Als Eingabewert ist jede ganze Zahl zwischen `1` und `65535` möglich. **Ziel-Port von** und **Bis** ergeben zusammen einen Portbereich. Um einen einzelnen Port einzugeben, geben Sie in beide Felder denselben Wert ein oder lassen Sie **Bis** frei.

Eingabefeld	Beschreibung
	› Geben Sie ein Protokoll an, auf das der Dienst angewendet werden soll, indem Sie es aus der Liste auswählen. Definieren Sie fehlende Protokolle ggf. unter *Protokolle* auf Seite 133. Mit den Schaltflächen unten rechts im Bearbeitungsfenster können Sie Ihre Änderungen speichern (**OK**) oder verwerfen (**Abbrechen**). Das Fenster **Dienst bearbeiten** schließt sich automatisch. Die angegebenen Ports / Portbereiche und / oder das Protokoll erscheinen als Listeneintrag. Sie können einzelne Einträge in den Listen bearbeiten oder löschen, indem Sie auf die entsprechende Schaltfläche neben einem Eintrag klicken. Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28.

Die Schaltflächen rechts unten im Bearbeitungsfeld hängen davon ab, ob Sie einen neuen benutzerdefinierten Dienst hinzufügen oder einen bestehenden bearbeiten. Klicken Sie für einen neu konfigurierten benutzerdefinierten Dienst auf **Erstellen**, um ihn zur Liste der verfügbaren Dienste hinzuzufügen, oder auf **Abbrechen**, um Ihre Änderungen zu verwerfen. Zum Bearbeiten eines vorhandenen benutzerdefinierten Dienstes klicken Sie auf **Speichern**, um den benutzerdefinierten Dienst zu speichern, oder auf **Zurücksetzen**, um Ihre Änderungen zu verwerfen. Sie können auf **Schließen** klicken, um das Bearbeitungsfenster zu schließen, solange keine Änderungen darin vorgenommen wurden.

Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

Die hier definierten benutzerdefinierten Dienste stehen zur Verwendung in benutzerdefinierten Firewall-Regeln zur Verfügung (weiterführende Informationen finden Sie unter *Erstellen einer Firewall-Regel* auf Seite 31).

3.4.4.6 Protokolle

Navigieren Sie zu **Desktop** > **Protokolle**, um die Liste der im System angelegten Protokolle in der Objektleiste anzuzeigen. Protokolle sind Kombinationen aus dem Namen des Protokolls und den zugehörigen Ports.

Die nachfolgenden Abschnitte enthalten weitere Informationen zu den vordefinierten bzw. vom Benutzer definierten Protokollen.

3.4.4.6.1 Vordefinierte Protokolle

Navigieren Sie zu **Desktop** > **Protokolle** > **Vordefinierte Protokolle**, um die Liste der derzeit im System angelegten vordefinierten Protokolle und des zugehörigen Ports anzuzeigen. Bei den vordefinierten Protokollen handelt es sich um ICMP, TCP, UDP, GRE, ESP, AH, IGMP, OSPF und VRRP.

Die Protokolle stehen zur Verwendung in benutzerdefinierten Diensten zur Verfügung (siehe *Benutzerdefinierte Dienste* auf Seite 132).

3.4.4.6.2 Benutzerdefinierte Protokolle

Wenn Sie einen Port oder ein Protokoll benötigen, das nicht von einem der vordefinierten Protokolle abgedeckt ist, können Sie ein benutzerdefiniertes Protokoll erstellen, das bei einem Dienst verwendet werden kann.

Navigieren Sie zu **Desktop** > **Protokolle** > **Benutzerdefinierte Protokolle**, um die Liste der im System angelegten benutzerdefinierten Protokolle in der Objektliste anzuzeigen.

Hier können Sie einen neues benutzerdefiniertes Protokoll hinzufügen oder ein vorhandenes benutzerdefiniertes Protokoll bearbeiten.

Im Bearbeitungsfenster **Protokoll** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Protokollnummer	Eine Protokollnummer von 0 bis 255 kann gewählt werden. Die vorgeschlagenen Werte entsprechen denen der *IANA*.

Eingabefeld	Beschreibung
	Bereits verwendete Protokollnummern werden nicht angezeigt. Durch direkte Eingabe der Nummer können diese jedoch erneut verwendet werden. Wird ein bekanntes Protokoll verwendet, wird der Name automatisch vorgeschlagen. Alle anderen Protokollnummern werden als benutzerdefiniertes Protokoll gekennzeichnet und der Name wird nicht automatisch vorausgefüllt.
Name	Übernehmen Sie den vorgeschlagenen Namen oder geben Sie einen eigenen Namen für dieses benutzerdefinierte Protokoll ein.

Die Schaltflächen rechts unten im Bearbeitungsfeld hängen davon ab, ob Sie ein neues benutzerdefiniertes Protokoll hinzufügen oder ein bestehendes bearbeiten. Klicken Sie für ein neu konfiguriertes benutzerdefiniertes Protokoll auf **Erstellen**, um es zur Liste der verfügbaren Protokolle hinzuzufügen, oder auf **Abbrechen**, um Ihre Änderungen zu verwerfen. Zum Bearbeiten eines vorhandenen benutzerdefinierten Protokolls klicken Sie auf **Speichern**, um das benutzerdefinierte Protokoll zu speichern, oder auf **Zurücksetzen**, um Ihre Änderungen zu verwerfen. Sie können auf **Schließen** klicken, um das Bearbeitungsfenster zu schließen, solange keine Änderungen darin vorgenommen wurden.

Die hier definierten benutzerdefinierten Protokolle stehen zur Verwendung in benutzerdefinierten Diensten zur Verfügung (weiterführende Informationen finden Sie unter *Benutzerdefinierte Dienste* auf Seite 132).

3.4.5 UTM

Mit den **UTM** Einstellungen können Sie neue Anwendungsfilterprofile erstellen oder bestehende bearbeiten, URL- und Contentfilter definieren sowie Antivirus-Anwendungen, E-Mail-Sicherheitseinstellungen und Proxies konfigurieren, um Ihr Netzwerk zu schützen.

3.4.5.1 Antivirus-Einstellungen

Ihre LANCOM R&S®Unified Firewall schützt Ihr internes Netzwerk mit einem integrierten Virenscanner von Avira vor Computerviren.

Der Virenscanner ist in der UTM-Lizenz enthalten. Wenn Sie Ihre LANCOM R&S®Unified Firewall das erste Mal starten, läuft der Virenscanner 30 Tage als Testversion. Nach Ablauf dieser Frist wird der Virenscanner automatisch deaktiviert. Weitere Informationen finden Sie unter *Lizenz* auf Seite 47.

Navigieren Sie zu **UTM** > **Antivirus-Einstellungen**, um einen Konfigurationsdialog zu öffnen, in dem Sie die Antivirus-Einstellungen für Ihren Web- und E-Mail-Proxy anzeigen, aktivieren und anpassen können.

Im Fenster **Antivirus-Einstellungen** können Sie die folgenden Informationen einsehen und konfigurieren:

Eingabefeld	Beschreibung
Lizenz	Dieses Feld zeigt die Lizenzinformationen zu Ihrem Virenscanner an.
Updates	Dieses Feld zeigt das Datum des letzten Aktualisierungsversuches des Virenscanners an. Klicken Sie auf **Jetzt Updaten**, um den Virenscanner manuell zu aktualisieren.
Letztes erfolgreiches Update	Dieses Feld zeigt Datum und Uhrzeit der letzten erfolgreichen Aktualisierung des Virenscanners an.

Scanner

Im Tab **Scanner** aktivieren oder deaktivieren Sie den Virenscanner für E-Mail, HTTP(S) und FTP und passen die Antivirus-Einstellungen an.

Bei einem Download wird die Datei von der LANCOM R&S®Unified Firewall zuerst heruntergeladen und erst nach einem negativen Scan an das Endgerät gesendet. Dabei erfolgt der Download auf der LANCOM R&S®Unified Firewall mit voller Geschwindigkeit. Währenddessen sendet die LANCOM R&S®Unified Firewall lediglich einen

Datenstrom mit sehr geringer Bandbreite an das Endgerät, um den Download aufrecht zu erhalten. Nach Abschluss des Vorgangs auf der LANCOM R&S®Unified Firewall wird die Datei dann mit voller Geschwindigkeit an das Endgerät ausgeliefert. Gerade bei großen Dateien kann dies den Eindruck erwecken, dass die Download-Geschwindigkeit zu gering ist und es gegebenenfalls ein Performance-Problem gibt. Es handelt sich hierbei aber um einen ganz normalen Vorgang.

Eingabefeld	Beschreibung
Cloud-Scan aktivieren	Dieses Häkchen ist standardmäßig nicht gesetzt. Setzen Sie das Häkchen, um das Scannen von Dateien in der Bitdefender Cloud zu erlauben. Wird eine Datei von der lokalen Antivirus-Anwendung nicht als Bedrohung identifiziert, aber als Risiko eingestuft, wird ein Hash und einige anonyme Meta-Informationen der Datei, sowie Details der lokalen Überprüfung der Datei an die Bitdefender Cloud gesendet. Falls der Hash bekannt ist, wird dies als Ergebnis zurückgesendet. Falls der Hash unbekannt ist und es sich um eine ausführbare Datei handelt, wird die Datei in die Bitdefender Cloud hochgeladen und überprüft. Dieser Abgleich findet nur statt, wenn die lokale Antivirus-Anwendung das Risiko der Datei als ausreichend hoch einstuft.

Die folgenden Einstellungen sind jeweils für **Mail** bzw. **HTTP(s) und FTP** getrennt einstellbar.

Eingabefeld	Beschreibung
Aktiv	Zwei Schiebeschalter geben an, ob der Virenscanner für E-Mail und/oder HTTP(S) und FTP derzeit aktiv (**I**) oder inaktiv (**0**) ist. Mit einem Klick auf den jeweiligen Schiebeschalter ändern Sie den Status dieser Option. Diese Optionen sind für alle Dienste standardmäßig aktiviert.
Max. zu scannende Datei-Größe	Stellen Sie die maximal zu scannende Datei-Größe in MB ein (Min: 1 MB, Max: 4096 MB).
Dateien bei Überschreiten der max. Datei-Größe blockieren	Falls eine Datei die maximale Datei-Größe für eine zu scannende Datei überschreitet, dann kann sie blockiert werden. Wenn Sie diese Option deaktivieren, dann werden die Dateien ohne Antiviren-Scan heruntergeladen.
Fehlerhaft gescannte Dateien blockieren	Setzen Sie dieses Häkchen, um E-Mails zu blockieren und/oder den Download von Dateien in HTTP(S) und FTP abzubrechen, falls der Virenscanner deren Überprüfung nicht erfolgreich abschließen konnte. Falls also während der Überprüfung ein Fehler auftritt, wird die E-Mail blockiert und der Empfänger wird darüber informiert. Wenn Sie das Häkchen entfernen, erhält der Empfänger eine Ersatz-E-Mail, die die Original-E-Mail als verschlüsselten Anhang zusammen mit dem zur Entschlüsselung benötigten Passwort enthält.
Archivdateien scannen	Dieses Häkchen ist standardmäßig gesetzt. Entfernen Sie das Häkchen, wenn Sie nicht möchten, dass der Virenscanner archivierte Dateien auf Viren überprüft.

Whitelist

Im Tab **Whitelists** setzen Sie vertrauenswürdige Hosts und Server auf eine Whitelist. Daten, die von diesen Hosts über HTTP oder FTP übertragen werden sowie E-Mail-Adressen werden nicht auf Viren überprüft.

Geben Sie im Eingabefeld **Vertrauenswürdige HTTP / FTP-Quellen** die IP-Adresse oder den Domainnamen des vertrauenswürdigen Hosts oder Servers ein.

Die Einträge, um mehrere Einträge über Platzhalterzeichen darzustellen, unterscheiden sich für HTTP(S)/FTP und E-Mail.

- Für HTTP(S)/FTP: Um eine Domain „example.com“ inklusive aller Subdomains wie z. B. „www.example.com“ freizugeben, schreiben Sie „.example.com“ mit einem Punkt am Anfang. Um nur die Domain „example.com“ ohne Subdomains freizugeben, schreiben Sie „example.com“ ohne einen Punkt am Anfang.
- Für E-Mail:
  - Einträge mit einem Punkt am Anfang verhalten sich genau wie die für HTTP(S)/FTP.
  - Einträge beginnend mit „*@“ bzw. „@“ oder ohne „@“ im Text werden nur mit dem Domainteil einer E-Mail-Adresse verglichen. Der Vergleich muss exakt passen. So würde „@test.de“ zu allen Adressen mit `@test.de` passen, aber z. B. nicht auf `@subdomain.test.de`.
  - Eine vollständige E-Mail-Adresse passt nur zu exakt dieser Adresse.

Klicken Sie auf ⊕, um den Host oder Server zur Liste hinzuzufügen.

Sie können einzelne Einträge in den Listen bearbeiten oder löschen, indem Sie auf die entsprechende Schaltfläche neben einem Eintrag klicken.

Wenn Sie einen Eintrag bearbeiten, erscheint auf der rechten Seite des Eintrags ein Haken. Setzen Sie den Haken im Kontrolkästchen, um Ihre Änderungen zu übernehmen.

Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28.

Klicken Sie auf **Export**, um Ihre Whitelist in das Dateisystem zu exportieren. Klicken Sie auf **Import**, um eine Whitelist zu importieren.

Um vertrauenswürdige E-Mail-Adressen hinzuzufügen, wählen Sie unter **Vertrauenswürdige Mail-Adressen** aus den folgenden Optionen aus:

- **Sender**

  Alle von diesen E-Mail-Adressen aus gesendeten E-Mails werden vom Virenscanner ausgeschlossen.
- **Empfänger**

  Alle an diese E-Mail-Adressen gesendeten E-Mails werden vom Virenscanner ausgeschlossen.
- **Sender / Empfänger**

  Alle E-Mails, die von ODER an diese E-Mail-Adresse gesendet werden, werden vom Virenscanner ausgeschlossen.

Klicken Sie auf ⊕, um die E-Mail-Adresse zur Liste hinzuzufügen.

Sie können einzelne Einträge in den Listen bearbeiten oder löschen, indem Sie auf die entsprechende Schaltfläche neben einem Eintrag klicken.

Wenn Sie einen Eintrag bearbeiten, erscheint auf der rechten Seite des Eintrags ein Haken. Setzen Sie den Haken im Kontrolkästchen, um Ihre Änderungen zu übernehmen.

Update

Im Tab **Updates** richten Sie automatische Aktualisierungen des Virenscanners ein:

Eingabefeld	Beschreibung
Update-Server	Der Standard-Updateserver ist: http://cybersecurity.rohde-schwarz.com/updateserver/av Fügen Sie eine beliebige Anzahl an Update-Servern hinzu. Geben Sie im Eingabefeld die URL des Servers ein und klicken Sie dann auf ⊕. Der Server wird zur Liste hinzugefügt.

Eingabefeld	Beschreibung
	Die Liste der Update-Server wird von oben nach unten abgearbeitet. Sobald der erste Update-Server erreicht wird, werden die weiteren Alternativen in diesem Update-Prozess nicht kontaktiert. Sie können einzelne Einträge in den Listen bearbeiten oder löschen, indem Sie auf die entsprechende Schaltfläche neben einem Eintrag klicken. Wenn Sie einen Eintrag bearbeiten, erscheint auf der rechten Seite des Eintrags ein Haken. Setzen Sie den Haken im Kontrolkästchen, um Ihre Änderungen zu übernehmen. Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28.
Automatische Updates	Geben Sie Datum und Uhrzeit der ersten automatischen Aktualisierung des Virenscanners ein. Sie können das Datum im Format `MM/TT/JJJJ` eingeben oder im Auswahlfenster ein Datum auswählen. Geben Sie die Uhrzeit im Format `hh:mm:ss` ein. Geben Sie ein **Intervall** in Stunden ein, mit dem der Virenscanner aktualisiert werden soll. Wenn Sie an dieser Stelle `0 h` eingeben, wird die Aktualisierung sofort durchgeführt. Klicken Sie auf ⊕, um den Aktualisierungsplan zur Liste hinzuzufügen. Sie können einzelne Einträge in den Listen bearbeiten oder löschen, indem Sie auf die entsprechende Schaltfläche neben einem Eintrag klicken. Wenn Sie einen Eintrag bearbeiten, erscheint auf der rechten Seite des Eintrags ein Haken. Setzen Sie den Haken im Kontrolkästchen, um Ihre Änderungen zu übernehmen. Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28.

Wenn Sie Änderungen vorgenommen haben, können Sie diese mit den Schaltflächen unten rechts im Bearbeitungsfenster speichern (**Speichern**) oder verwerfen (**Zurücksetzen**). Andernfalls können Sie das Fenster schließen (**Schließen**).

Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

Die Antivirus-Einstellungen für bestimmte Protokolle (HTTP, FTP, E-Mail) werden nur auf Datenverkehr angewandt, der mit einer Regel mit einem für dieses Protokoll aktiven Proxy übereinstimmt. Um einen Proxy zu konfigurieren, navigieren Sie zu den Proxyeinstellungen und erstellen oder bearbeiten Sie eine Firewall-Regel, um den Proxy für das entsprechende Protokoll zu aktivieren (siehe auch *HTTP(S)-Proxy-Einstellungen* auf Seite 144 und *E-Mail Sicherheit* auf Seite 140).

3.4.5.2 Application-Management

Mit dem Application-Management filtern Sie Datenverkehr im Netzwerk auf der Basis des Verhaltens des Datenstroms. So können Teile einer Anwendung, wie z. B. der Chatfunktion von Skype, systematisch ausgefiltert werden, selbst wenn diese verschlüsselt sind.

In einigen Fällen, z. B. im Fall von Skype, kann der Filter des Application-Managements Anwendungen erst einordnen, wenn eine bestimmte Anzahl an Paketen ausgetauscht wurde. Das bedeutet, dass ein Erstkontakt nicht verhindert werden kann. Alle weiteren Pakete werden dann aber blockiert.

3.4.5.2.1 Einstellungen

Mit den **Application-Filter-Einstellungen** können Sie Filter generell aktivieren oder deaktivieren.

Eingabefeld	Beschreibung
I/0	Ein Schiebeschalter gibt an, ob das Application-Management aktiv (**I**) oder inaktiv (**0**) ist. Mit einem Klick auf den Schiebeschalter ändern Sie den Status dieser Option. Das Application-Management ist standardmäßig deaktiviert.
Lizenz	Zeigt die Lizenzinformationen zu Ihrem Application-Filter an. Weitere Informationen finden Sie unter *Lizenz* auf Seite 47.
CA für SSL-Überwachung	Diese Zertifizierungsstelle wird vom Applikations-Filter verwendet, um Pseudo-Zertifikate zu erstellen, wenn SSL-Interception in dem Profil aktiviert wurde.

Wenn Sie Änderungen vorgenommen haben, können Sie diese mit den Schaltflächen unten rechts im Bearbeitungsfenster speichern (**Speichern**) oder verwerfen (**Zurücksetzen**). Andernfalls können Sie das Fenster schließen (**Schließen**).

Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

3.4.5.2.2 Filter-Profile

Navigieren Sie zu **UTM** > **Application-Management** > **Filter-Profile**, um die Liste der im System angelegten Filter-Profile des Application-Managements in der Objektleiste anzuzeigen.

In der erweiterten Ansicht werden in den Tabellenspalten der **Name** des Profils und die Anzahl der ausgewählten Protokolle und Anwendungen angezeigt. Mithilfe der Schaltflächen in der letzten Spalte können Sie die Einstellungen für ein vorhandenes Application-Filter-Profil einsehen und anpassen, ein neues Profil auf der Grundlage einer Kopie eines vorhandenen Profils anlegen oder ein Profil aus dem System löschen.

Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28.

Mit den **Application-Filter-Profil** Einstellungen können Sie die folgenden Optionen konfigurieren:

Eingabefeld	Beschreibung
Profilname	Geben Sie einen Namen für das Filter-Profil an.
SSL-Überwachung	Setzen Sie den Haken in diesem Kontrollkästchen, um SSL-Untersuchung zu aktivieren. Durch SSL-Untersuchung kann Ihre LANCOM R&S®Unified Firewall den über SSL-verschlüsselte Verbindungen gerouteten eingehenden Datenverkehr auswerten und das konfigurierte Filter-Profil darauf anwenden.
Regeln	Wählen Sie die Protokolle und Anwendungen aus, die Sie zum Profil hinzufügen möchten. Die Protokolle und Anwendungen werden in der Tabelle nach **Kategorie** geordnet. Mit dem **Filter**-Eingabefeld können Sie die Liste der Protokolle und Anwendungen filtern, sodass nur Einträge angezeigt werden, die mit Ihrer Sucheingabe übereinstimmen. Klicken Sie auf ⊗, um die ungefilterte Liste der Protokolle und Anwendungen anzuzeigen. Klicken Sie auf die Schaltfläche › neben einer Kategorie, um die Protokolle und Anwendungen, die sie enthält, zusammen mit einer kurzen Beschreibung anzuzeigen. Wählen Sie ganze Kategorien oder einzelne Protokolle oder Anwendungen aus, indem Sie einen Haken in den entsprechenden Kontrollkästchen setzen. Entfernen Sie den Haken im Kontrollkästchen neben einer Kategorie, einem Protokoll oder einer Anwendung, um diese aus dem Application-Filter-Profil zu entfernen. Um Protokolle und Anwendungen auszublenden, klicken Sie auf die Schaltfläche ⌄ neben der Kategorie.

Die Schaltflächen rechts unten im Bearbeitungsfeld hängen davon ab, ob Sie ein neues Filter-Profil hinzufügen oder ein bestehendes Profil bearbeiten. Klicken Sie für ein neu konfiguriertes Profil auf **Erstellen**, um es zur Liste der verfügbaren Profile hinzuzufügen, oder auf **Abbrechen**, um Ihre Änderungen zu verwerfen.

Wenn Sie Änderungen vorgenommen haben, können Sie diese mit den Schaltflächen unten rechts im Bearbeitungsfenster speichern (**Speichern**) oder verwerfen (**Zurücksetzen**). Andernfalls können Sie das Fenster schließen (**Schließen**).

Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

Die hier definierten Filter-Profile stehen zur Verwendung in benutzerdefinierten Firewall-Regeln zur Verfügung, in denen die ausgewählten Protokolle und Anwendungen auf der Blacklist stehen (weiterführende Informationen finden Sie unter *Firewall* auf Seite 33 und *Einstellungen für Desktopverbindungen* auf Seite 115).

3.4.5.2.3 Routing-Profile

Navigieren Sie zu **UTM** > **Application-Management** > **Routing-Profile**, um die Liste der im System angelegten Routing-Profile des Application Managements in der Objektleiste anzuzeigen.

In der erweiterten Ansicht werden in den Tabellenspalten der **Name** des Profils und die Anzahl der ausgewählten Protokolle und Anwendungen angezeigt. Mithilfe der Schaltflächen in der letzten Spalte können Sie die Einstellungen für ein vorhandenes Routing-Profil einsehen und anpassen, ein neues Profil auf der Grundlage einer Kopie eines vorhandenen Profils anlegen oder ein Profil aus dem System löschen.

Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28.

Mit den Einstellungen für **Routing-Profile** können Sie die folgenden Optionen konfigurieren:

Eingabefeld	Beschreibung
Name	Geben Sie einen Namen für das Routing-Profil an.
Internet-Verbindung	Konfiguriert die Internet-Verbindung über die der Traffic geleitet werden soll.
Traffic-Gruppe	Wählen Sie optional den Namen einer Traffic-Gruppe aus. Dadurch werden die für diese Gruppe definierten Regeln für den Datenverkehr angewendet, der vom Application Filter den im Routing-Profil ausgewählten Regeln zugeordnet wird. Dafür muss der Datenverkehr zunächst auch der Desktop-Verbindung entsprechen, in der das bearbeitete App-Routing-Profil verwendet wird. Siehe auch *Traffic Shaping* auf Seite 105.
Proxy umgehen	Setzen Sie den Haken in diesem Kontrollkästchen, um die Umgehung des Proxys zu aktivieren. Dadurch wird der Traffic nicht über den Proxy geleitet. Damit ist es insbesondere möglich, bestimmte Applikationen vom Proxy auszunehmen, zum Beispiel Applikationen für mobile Geräte, die Certificate Pinning erzwingen.
IPsec umgehen	Setzen Sie den Haken in diesem Kontrollkästchen, um die Umgehung eines IPsec-Tunnels zu aktivieren. Dadurch wird der Traffic nicht über IPsec-Tunnel geleitet. Dieses Feature kann unter Anderem für Zweigstellen genutzt werden, die ihren gesamten Internet-Verkehr per IPsec durch eine Zentrale leiten. Hier macht es häufig Sinn, bestimmte vertrauenswürdige Applikationen, die eine niedrige Latenz brauchen, wie zum Microsoft Office 365, vom der Umleitung durch die Zentrale auszunehmen.
DSCP ausgehend	Wählen Sie einen optionalen DSCP-Wert für ausgehenden Datenverkehr aus der Liste aus. Die Liste enthält die Bezeichnungen aus den relevanten RFCs (z. B. „CS0“) und der Gruppe (z. B. „Standard“). Zusätzlich wird der Wert ebenfalls in seiner numerischen Repräsentation zu verschiedenen Basen (binär, hexadezimal und dezimal) angezeigt. Die Liste kann entsprechend dieser Darstellungen durchsucht werden, so dass Sie unabhängig von der individuell bevorzugten Darstellung schnell den gewünschten Wert finden.
Regeln	Wählen Sie die Protokolle und Anwendungen aus, die Sie zum Profil hinzufügen möchten. Die Protokolle und Anwendungen werden in der Tabelle nach **Kategorie** geordnet. Mit dem **Filter**-Eingabefeld können Sie die Liste der Protokolle und Anwendungen filtern, sodass nur Einträge angezeigt werden, die mit Ihrer Sucheingabe übereinstimmen. Klicken Sie auf ⊗, um die ungefilterte Liste der Protokolle und Anwendungen anzuzeigen. Klicken Sie auf die Schaltfläche › neben einer Kategorie, um die Protokolle und Anwendungen, die sie enthält, zusammen mit einer kurzen Beschreibung anzuzeigen. Wählen Sie ganze Kategorien oder einzelne Protokolle oder Anwendungen aus, indem Sie einen Haken in den entsprechenden Kontrollkästchen setzen. Entfernen Sie den Haken im Kontrollkästchen neben einer Kategorie, einem Protokoll oder einer Anwendung, um diese aus dem Application-Filter-Profil zu entfernen. Um Protokolle und Anwendungen auszublenden, klicken Sie auf die Schaltfläche ⌄ neben der Kategorie.

Die Schaltflächen rechts unten im Bearbeitungsfeld hängen davon ab, ob Sie ein neues Routing-Profil hinzufügen oder ein bestehendes Profil bearbeiten. Klicken Sie für ein neu konfiguriertes Profil auf **Erstellen**, um es zur Liste der verfügbaren Profile hinzuzufügen, oder auf **Abbrechen**, um Ihre Änderungen zu verwerfen.

Wenn Sie Änderungen vorgenommen haben, können Sie diese mit den Schaltflächen unten rechts im Bearbeitungsfenster speichern (**Speichern**) oder verwerfen (**Zurücksetzen**). Andernfalls können Sie das Fenster schließen (**Schließen**).

Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

Die hier definierten Routing-Profile stehen als Application Based Routing zur Verwendung in benutzerdefinierten Firewall-Regeln zur Verfügung. Weiterführende Informationen finden Sie unter *Firewall* auf Seite 33 und *Einstellungen für Desktopverbindungen* auf Seite 115.

3.4.5.3 E-Mail Sicherheit

Unter **UTM** > **E-Mail-Sicherheit** können Sie Einstellungen zu Ihren E-Mail- und Spamfiltern vornehmen.

3.4.5.3.1 Antispam-Einstellungen

Sie können Ihre LANCOM R&S®Unified Firewall konfigurieren, um Ihr System vor Spam-E-Mail zu schützen.

Der Spamfilter ist in der UTM-Lizenz enthalten. Wenn Sie Ihre LANCOM R&S®Unified Firewall das erste Mal starten, läuft der Spamfilter 30 Tage als Testversion. Nach Ablauf dieser Frist wird der Spamfilter automatisch deaktiviert. Weitere Informationen zu den Lizenzen finden Sie unter *Lizenz* auf Seite 47.

Navigieren Sie zu **UTM** > **E-Mail-Sicherheit** > **Antispam-Einstellungen**, um ein Bearbeitungsfenster zu öffnen, in dem Sie die Spamfilter-Einstellungen anzeigen, aktivieren und anpassen können.

Im Fenster **Antispam Einstellungen** können Sie die folgenden Informationen einsehen und die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
I/0	Ein Schiebeschalter gibt an, ob der jeweilige Antispam aktiv (**I**) oder inaktiv (**0**) ist. Mit einem Klick auf den Schiebeschalter ändern Sie den Status dieser Option. Diese Option ist standardmäßig aktiviert.
Lizenz	Dieses Feld zeigt die Lizenzinformationen zu Ihrem Spamfilter an.
Spam-Erkennung	Wählen Sie eine der folgenden Optionen aus, indem Sie auf die entsprechende Schaltfläche klicken: › **Bestätigt** – E-Mails, die bekannte und verifizierte Spam-Muster enthalten, werden als Spam eingestuft. › **Masse** – Zusätzlich zur Einstellung `Confirmed` werden E-Mails von Mailkonten, die bekanntermaßen Massenmails verschicken, als Spam eingeordnet (dies ist die Standardeinstellung). › **Verdächtig** – Zusätzlich zu den Einstellungen `Confirmed` und `Bulk` werden E-Mails von Mailkonten, die verdächtige Mengen an E-Mails versenden, als Spam eingeordnet.
Spam-Markierung	Legen Sie fest, wie Spam gekennzeichnet wird, indem Sie eine der folgenden Optionen auswählen: › **Header** – Die originale E-Mail wird in der Kopfzeile als Spam markiert. › **Betreff** – Die originale E-Mail wird in der Kopfzeile als Spam markiert. Der Betreff wird entsprechend der Betreffsformatierung geändert (Standardeinstellung). › **Anhang** – Eine als Spam erkannte E-Mail wird an eine neue E-Mail angehängt, die sowohl im Betreff (entsprechend der Betreffsformatierung) als auch in der Kopfzeile als Spam markiert ist.

Eingabefeld	Beschreibung
Betreffzeile	Legen Sie fest, wie E-Mails, die als Spam identifiziert wurden, markiert werden. Sie können selbst einen Text für die Markierung im Betreff wählen. Verwenden Sie die folgenden Variablen: `%SUBJECT%` (originaler Betreff der Spam-E-Mail), `%SPAMCLASS%` und `%SPAMCLASSNUM%` (Spamkategorie). Klicken Sie auf ↺,um die Markierung auf die Standardeinstellung `*****SPAM*****  [%SUBJECT%]` zu setzen.
Mail-Listen	Sie können eine Blacklist und / oder eine Whitelist anlegen, indem Sie eine beliebige Anzahl an E-Mail-Adressen zur jeweiligen Liste hinzufügen. Beide Adresslisten können zur selben Zeit angewandt werden. Für beide Listen bestehen zwei Möglichkeiten, E-Mail-Adressen hinzuzufügen. › E-Mail-Adressen können manuell hinzugefügt werden, indem Sie eine Adresse in das Eingabefeld eintragen und anschließend auf **Hinzufügen** klicken. › E-Mail-Adressen können auch aus einer Textdatei importiert werden. Klicken Sie dazu unter der entsprechenden Liste auf **Import** und öffnen Sie die gewünschte Datei. Die maximale Dateigröße für Importe beträgt standardmäßig 1 Megabyte. Jede nicht leere Zeile der ausgewählten Textdatei wird als Eintrag zur entsprechenden Liste hinzugefügt. Sie können eine Adressliste komplett als Textdatei auf die lokale Festplatte exportieren, indem Sie rechts unter der entsprechenden Liste auf **Export** klicken. Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28. Die E-Mail-Adressen in jeder der Adresslisten können die folgenden Platzhalter enthalten: * für Wörter, ? für einzelne Zeichen.

Wenn Sie Änderungen vorgenommen haben, können Sie diese mit den Schaltflächen unten rechts im Bearbeitungsfenster speichern (**Speichern**) oder verwerfen (**Zurücksetzen**). Andernfalls können Sie das Fenster schließen (**Schließen**).

Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

Die hier festgelegten Antispam-Einstellungen für das Mailprotokoll werden nur auf Datenverkehr angewandt, der mit einer Regel mit einem für dieses Protokoll aktiven Proxy übereinstimmt. Außerdem muss der Proxy wie unter *Einstellungen für Mail-Filter* auf Seite 141 beschrieben aktiviert werden.

3.4.5.3.2 Einstellungen für Mail-Filter

Unter **UTM** > **E-Mail-Sicherheit** > **Mailfilter Einstellungen** aktivieren Sie den Mailproxy Ihrer LANCOM R&S®Unified Firewall. Sobald Sie den Mailproxy aktiviert haben, können Sie E-Mails nach ihrer Zieladresse filtern. Wenn sie ausgefiltert werden, erreichen diese E-Mails den Empfänger und / oder den Mailserver nicht.

Im Bearbeitungsfenster **Mailfilter Einstellungen** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
I/0	Ein Schiebeschalter gibt an, ob der Mail-Proxy derzeit aktiv (**I**) oder inaktiv (**0**) ist. Mit einem Klick auf den Schiebeschalter ändern Sie den Status dieser Option. Diese Option ist standardmäßig deaktiviert.
Filter-Modus	Wählen Sie die Optionsschaltfläche mit dem gewünschten Filtermodus aus. Wenn **Blacklist** (Standardeinstellung) ausgewählt wurde, werden E-Mails von allen Adressen auf der Blacklist (siehe unten) keinesfalls zum Mailserver weitergeleitet. Wenn Sie **Whitelists** auswählen, werden ausschließlich Adressen auf der Whitelist (siehe unten) zum Mailserver weitergeleitet.
Aktion	Wählen Sie die Schaltfläche mit der Aktion, die Sie auf die gefilterten E-Mails anwenden möchten. Während **E-Mails ablehnen** (Standardeinstellung) unerwünschte E-Mails mit einer RFC-konformen Antwort ablehnt, verwirft **E-Mails löschen** unerwünschte E-Mails und lässt den Sender glauben, dass die E-Mail den Mailserver erreicht hat.

Eingabefeld	Beschreibung
	Die Option **E-Mails löschen** ist NICHT RFC-konform. Eine falsche Konfiguration kann dazu führen, dass wichtige E-Mails gelöscht werden.
Blacklist / **Whitelists**	Je nach ausgewähltem Filtermodus können Sie beliebig viele E-Mail-Adressen zu einer Blacklist oder einer Whitelist hinzufügen. Für beide Listen bestehen folgende Möglichkeiten, E-Mail-Adressen hinzuzufügen: › E-Mail-Adressen können manuell hinzugefügt werden, indem Sie eine Adresse in das Eingabefeld eintragen und anschließend auf **Hinzufügen** klicken. › Alternativ können E-Mail-Adressen auch aus einer Textdatei importiert werden, indem Sie auf **Import** klicken und die gewünschte Datei öffnen. Die maximale Dateigröße für Importe beträgt standardmäßig 1 Megabyte. Jede nicht leere Zeile der ausgewählten Textdatei wird als Eintrag zur entsprechenden Liste hinzugefügt. Sie können einzelne Einträge in der Liste bearbeiten oder löschen, indem Sie auf die entsprechende Schaltfläche neben einem Eintrag klicken. Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28. Sie können die komplette Liste der Mail-Filter als Textdatei auf die lokale Festplatte exportieren, indem Sie rechts unter entsprechenden Liste auf **Export** klicken. Die E-Mail-Adressen in jeder der Adresslisten können die folgenden Platzhalter enthalten: * für Wörter, ? für einzelne Zeichen.

Wenn Sie Änderungen vorgenommen haben, können Sie diese mit den Schaltflächen unten rechts im Bearbeitungsfenster speichern (**Speichern**) oder verwerfen (**Zurücksetzen**). Andernfalls können Sie das Fenster schließen (**Schließen**).

Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

Nur wenn der Mailproxy aktiviert wurde, werden die weiteren Mailfilter-, Antispam- und Antivirus-Einstellungen aktiv. Weitere Informationen finden Sie unter *Antispam-Einstellungen* auf Seite 140 und *Antivirus-Einstellungen* auf Seite 134.

Wenn Sie sowohl im Mail-Filter als auch in Firewall-Regeln SSL-Untersuchung verwenden, müssen Sie Ihre Zertifizierungsstelle zum Truststore Ihrer LANCOM R&S®Unified Firewall und Ihrer Clientgeräte hinzufügen.

3.4.5.4 IDS / IPS

Das Intrusion Detection / Prevention System („IDS / IPS“) pflegt eine Datenbank bekannter Bedrohungen, um die Computer in Ihrem Netzwerk vor einem breiten Spektrum von feindlichen Angriffen zu schützen, Warnmeldungen auszugeben, wenn solche Bedrohungen festgestellt werden, und die Kommunikationsverbindung zu feindlichen Quellen zu beenden. Das System zur Erkennung und Bekämpfung von Netzwerkbedrohungen basiert auf Suricata.

Seine Bedrohungsdatenbank besteht aus einem von ProofPoint bereitgestellten, ausführlichen Regelsatz. Dieser Regelsatz enthält eine Blacklist mit IP-Adressen, Muster zur Erkennung von Malware in Kommunikationsverbindungen, Muster für Netzwerk-Scans, Muster für Brute-Force-Angriffe und mehr. Im IDS-Modus generiert die IDS / IPS-Vorrichtung lediglich Warnmeldungen, wenn eine Regel auf den Datenverkehr zutrifft. Im IPS-Modus generiert die IDS / IPS-Vorrichtung Warnmeldungen und blockiert bösartigen Datenverkehr zusätzlich. Sobald Sie IDS / IPS aktivieren, sind alle Regeln standardmäßig aktiv. Falls Dienste fälschlicherweise im Netzwerk von IDS / IPS blockiert werden, können Sie die IDS / IPS-Vorrichtung so konfigurieren, dass sie die Regel ignoriert, die den falschen Alarm ausgelöst hat.

Wenn die IDS / IPS-Vorrichtung aktiviert ist, scannt sie durchgehend den gesamten Datenverkehr.

IDS / IPS ist in der UTM-Lizenz enthalten. Wenn Sie Ihre LANCOM R&S®Unified Firewall das erste Mal starten, läuft IDS / IPS 30 Tage als Testversion. Nach Ablauf dieser Frist wird IDS / IPS automatisch deaktiviert. Weitere Informationen zu den Lizenzen finden Sie unter *Lizenz* auf Seite 47.

Navigieren Sie zu **UTM** > **IDS/IPS**, um ein Bearbeitungsfenster zu öffnen, in dem Sie die IDS / IPS-Einstellungen anzeigen, aktivieren und anpassen können.

Im Bearbeitungsfenster **IDS/IPS** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
I/0	Ein Schiebeschalter gibt an, ob der jeweilige IDS / IPS aktiv (**I**) oder inaktiv (**0**) ist. Klicken Sie auf den Schiebeschalter, um den Status von IDS / IPS zu ändern. IDS / IPS ist standardmäßig deaktiviert.
IDS/IPS-Lizenz	Dieses Feld zeigt die Lizenzinformationen zu IDS / IPS an.
Modus	Wählen Sie den gewünschten IDS / IPS-Modus aus, indem Sie die entsprechende Optionsschaltfläche auswählen. Die folgenden Modi sind verfügbar: › **IDS (Ereignisse loggen)** – In diesem Modus werden Ereignisse lediglich aufgezeichnet. Es wird keine Aktion ausgelöst. › **IPS Drop (Pakete verwerfen und loggen)** – Wenn ein Ereignis ausgelöst wird, werden die Pakete in Verbindung mit dem Ereignis ohne Mitteilung an den Absender verworfen. Ein Protokolleintrag wird erstellt. › **IPS Reject (Pakete ablehnen und loggen)** – Wenn ein Ereignis ausgelöst wird, werden die Pakete in Verbindung mit dem Ereignis abgelehnt. Bei TCP-Verbindungen sendet Ihre LANCOM R&S®Unified Firewall hierzu ein RST-Paket an den Absender und erstellt einen Protokolleintrag (siehe auch *Protokolle* auf Seite 69).

Im Tab **Regeln** legen Sie IDS / IPS-Regeln fest, die ignoriert werden sollen. Fügen Sie beliebig viele Regeln hinzu.

Eingabefeld	Beschreibung
SID	Geben Sie die eindeutige Signatur-ID (SID) einer Regel ein und klicken Sie auf ⊕, um die Regel zur Liste hinzuzufügen. Sie können einzelne Einträge in der Liste bearbeiten oder löschen, indem Sie auf die entsprechende Schaltfläche neben einem Eintrag klicken. Die SID einer Regel entnehmen Sie dem entsprechenden Protokolleintrag (siehe auch *Protokolle* auf Seite 69). Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28.
Beschreibung	Optional: In dieses Eingabefeld können Sie zusätzliche Informationen zur IDS / IPS-Regel, die ignoriert werden soll, eintragen. Wenn Sie dieses Feld freilassen, wird es automatisch gefüllt, sobald Ihre LANCOM R&S®Unified Firewall auf eine Regel stößt, die mit der Signatur-ID übereinstimmt.

Alternativ können Sie IDS / IPS-Regeln, die ignoriert werden sollen, aus dem Systemprotokoll auswählen und hinzufügen. Weitere Informationen finden Sie unter *Systemprotokoll* auf Seite 73.

Mit der Schaltfläche **Ignorierte Regeln löschen** unten links im Bearbeitungsfenster können Sie alle ignorierten IDS / IPS-Regeln gleichzeitig entfernen.

Im Tab können Sie Profile für automatische IDS / IPS-Aktualisierungen erstellen:

Eingabefeld	Beschreibung
Von	Geben Sie den Zeitpunkt der ersten automatischen IDS / IPS-Aktualisierung ein. Sie können das Datum im Format `MM/TT/JJJJ` eingeben oder im Auswahlfenster ein Datum auswählen. Geben Sie die Uhrzeit im Format `hh:mm:ss` ein.

Eingabefeld	Beschreibung
Intervall	Geben Sie das Aktualisierungsintervall für IDS / IPS in Stunden an. Wenn Sie 0 Stunden eingeben, wird die Aktualisierung sofort durchgeführt.

Klicken Sie auf **Hinzufügen**, um das Profil zur Liste hinzuzufügen. Sie können einzelne Einträge in der Liste bearbeiten oder löschen, indem Sie auf die entsprechende Schaltfläche neben einem Eintrag klicken.

Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28.

Wenn Sie Änderungen vorgenommen haben, können Sie diese mit den Schaltflächen unten rechts im Bearbeitungsfenster speichern (**Speichern**) oder verwerfen (**Zurücksetzen**). Andernfalls können Sie das Fenster schließen (**Schließen**).

Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

3.4.5.5 Proxy

Ein Proxy nimmt Anfragen stellvertretend entgegen und maskiert diese nach außen hinter der eigenen Adresse.

Unter **UTM** > **Proxy** können Sie die Einstellungen zu HTTP(S)-, E-Mail- und VoIP-Proxys anpassen.

3.4.5.5.1 HTTP(S)-Proxy-Einstellungen

Ihre LANCOM R&S®Unified Firewall verwendet den Proxy Squid. Dieser Proxy dient als Schnittstelle zum Contentfilter und zum Virenscanner (siehe *URL- / Contentfilter* auf Seite 149 und *Antivirus-Einstellungen* auf Seite 134).

Unter **UTM** > **Proxy** > **HTTP-Proxy-Einstellungen** können Sie den HTTP(S)-Proxy Ihrer LANCOM R&S®Unified Firewall konfigurieren.

Der HTTP(S)-Proxy dient als Mittelsmann. Er stellt eine Verbindung zum Webserver her, generiert mithilfe seiner eigenen HTTP(S)-Proxy-CA ein Pseudo-Zertifikat für die Website und verwendet dieses, um eine Verbindung zum Browser herzustellen. So kann der Proxy den Datenverkehr analysieren, URL- und Contentfilter anwenden und nach Viren suchen.

Stellen Sie sicher, dass der DNS-Server die Domains, auf die zugegriffen wird, korrekt auflösen kann, wenn der HTTP(S)-Proxy aktiv ist. Importieren Sie außerdem die HTTP(S)-Proxy-CA Ihrer LANCOM R&S®Unified Firewall als vertrauenswürdige Zertifizierungsstelle in die Browser aller Clients.

Eingabefeld	Beschreibung
I/0	Ein Schiebeschalter gibt an, ob der HTTP(S) Proxy derzeit aktiv (**I**) oder inaktiv (**0**) ist. Mit einem Klick auf den Schiebeschalter können Sie unabhängig von den konfigurierten Proxy-Modi den Status dieses Dienstes ändern. Der HTTP(S)-Proxy ist standardmäßig deaktiviert. Mit Aktivieren oder Deaktivieren des HTTP(S)-Proxy wird der FTP-Proxy ebenfalls aktiviert oder deaktiviert.
Klartext-HTTP-Proxy	Um den HTTP-Proxy zu deaktivieren, wählen Sie die „Proxy deaktivieren"-Option aus. Wenn Sie **Transparent** auswählen, leitet Ihre LANCOM R&S®Unified Firewall automatisch alle Anfragen, die auf Port 80 (HTTP) eintreffen, über den Proxy weiter (Standardeinstellung). Wenn Sie **Intransparent** auswählen, muss der HTTP-Proxy Ihrer LANCOM R&S®Unified Firewall explizit auf Port 10080 eingestellt sein.
HTTPS Proxy	Um den HTTPS-Proxy zu deaktivieren, wählen Sie die Option **Proxy deaktivieren** aus. Sie können den HTTPS-Proxy unabhängig vom HTTP-Proxy konfigurieren. Wenn Sie **Transparent** auswählen, leitet Ihre LANCOM R&S®Unified Firewall automatisch alle Anfragen, die auf Port 443 (HTTPS) eintreffen, über den Proxy weiter (Standardeinstellung). Wenn Sie **Intransparent** auswählen, muss der HTTPS-Proxy Ihrer Firewall explizit auf Port 10443 eingestellt sein.
Proxy CA	Die Zertifizierungsstelle wird vom HTTP(S)-Proxy verwendet, um Pseudo-Zertifikate auszustellen.

Eingabefeld	Beschreibung
	Je nach Zertifikatstyp schlägt Ihre LANCOM R&S®Unified Firewall vor, welche Zertifikate nützlich sind und welche nicht. Die Zertifizierungsstelle wird nur angezeigt, wenn der **HTTPS Proxy** auf **Transparent** oder **Intransparent** eingestellt ist.
Client-Authentifizierung	Nur verfügbar, wenn **Klartext-HTTP-Proxy** oder **HTTPS Proxy** auf **Intransparent** eingestellt sind. Setzen Sie den Haken in diesem Kontrollkästchen, um die HTTP(S)-Client-Authentifizierung mithilfe der LANCOM R&S®Unified Firewall Benutzerverwaltung zu aktivieren. Wenn Sie **Client-Authentifizierung** aktivieren, wird der FTP-Proxy deaktiviert. In diesem Fall wird eine Warnmeldung angezeigt. Der Proxy kann nur HTTP-Datenpakete verarbeiten. Wenn ein Programm versucht, Datenpakete anderer Protokolle an diesen Port zu übermitteln, werden die Pakete blockiert.
Whitelists	Sie können separate Whitelists für einzelne Domänengruppen festlegen. Eine Domaingruppe besteht aus einem Namen, einer optionalen Beschreibung und einer Liste von URLs (Domains), die von SSL-Untersuchung, Virenscanner und URL-Filter ausgeschlossen werden sollen. Sie können einer Domaingruppe beliebig viele Domains hinzufügen. Geben Sie eine Domain ein und klicken Sie auf ⊕, um sie zur Liste hinzuzufügen. Domaingruppen auf der Whitelist werden vom HTTP(S)-Proxy ohne Analyse akzeptiert und sind direkt im Browser des Benutzers verfügbar. Es werden keine Zertifikate erstellt. Diese Einstellung wird für Dienste benötigt, die striktes Certificate Pinning verwenden (Beispiel: Windows Update unter `windowsupdate.com`). Sie können eine Domaingruppe bearbeiten oder löschen, indem Sie auf die entsprechende Schaltfläche neben einem Eintrag klicken. Setzen oder Enfernen Sie den Haken im Kontrollkästchen links von einer Domaingruppe, um deren Verwendung zu aktivieren oder abzuschalten. Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28. Um eine Domain „example.com“ inklusive aller Subdomains wie z. B. „www.example.com“ freizugeben, schreiben Sie „.example.com“ mit einem Punkt am Anfang. Um nur die Domain „example.com“ ohne Subdomains freizugeben, schreiben Sie „example.com“ ohne einen Punkt am Anfang.

Wenn Sie Änderungen vorgenommen haben, können Sie diese mit den Schaltflächen unten rechts im Bearbeitungsfenster speichern (**Speichern**) oder verwerfen (**Zurücksetzen**). Andernfalls können Sie das Fenster schließen (**Schließen**).

Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

3.4.5.5.2 Mail-Proxy-Einstellungen

Mithilfe dieses Mail-Proxy können Sie Ihre LANCOM R&S®Unified Firewall als Proxy für E-Mails verwenden.

Unter **UTM** > **Proxy** > **Mail-Proxy-Einstellungen** können Sie den Mail-Proxy konfigurieren:

Eingabefeld	Beschreibung
I/0	Ein Schiebeschalter gibt an, ob der Mail-Proxy derzeit aktiv (**I**) oder inaktiv (**0**) ist. Mit einem Klick auf den Schiebeschalter ändern Sie den Status dieser Option. Diese Option ist standardmäßig aktiviert.
Server-Zertifikate verifizieren	Wählen Sie dieses Kontrollkästchen, wenn Sie möchten, dass der Mail-Proxy Ihrer LANCOM R&S®Unified Firewall Server-Zertifikate validiert.
StartTLS (SMTP) verwenden	Wählen Sie dieses Kontrollkästchen, um StartTLS für über den Proxy geleitete SMTP-Verbindungen zu aktivieren.

Eingabefeld	Beschreibung
Zertifikate	Wählen Sie den Zertifikatstyp aus, den Sie für den Mail-Proxy verwenden möchten, indem Sie die entsprechende Optionsschaltfläche auswählen. Die folgenden Optionen stehen zur Verfügung: › **Zertifikate automatisch erstellen** Es werden automatisch Pseudo-Zertifikate für jeden Mail-Server erstellt. › **Zertifikat auswählen** Ihre LANCOM R&S®Unified Firewall verwendet ein Zertifikat für alle Mail-Server. Wählen Sie aus der Drop-Down-Liste **Proxy-Zertifikat** ein Zertifikat aus. Hinweise zum Erstellen dieser Zertifikate finden Sie unter *Zertifikatsverwaltung* auf Seite 205. Es sind nur Non-CA-Zertifikate unter Verwendung eines privaten Schlüssels erlaubt.

Wenn Sie Änderungen vorgenommen haben, können Sie diese mit den Schaltflächen unten rechts im Bearbeitungsfenster speichern (**Speichern**) oder verwerfen (**Zurücksetzen**). Andernfalls können Sie das Fenster schließen (**Schließen**).

Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

3.4.5.5.3 VoIP-Proxy-Einstellungen

Mithilfe des VoIP-Proxy können Sie Ihre LANCOM R&S®Unified Firewall als Proxy für VoIP-Verbindungen verwenden. In diesem Fall müssen sich die SIP-Telefone an der LANCOM R&S®Unified Firewall registrieren. Die SIP-Pakete werden dann durch den VoIP-Proxy in Richtung Internet maskiert (NAT).

Eine Priorisierung der SIP-Pakete findet durch den VoIP-Proxy nicht statt.

Unter **UTM** > **Proxy** > **VoIP-Proxy-Einstellungen** konfigurieren Sie den VoIP-Proxy Ihrer LANCOM R&S®Unified Firewall:

Eingabefeld	Beschreibung
Internes Netz	Wählen Sie aus der Drop-down-Liste Ihre lokale Netzwerkschnittstelle aus, die für Telefonanrufe verwendet werden soll.
Internet-Verbindung	Wählen Sie aus der Drop-down-Liste die Internetverbindung aus, die Ihre LANCOM R&S®Unified Firewall verwendet, um VoIP-Verbindungen weiterzuleiten.
SIP Proxy aktivieren	Wählen Sie dieses Kontrollkästchen, wenn Ihre LANCOM R&S®Unified Firewall als VoIP-Proxy für das SIP verwendet werden soll. Der Proxy ist dann über Port 5060 erreichbar.
Daten an einen externen SIP-Proxy weiterleiten	Wählen Sie dieses Kontrollkästchen, um alle VoIP-Daten im SIP an einen externen SIP-Proxy weiterzuleiten.
Adresse des externen Proxies	Geben Sie die IP-Adresse des externen SIP-Proxy ein.
Port	Geben Sie den Port des externen SIP-Proxy ein.

Um den VoIP-Proxy zu verwenden, müssen Sie auf Ihren VoIP-Geräten die IP-Adresse Ihrer LANCOM R&S®Unified Firewall mit Port 5060 eingeben. Weitere Details finden Sie in der Dokumentation Ihrer VoIP-Endgeräte.

Wenn Sie Änderungen vorgenommen haben, können Sie diese mit den Schaltflächen unten rechts im Bearbeitungsfenster speichern (**Speichern**) oder verwerfen (**Zurücksetzen**). Andernfalls können Sie das Fenster schließen (**Schließen**).

Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

3.4.5.6 Reverse-Proxy

Unter **UTM** > **Reverse-Proxy** können Sie die Einstellungen für Backends, Frontends und Reverse-Proxy verwalten.

Ein Reverse-Proxy ist sinnvoll, wenn Sie auf Ihrem eigenen Netzwerk eine öffentliche Website hosten.

Wenn der Reverse-Proxy aktiv ist, nimmt Ihre LANCOM R&S®Unified Firewall Anfragen auf diese Website aus externen Netzwerken (z. B. dem Internet) entgegen. Es leitet diese dann entsprechend Ihrer Konfiguration an einen oder mehrere interne Webserver weiter.

Mit dem Reverse-Proxy können Sie mehrere Domains auf einer IP-Adresse hosten. Er dient außerdem zur Lastverteilung und als Ausfallsicherung, wenn Sie mehrere interne Server verwenden.

3.4.5.6.1 Reverse-Proxy-Einstellungen

Unter **UTM** > **Reverse-Proxy** > **Reverse-Proxy-Einstellungen** können Sie den Reverse Proxy generell aktivieren oder deaktivieren.

Abbildung 26: Reverse-Proxy-Einstellungen

Eingabefeld	Beschreibung
I/0	Ein Schiebeschalter gibt an, ob der Reverse-Proxy derzeit aktiv (**I**) oder inaktiv (**0**) ist. Mit einem Klick auf den Schiebeschalter ändern Sie den Status des Reverse-Proxy. Der Reverse-Proxy ist standardmäßig aktiviert.

3.4.5.6.2 HTTP(S)-Backends

Navigieren Sie zu **UTM** > **Reverse-Proxy** > **HTTP(S)-Backends**, um mindestens ein Backend mit einem Server anzulegen. Ein Backend besteht aus einem oder mehreren internen Webservern, die Ihre Website bereitstellen.

Im Fenster **Reverse-Proxy-Backend** können Sie die folgenden Informationen einsehen und die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Name	Geben Sie einen Namen für das Backend ein.
SSL	Aktivieren Sie dieses Kontrollkästchen, um SSL zu aktivieren. Wenn SSL aktiviert ist, wird die Verbindung zwischen Reverse-Proxy und Backend verschlüsselt.
Server	Weisen Sie dem Backend einen oder mehrere Server zu. Geben Sie eine Serveradresse ein. Klicken Sie auf ⊕, um die IP-Adresse zur Liste hinzuzufügen.

Mit den Schaltflächen unten rechts im Bearbeitungsfenster können Sie Ihre Änderungen verwerfen (**Abbrechen**), oder ein neues Backend anlegen (**Erstellen**).

Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

3.4.5.6.3 HTTP(S)-Frontends

Navigieren Sie zu **UTM** > **Reverse-Proxy** > **HTTP(S)-Frontends**, um Ihre Frontends zu konfigurieren.

Um die Konfiguration vorzunehmen, müssen Sie mindestens ein Backend mit mindestens einem Server angelegt haben.

Nachdem Sie ein Backend erstellt haben, können Sie im **Reverse-Proxy-Frontend** ein Frontend erstellen. Jedes konfigurierte Frontend stellt eine Website mit externer IP-Adresse, Port, Domain und – sofern SSL aktiviert ist – Zertifikat dar.

Im Fenster **Reverse-Proxy-Frontend** können Sie die folgenden Informationen einsehen und die folgenden Elemente konfigurieren:

Tabelle 5: Allgemein

Eingabefeld	Beschreibung
I/0	Ein Schiebeschalter gibt an, ob der Reverse-Proxy derzeit aktiv (**I**) oder inaktiv (**0**) ist. Mit einem Klick auf den Schiebeschalter ändern Sie den Status des Reverse-Proxy. Der Reverse-Proxy ist standardmäßig aktiviert.
Domäne oder IP-Adresse	Geben Sie den Namen der Domain oder die IP-Adresse ein, der das Frontend zugewiesen ist.
Verbindung	Wählen Sie eine Verbindung aus. Sie können sowohl eine Netzwerkverbindung, eine PPP-Verbindung als auch eine Wireguard-Verbindung auswählen.
Port	Konfigurieren Sie den externen Listen-Port für den Reverse-Proxy, z. B. den Port, der von externen Netzwerken aus erreichbar ist.
SSL	Aktivieren Sie dieses Kontrollkästchen, um SSL zu aktivieren. Wenn SSL aktiviert wird, stellt der Reverse-Proxy die Website mit SSL-Verschlüsselung bereit und verwendet das konfigurierte Zertifikat zur Authentifizierung.
Let's Encrypt verwenden	Verwendet ein Let's Encrypt-Zertifikat. Die verwendeten Zertifikate werden automatisch erzeugt und bei Ablauf der Gültigkeit automatisch verlängert. Siehe *Let's Encrypt* auf Seite 215.
Zertifikat	Wählen Sie ein Zertifikat mit einem privaten Schlüssel aus. Diese Option ist nur verfügbar, wenn SSL aktiviert ist.
"Outlook Anywhere" erlauben	Aktiviert zusätzliche Optionen um Outlook Anywhere durch den Reverse Proxy zu ermöglichen.
HTTP auf HTTPS umleiten	Über diese Option werden HTTP-Anfragen an die konfigurierte Domain oder IP-Adresse auf HTTPS umgeleitet.
Host-Header bewahren	Setzen Sie diese Option, um den „Host"-HTTP-Header beim Reverse Proxy eingehender HTTP-Anfragen beizubehalten. Je nach Anwenungsszenario kann das An- oder Abschalten dieser Option Probleme in der Kommunikation mit dem Ziel-Server beheben.
Proxy-Pfade	Wählen Sie ein konfiguriertes Backend aus. Geben Sie einen URL-Pfad ein. Der URL-Pfad muss absolut sein, d. h. er muss mit einem / beginnen. Setzen Sie die Option Websocket, falls es sich um eine bidirektionale Websocket-Verbindung handelt. Für Websockets müssen sowohl im Frontend als auch im Backend die Option **SSL** aktiviert sein. Sie können nun Anfragen weiterleiten, die mit den URL-Parametern des konfigurierten Backends übereinstimmen.
Blockierte Pfade	Anfragen, die mit den URL-Parametern übereinstimmen, werden blockiert. Geben Sie einen URL-Pfad ein. Der URL-Pfad muss absolut sein, d. h. er muss mit einem / beginnen.

Tabelle 6: Beschränkungen

Eingabefeld	Beschreibung
Zugänglich für	Einzelne Reverse-Proxy-Frontends können hier mit Zugangsbeschränkungen versehen werden. Wenn Zugangsbeschränkungen eingerichtet sind, dann ist das Reverse-Proxy-Frontend nur für die eingestellten Benutzer (bzw. Benutzer, die Mitglied einer eingestellten Gruppe sind) möglich. Die Authentifizierung eines Benutzers erfolgt über das **Externe** Portal. Zur Auswahl stehen Lokale Firewall-Benutzer, LDAP-Nutzer und -Gruppen, sowie Nutzer und Gruppen des unter **Benutzerauthentifizierung** > **Externes Portal** > **SAML** eingestellten Identity Providers. Sind keine Beschränkungen eingerichtet, kann das Reverse Proxy Frontend ohne vorherige Authentifizierug verwendet werden.

Mit den Schaltflächen unten rechts im Bearbeitungsfenster können Sie Ihre Änderungen verwerfen (**Abbrechen**) oder ein neues Frontend anlegen (**Erstellen**).

Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

3.4.5.6.4 TCP-Load-Balancer

Navigieren Sie zu **UTM** > **Reverse-Proxy** > **TCP-Load-Balancer**, um einen TCP-Load-Balancer anzulegen. Sie können mehrere Load Balancer anlegen.

Im Fenster **TCP-Load-Balancer** können Sie die folgenden Informationen einsehen und die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Modus	Der Modus bestimmt, wie die Last verteilt wird.
Adresse	Optionale IP-Adresse, an die der Load Balancer gebunden ist. Voreingestellt ist 0.0.0.0, womit alle IP-Adressen der Unified Firewall eingeschlossen sind.
Port	Port, an den der Load Balancer gebunden ist.
Überprüfungsintervall	Intervall in Sekunden, wonach Überprüfungen auf die Verfügbarkeit der unter Server angegebenen Adressen durchgeführt werden.
Anzahl fehlgeschlagener Überprüfungen	Ab welcher Anzahl fehgeschlagener Überprüfungen ein Server als nicht verfügbar angesehen wird.
Anzahl erfolgreicher Überprüfungen	Ab welcher Anzahl erfolgreicher Überprüfungen ein als nicht verfügbar angesehener Server wieder als verfügbar angesehen wird.
Server	Die **Adresse** und der **Port** eines Servers zur Lastverteilung. Über die **Gewichtung** kann die Verwendung gesteuert werden. Je höher der Wert desto eher wird der Server verwendet.

Mit den Schaltflächen unten rechts im Bearbeitungsfenster können Sie Ihre Änderungen verwerfen (**Abbrechen**), oder einen neuen Load Balancer anlegen (**Erstellen**).

Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

3.4.5.7 URL- / Contentfilter

URL- und Contentfilter bestimmen, welche Websites für Computer im geschützten Netzwerk erreichbar sind.

Die URL-Filterfunktion Ihrer LANCOM R&S®Unified Firewall überprüft Internetadressen (URLs), die im HTTP-Datenverkehr empfangen werden, nach erlaubten und / oder nicht erlaubten Begriffen je nach Einordnung in Black- und Whitelists. Diese Listen sind leer und müssen durch Sie befüllt werden.

Ein „Blacklist" Ansatz legt eine Liste von gesperrten Seiten fest und gewährt Zugriff auf alle Seiten, die nicht ausdrücklich verboten sind. Wenn zum Beispiel die URL einer Website auf einer Blacklist steht, wird der Zugriff auf diese Seite gesperrt. Z. B. könnte die URL `http://www.some-shop.com` gesperrt werden, wenn Sie diese URL einer Blacklist hinzufügen.

Durch eine „Whitelist“ kann der Zugriff auf eine Liste von Seiten begrenzt werden, die speziell für die Benutzung zugelassen wurden, während alle anderen gesperrt sind. Wenn Sie zum Beispiel den Zugriff auf die URL `http://www.some-shop.com` erlauben möchten, sollten Sie diese URL in eine Whitelist eintragen.

Wenn Sie eine Contentfilterkategorie aktivieren, dann wird jede Anfrage an unseren OEM-Partner weitergeleitet. Dort werden für die Kategorien aktiv gepflegte Datenbanken abgefragt. Sollte die weitergeleitete URL bereits eine oder mehrere Klassifizierungen haben, werden diese Ihrer LANCOM R&S®Unified Firewall mitgeteilt. Diese werden mit den geblockten Kategorien der Verbindung verglichen und bei einer Übereinstimmung der Zugriff auf die angefragte URL geblockt.

Zusätztlich kann die LANCOM R&S®Unified Firewall Seiten über das BPJM-Modul der Bundeszentrale für Kinder- und Jugendmedienschutz sperren.

Um URL- und Contentfilter für HTTP- und HTTPS-Verbindungen zu verwenden, wird der HTTP-Proxy benötigt. Die HTTP-Datenkommunikation einer Verbindung kann nur nach URL-Listen und Inhalten gefiltert werden, wenn der HTTP-Proxy bei der Bearbeitung der Regeln für diese Verbindung aktiviert wurde.

Um URL- und Contentfilter für DNS-Anfragen zu verwenden, muss der Web-Filter-Modus auf „DNS“ oder „Proxy und DNS“ gesetzt werden.

Die hier definierten URL- und Contentfilter stehen zur Verwendung in benutzerdefinierten Firewall-Regeln zur Verfügung. Weiterführende Informationen finden Sie unter *Einstellungen für Firewall-Regeln* auf Seite 30.

Weiterführende Informationen zu URL- / Contentfiltern finden Sie in den folgenden Abschnitten.

3.4.5.7.1 Einstellungen für URL- / Contentfilter

Navigieren Sie zu **UTM** > **URL-/Contentfilter** > **Einstellungen**, um die URL- und Contentfilter Ihrer LANCOM R&S®Unified Firewall zu konfigurieren.

Eingabefeld	Beschreibung
Content-Filter-Lizenz	Dieses Feld zeigt die Lizenzinformationen zu Ihrem Contentfilter an.
URLs	Setzen Sie diesen Haken, um Abschnitte hinter einem `?` (Dieses trennt den URL-Pfad von den überreichten Anfragen an den Server.) von Black- und Whitelists auszuschließen.
Safesearch	Setzen Sie dieses Häkchen, um die Einstellung `SafeSearch=strict` automatisch für alle Suchvorgänge über dies unterstützende Suchmaschinen wie z. B. Google und Yahoo zu konfigurieren, um nicht jugendfreie Inhalte in Suchanfragen zu verbergen. Die Suchmaschine Bing unterstützt diesen Parameter z. B. nicht. Benutzer können diese Einstellung nicht verändern. Um SafeSearch zu verwenden, wird kein aktives Contentfilter-Profil in den Verbindungen benötigt. SafeSearch funktioniert nur, wenn der HTTPS-Proxy aktiv ist, da die meisten Suchmaschinenanbieter auf ihren Websites verschlüsselte HTTPS-Verbindungen verwenden.
Ausnahme-Modus für Kategorien	Falls eine Webseite gesperrt wurde, können Sie hier das Verhalten Ihrer Firewall steuern: › **Deaktiviert** Keine Ausnahmen erlauben. › **Ausnahmen erlauben** Falls eine Webseite gesperrt wurde, können Sie die Sperrmechanismen des Contentfilters für eine gewählte Zeitspanne überschreiben. Geben Sie die Zeitspanne für die Contentfilter-Kategorie in Minuten ein, um das entsprechende Profil zu deaktivieren.

Eingabefeld	Beschreibung
	Nur die aktuelle Kategorie eines URL- / Contentfilter-Profils wird als nicht gesperrt für eine bestimmte Zeitspanne überschrieben). › **Ausnahme nur mit Code erlauben** Falls eine Webseite gesperrt wurde, können Ihre Benutzer die Sperrmechanismen des Contentfilters durch die Eingabe einer kurzen numerischen Sequenz (Code) übergehen. Geben Sie hier die Benutzer an, die entsprechende Codes verwalten dürfen. Hierfür kommen alle für Funktionen des internen Portals nutzbaren Benutzer und Gruppen in Frage (siehe *Benutzerauthentifizierung* auf Seite 164). Siehe *URL- / Contentfilter-Codes managen* auf Seite 152

Wenn Sie Änderungen vorgenommen haben, können Sie diese mit den Schaltflächen unten rechts im Bearbeitungsfenster speichern (**Speichern**) oder verwerfen (**Zurücksetzen**). Andernfalls können Sie das Fenster schließen (**Schließen**).

Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

3.4.5.7.2 Übersicht URL- / Contentfilter

Navigieren Sie zu **UTM** > **URL-/Contentfilter** > **URL-/Contentfilter**, um die Liste der im System angelegten URL- und Contentfilter anzuzeigen.

In der erweiterten Ansicht wird in den Tabellenspalten der **Name** des Filters und die Anzahl der ausgewählten Einträge in Contentfiltern, Blacklists und Whitelists angezeigt. Mithilfe der Schaltflächen in der letzten Spalte können Sie die Einstellungen für URL- und Contentfilter-Profile einsehen und anpassen, einen neuen Filter auf der Grundlage einer Kopie eines vorhandenen Filters anlegen oder einen selbstdefinierten Filter aus dem System löschen.

Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28.

Einstellungen für ein URL- / Contentfilter-Profil

Mit diesen Einstellungen können Sie die folgenden Optionen konfigurieren:

Eingabefeld	Beschreibung
Name	Geben Sie einen Namen für den URL- und Contentfilter an.
Überschreiben durch Benutzer	Setzen Sie dieses Häkchen, um ein Contentfilterprofil als überschreibbar zu markieren. Abhängig von Ihren Einstellungen wird ggf. alternativ ein Code benötigt. Wie Sie die Dauer dieser Option einstellen oder ob ein Code benötigt wird, finden Sie unter *Einstellungen für URL- / Contentfilter* auf Seite 150. Näheres zur Verwaltung der Codes finden Sie unter *URL- / Contentfilter-Codes managen* auf Seite 152. Diese Option ist nur für Profile verfügbar, die keine Standardprofile sind.

Contentfilter

Im Abschnitt **Content-Filter** legen Sie fest, welche Websites für die Benutzer im Netzwerk verfügbar und welche gesperrt sein sollen.

Klicken Sie auf die Schaltfläche › neben einer Kategorie, um ihre Unterkategorien anzuzeigen. Wählen Sie ganze Kategorien oder einzelne Unterkategorien aus, indem Sie die das entsprechende Häkchen setzen. Entfernen Sie das Häkchen neben einer Kategorie oder Unterkategorie, um diese von der Blacklist oder Whitelist zu entfernen. Um die Unterkategorien zu verbergen, klicken Sie auf die Schaltfläche ⌄ neben der Kategorie.

URL-Filter

Im Abschnitt **URL-Filter** können Sie Blacklist- und / oder Whitelistfilter für URLs definieren.

Eingabefeld	Beschreibung
Blacklist / **Whitelists**	Sie können eine Blacklist und / oder eine Whitelist anlegen, indem Sie beliebig viele Begriffe zur jeweiligen Liste hinzufügen. Wenn beide Listen gleichzeitig angewendet werden, wird die Whitelist mit höherer Priorität behandelt. Für beide Listen bestehen zwei Möglichkeiten, Begriffe hinzuzufügen: › Die Einträge werden in einer langen Liste wie in einem einfachen Texteditor angezeigt. Klicken Sie einfach eine beliebige Stelle an und bearbeiten dann den angeklickten Eintrag. › Alternativ können Sie Einträge auch aus einer Textdatei importieren, indem Sie auf **Import** klicken und die gewünschte Datei öffnen. Die maximale Dateigröße für Importe beträgt standardmäßig 1 Megabyte. Jede nicht leere Zeile der ausgewählten Textdatei wird als Eintrag zur entsprechenden Liste hinzugefügt. Über das Suchfeld können Sie einen Eintrag eingeben, um nach diesem in der jeweiligen Liste zu suchen. Anschließend können Sie diesen wie in einem Texteditor bearbeiten oder einfach aus der Liste löschen. Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28. Sie können eine Liste mit Begriffen komplett als Textdatei auf die lokale Festplatte exportieren, indem Sie rechts unter der entsprechenden Liste auf **Export** klicken. Die Begriffe in jeder der Listen können die folgenden Platzhalter enthalten: * für ganze Wörter, ? für einzelne Zeichen.

Um eine **Blacklist** oder **Whitelists** zu erstellen, können Sie Einträge entweder direkt eingeben, oder reguläre Ausdrücke (RegEx) verwenden.

RegEx	Beschreibung	Beispiel
`.`	Platzhalter für einzelne Zeichen	`ho.me` – z. B. home, hole
`*`	Beliebig viele Wiederholungen des Zeichens	`hom*` – z. B. hom, homm
`.*`	Eine beliebige Anzahl an Zeichen	`ho.*e` – z. B. home, house
`^`	Beginn einer Zeile	`^home` – home steht nur am Zeilenanfang
`$`	Ende einer Zeile	`home$` – home steht nur am Ende der Zeile

Die Schaltflächen rechts unten im Bearbeitungsfeld hängen davon ab, ob Sie einen neuen URL- und Contentfilter hinzufügen oder einen bestehenden bearbeiten. Klicken Sie für einen neu konfigurierten URL- und Contentfilter auf **Erstellen**, um ihn zur Liste der verfügbaren Dienste hinzuzufügen, oder auf **Abbrechen**, um Ihre Änderungen zu verwerfen.

Wenn Sie Änderungen vorgenommen haben, können Sie diese mit den Schaltflächen unten rechts im Bearbeitungsfenster speichern (**Speichern**) oder verwerfen (**Zurücksetzen**). Andernfalls können Sie das Fenster schließen (**Schließen**).

Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

3.4.5.7.3 URL- / Contentfilter-Codes managen

Falls eine Webseite gesperrt wurde, können Ihre Benutzer die Sperrmechanismen des Contentfilters ggf. durch die Eingabe einer kurzen numerischen Sequenz (Code) auf der Blockseite übergehen. Ein Benutzer, welcher die entsprechenden Codes verwalten darf, muss sich dazu als Benutzer an der LANCOM R&S®Unified Firewall anmelden. Siehe *Benutzerauthentifizierung* auf Seite 164 (Einloggen) und *Einstellungen für URL- / Contentfilter* auf Seite 150 (Definition der Benutzer).

Die zur Einrichtung von Codes berechtigen Benutzer muss der Administrator in der Konfiguration des Content-Filters unter **Ausnahme-Modus für Kategorien** eingetragen haben. Diese Benutzer verbinden sich dann per HTTPS zu einem der lokalen Firewall-Interfaces. Bei entsprechender DNS-Konfiguration im Netz z. B. einfach „https://firewall" oder die IP-Adresse („https://<IP-Adresse>") im Web-Browser eingeben. Diese Webseiten sind in einem responsiven Design erstellt, sodass sie sich an die Fähigkeiten des Geräts anpassen und auch von einem Smartphone aus bedient werden können. Falls der Administrator z. B. eine LDAP-Anbindung der Firewall an das Active Directory eingerichtet hat, melden Sie sich mit den Zugansdaten Ihres Windows-Accounts an.

Nach der Anmeldung sehen Sie unten links den Zugang zum Management-Interface der Codes. Darüber werden die bereits eingerichteten aktiven Codes angezeigt. „Aktiv" bedeutet hier, dass diese Codes verwendet werden können. Sie müssen sich allerdings aktuell nicht notwendigerweise in Verwendung befinden.

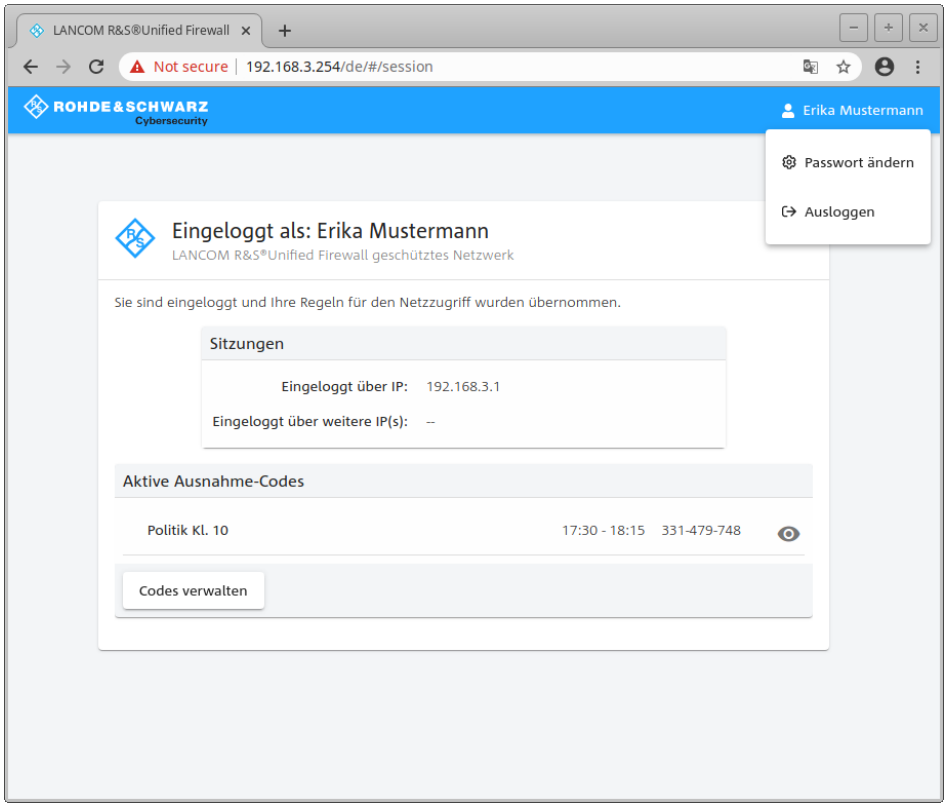


Abbildung 27: Ausnahme-Code: Einstieg in die Verwaltung

Wenn Sie das Augensymbol neben einem aktiven Code anklicken, dann wird der Code in einer Form gezeigt, die z. B. den vorgesehenen Benutzern gezeigt werden kann. Die Benutzer können den Code dann auf der Sperrseite eingeben, die einer entsprechend geblockten Seite angezeigt wird.

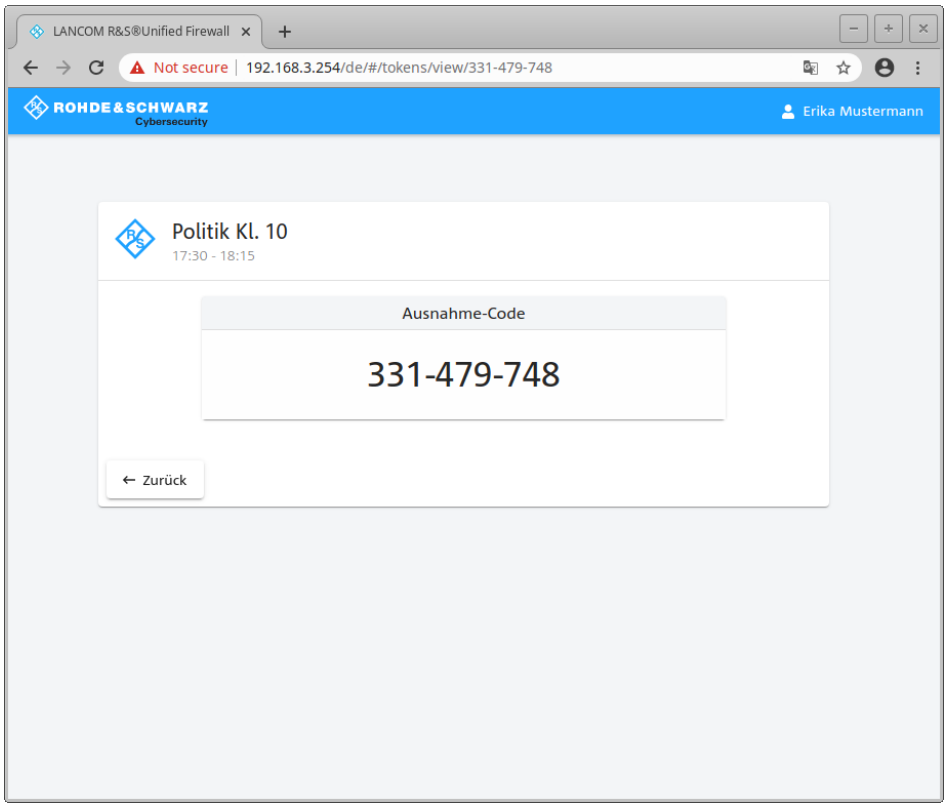


Abbildung 28: Ausnahme-Code: Präsentationsmodus

Über die Schaltfläche **Codes verwalten** auf der Hauptseite wird die Übersichtseite zur Verwaltung der Codes angezeigt. Hier sehen Sie alle Codes, also auch die abgelaufenen und solche, die erst in der Zukunft gültig werden.

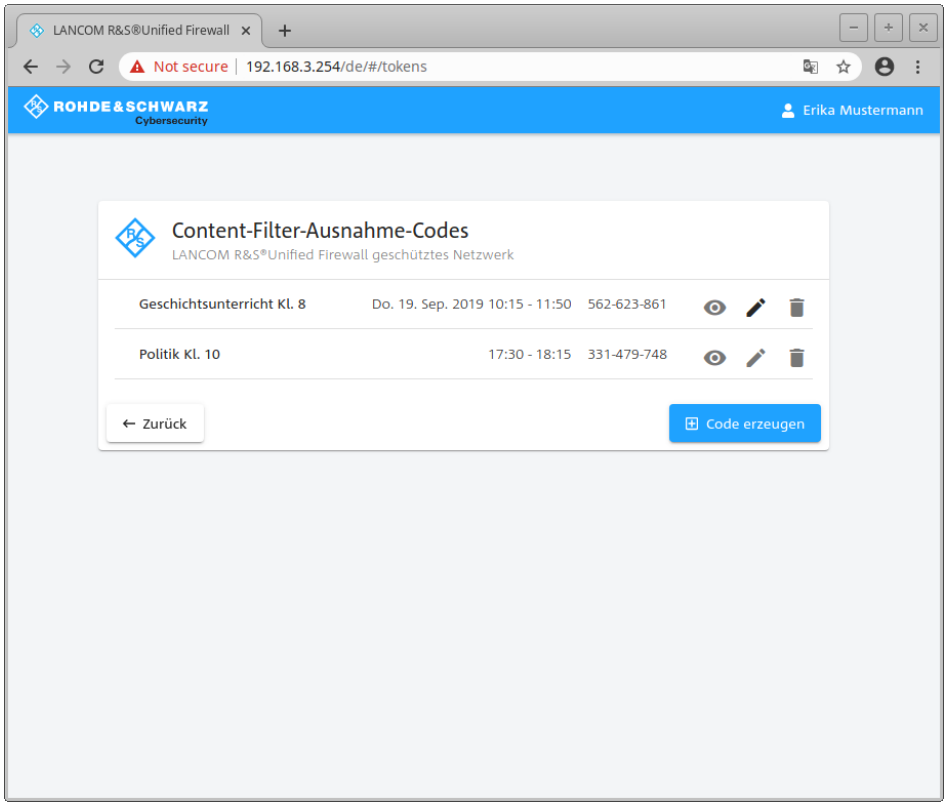


Abbildung 29: Ausnahme-Code: Managementmodus

Über die Symbole können Sie einen Code im Präsentationsmodus anzeigen (Auge), ihn bearbeiten (Stift) oder löschen (Mülleimer). Über die Schaltfläche **Code erzeugen** legen Sie einen neuen Code an. Hier können Sie die folgenden Optionen konfigurieren:

Eingabefeld	Beschreibung
Code-Name	Der Name des Codes, mit dem er angezeigt wird.
Code	Der eigentliche Code. Dieser kann nicht verändert werden.
Gültig am	Datum, an dem der Code gültig ist.
Gültig von	Uhrzeit, ab der dieser Code gültig wird und verwendet werden kann, um einen Filter zu übergehen.
Gültig bis	Uhrzeit, bis zu der dieser Code gültig ist und verwendet werden kann, um einen Filter zu übergehen.

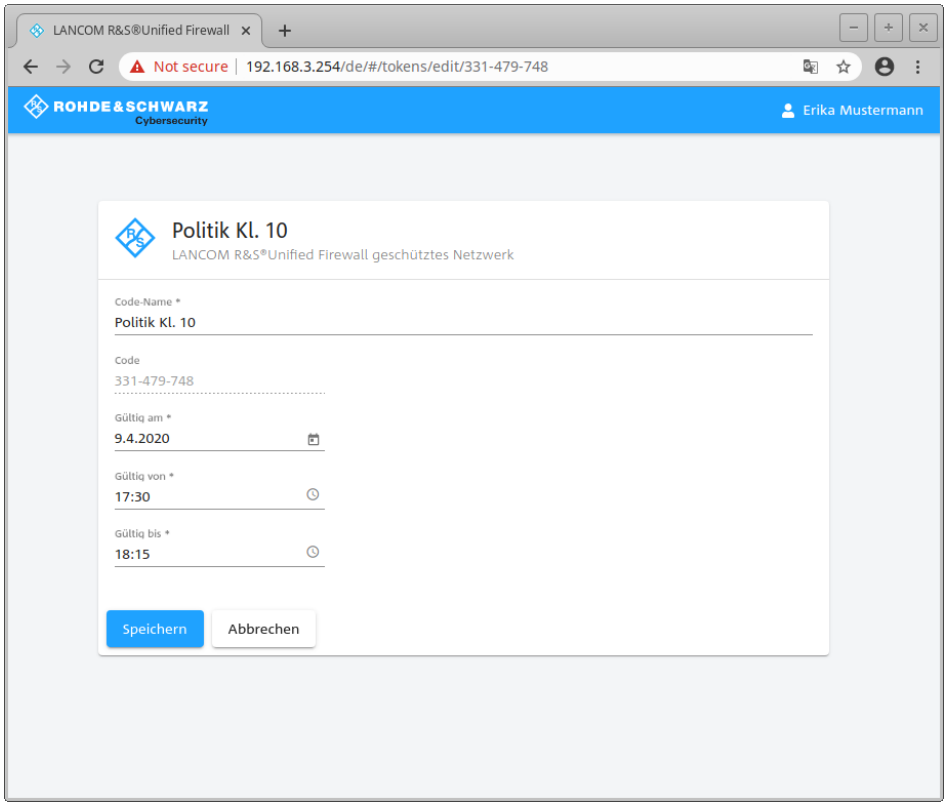


Abbildung 30: Ausnahme-Code: Code erzeugen

Sichern Sie ihren neuen oder geänderten Code durch einen Klick auf **Speichern** oder verwerfen Sie ihre Eingaben mit **Abbrechen**.

Wenn Sie Gültigkeitszeiten eines Codes ändern, dann gilt diese Änderung nicht für Benutzer, die diesen Code momentan bereits verwenden. Für diese Benutzer endet der Code zur ursprünglichen Endezeit. Daher muss der Code dann erneut eingegeben werden.

Ein Aufruf einer gesperrten Seite wird dann mit einer Meldung angezeigt, auf der ein gültiger Code eingegeben werden kann.

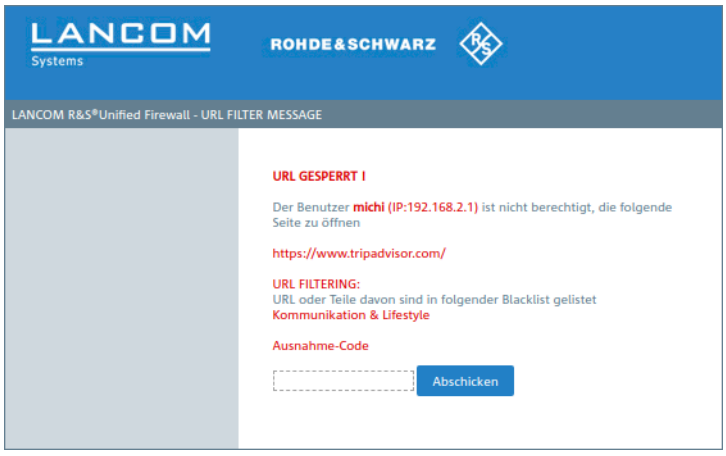


Abbildung 31: Ausnahme-Code: Meldung über gesperrte Seite

3.4.5.7.4 Detailbeschreibung der Kategorien und deren Sortierung im Web-Client

Dieser Abschnitt beschreibt die ab LCOS FX-Version 10.11 unterstützten Gruppen / Kategorien des OEM-Partners Bitdefender.

Potenziell Illegales

Illegales

Diese Kategorie umfasst Websites, die mit illegalen Aktivitäten in Verbindung stehen, darunter:

- Domains, die Peer-to-Peer-Tracker-Sites (BitTorrent, emule, DC++) hosten, die dafür bekannt sind, dass sie dazu beitragen, urheberrechtlich geschützte Inhalte ohne die Zustimmung des Urheberrechtsinhabers zu verbreiten;
- Domains, die Websites hosten, die Warez (raubkopierte kommerzielle Software) verbreiten, oder die entsprechende Diskussionsforen hosten;
- Domains, die Websites hosten, die der unlizenzierten Nutzung von Software gewidmet sind, wie z. B. das Hosten von Cracks, Schlüsselgeneratoren und Seriennummern, um die illegale Nutzung von Software zu erleichtern;
- Domains, die Material über sexuellen Kindesmissbrauch (CSAM) hosten.

Einige dieser Websites können auch als Pornografie- oder Alkohol- / Tabak-Websites erkannt werden, da sie oft Porno- oder Alkoholwerbung verwenden, um Geld zu verdienen.

Beispiel: *http://www.thepiratebay.org*

Hass, Gewalt & Rassismus

Diese Kategorie ist ein Sammelbegriff für die Kategorien „Hass, Gewalt & Rassismus" und soll die folgenden Kategorien von Websites blockieren:

- Websites, die terroristischen Organisationen angehören;
- Websites mit rassistischem oder fremdenfeindlichem Inhalt;
- Websites, die aggressive Sportarten diskutieren und/oder Gewalt fördern;

Beispiel: *http://nirvanaglobal.com*

Anstiftung zum Suizid

Diese Kategorie umfasst die Websites, die den Selbstmord fördern, anbieten oder befürworten. Sie deckt nicht die Kliniken zur Suizidprävention ab.

Beispiel: *http://suicidemethods.net*

Gewalttätige Cartoons

Diese Kategorie umfasst Websites, auf denen Gewalt-Cartoons oder Gewalt-Mangas diskutiert, geteilt und angeboten werden, die aufgrund von Gewalt, expliziter Sprache oder sexuellem Inhalt für Minderjährige ungeeignet sein könnten.

Diese Kategorie deckt nicht die Websites ab, die Mainstream-Cartoons wie „Tom und Jerry" anbieten.

Beispiel: *http://narutosquared.com*

Betäubungsmittel

Diese Kategorie umfasst die Websites, die Informationen über Betäubungsmittel wie Freizeitdrogen und illegale Drogen vermitteln. Diese Kategorie umfasst auch die Websites, die sich mit der Entwicklung oder dem Anbau von Drogen befassen.

Beispiel: *http://worldofseeds.eu*

Cyberbedrohungen

Hacking-Instrumente & Exploits

Diese Kategorie umfasst die Websites, die Hacking-Tools, Artikel und Diskussionsplattformen für Hacker anbieten. Sie umfasst auch die Websites, die Exploits für gängige Plattformen anbieten, die das Hacken von Facebook- oder Gmail-Konten erleichtern.

Beispiel: *http://passwordhacking.net*

File-Sharing

Diese Kategorie umfasst die File-Sharing-Websites, auf denen ein Benutzer eine Datei oder mehrere Dateien hochladen und mit anderen teilen kann. Sie umfasst auch einige Torrent-Sharing-Websites und Torrent-Tracker.

Beispiel: *http://www.mediafire.com*

Web-Proxies & Online-Anonymisierer

Diese Kategorie umfasst die Webseiten, die einen Web-Proxy-Dienst anbieten. Dabei handelt es sich um eine Website vom Typ „Browser im Browser", bei der ein Benutzer eine Webseite öffnet, die angeforderte URL in ein Formular eingibt und auf „Absenden" drückt. Die Web-Proxy-Site lädt die eigentliche Seite herunter und zeigt sie im Browser des Benutzers an.

Es gibt die folgenden Gründe, warum dieser Typ erkannt wird (und möglicherweise blockiert werden muss):

- Für das anonyme Surfen. Da die Anfragen an den Ziel-Webserver vom Proxy-Webserver aus erfolgen, ist nur dessen IP-Adresse sichtbar, und wenn die Server-Administratoren den Benutzer zurückverfolgen, endet die Rückverfolgung beim Web-Proxy, der möglicherweise Protokolle führt, die zur Lokalisierung des ursprünglichen Benutzers erforderlich sind, oder auch nicht.
- Für Standort-Spoofing. Die IP-Adressen der Nutzer werden häufig für die Erstellung von Profilen nach dem Herkunftsort verwendet (einige nationale Regierungswebsites sind möglicherweise nur von lokalen IP-Adressen aus zugänglich), und die Nutzung dieser Dienste könnte dem Nutzer helfen, seinen wahren Standort zu verschleiern.
- Für den Zugriff auf verbotene Inhalte. Bei Verwendung eines einfachen URL-Filters werden nur die Web-Proxy-URLs angezeigt und nicht die tatsächlichen Server, die der Benutzer besucht.
- Um die Überwachung durch das Unternehmen zu vermeiden. Eine Unternehmensrichtlinie kann die Überwachung der Internetnutzung von Mitarbeitern vorschreiben. Wenn der Benutzer über einen Web-Proxy auf alles zugreift, kann er sich der Überwachung entziehen, was keine korrekten Informationen liefert.

Da das SDK die HTML-Seite (sofern vorhanden) und nicht nur die URLs analysiert, kann das SDK bei einigen Kategorien den Inhalt dennoch erkennen. Andere Gründe lassen sich jedoch nicht durch die Verwendung des SDK vermeiden. Hier finden Sie eine große Liste von Web-Proxys.

Beispiel: *http://www.hidemyass.com*

Phishing-Webseiten

Dies bedeutet, dass die URL auf eine bekannte Phishing-Website verweist. Eine Phishing-Website ist eine Art von Website, die vorgibt, jemand anderes zu sein. Zum Beispiel kann sie vorgeben, eine Website Ihrer Bank zu sein, damit Sie Ihre Anmeldedaten eingeben.

Spam

Dies bedeutet, dass diese URL in den Spam-E-Mails gesehen wurde und daher durch Spamvertrieb gefördert wird. Der Inhalt der URL ist jedoch nicht notwendigerweise bösartig, es sei denn, andere Kennzeichen sind vorhanden.

Nicht vertrauenswürdig

Dies bedeutet, dass die URL bestimmte Besonderheiten aufweist, die Bitdefender zur Annahme veranlassen, dass sie nicht vertrauenswürdig ist. Die Details für diese Definition sind intern und können sich jederzeit ändern, daher sollte der Partner vorsichtig sein, ob er sich auf dieses Urteil verlässt oder nicht.

Malware

Dies bedeutet, dass die URL Malware enthält oder anbietet, bei der es sich um ausführbare Dateien, Exploits, bösartiges JavaScript usw. handeln kann.

Betrügerische Webseiten

Dies bedeutet, dass die URL auf eine bekannte betrügerische Website verweist. Im Gegensatz zu einer Phishing-Website gibt eine betrügerische Website nicht vor, jemand anderes zu sein. Stattdessen versucht sie, durch falsche Angaben oder Betrug etwas vom Benutzer zu erhalten (Informationen, Zahlungen, Anmeldedaten). Ein betrügerischer Online-Shop kann zum Beispiel sehr günstige Preise für beliebte Artikel anbieten (die er nie versendet).

Cryptowährungs-Miner

Dies bedeutet, dass die Website versucht, Kryptowährungen im Webbrowser des Nutzers zu schürfen und dabei die Computerressourcen zu nutzen. Die Website verbirgt diese Tatsache normalerweise vor dem Benutzer, obwohl einige Websites den Benutzer darüber informieren.

Potenziell unerwünschte Anwendungen

Dies bedeutet, dass diese Website potenziell unerwünschte Anwendungen enthält. Das sind Anwendungen, die häufig von Dritten installiert und für bösartige Zwecke verwendet werden. Auch wenn die Anwendungen selbst nicht bösartig sind, ist die Wahrscheinlichkeit, dass diese Anwendungen ohne die Zustimmung des Benutzers installiert und dann für bösartige Zwecke verwendet werden, nach Erfahrung von Bitdefender viel höher als bei anderen. Zu dieser Kategorie gehört Software wie Web- oder Socks-Proxies, Fernverwaltung, Standortverfolgung und so weiter.

Pornografie

Pornografie

Diese Kategorie umfasst Websites mit erotischen und pornografischen Inhalten. Sie umfasst sowohl kostenpflichtige als auch kostenlose Seiten. Sie umfasst Websites, die Bilder, Geschichten und Videos anbieten, und erkennt auch pornografische Inhalte auf Websites mit gemischtem Inhalt.

Beispiel: *http://www.redtube.com*

Nicht jugendfreie Inhalte

Diese Kategorie umfasst die Inhalte, die vom Ersteller der Website als für ein reifes Publikum geeignet eingestuft wurden. Sie umfasst eine breite Palette von Websites, von Kamasutra-Büchern und Websites zur Sexualerziehung bis hin zu Hardcore-Pornografie.

Beispiel: *http://www.kamasutra.com*

Werbung

Werbung

Diese Kategorie umfasst die Domains, deren Hauptzweck darin besteht, Werbung zu schalten.

Beispiel: *http://adbooth.com*

Spiele

Browser-Spiele

In diese Kategorie fallen Webseiten, die Online-Spiele anbieten – in der Regel Adobe Flash oder JAVA-Applets. Für die Erkennung spielt es keine Rolle, ob das Spiel kostenlos ist oder ein Abonnement erfordert, jedoch werden Webseiten im Casino-Stil in der Kategorie Glücksspiele erkannt. Diese Kategorie deckt nicht ab:

- Offizielle Websites von Unternehmen, die Videospiele entwickeln (es sei denn, es handelt sich um Online-Spiele);

- Diskussions-Websites, auf denen Spiele diskutiert werden;
- Websites, auf denen Nicht-Online-Spiele heruntergeladen werden können (einige von ihnen fallen unter die Kategorie *Illegales* auf Seite 157);
- Spiele, bei denen der Benutzer die ausführbare Datei herunterladen und ausführen muss, wie World of Warcraft. Diese können durch verschiedene Maßnahmen wie die Verwendung einer Firewall verhindert werden.

Beispiel: *http://www.flashgames247.com*

Online-Casinos & Glücksspiel

Diese Kategorie umfasst die Glücksspiel-Websites. Dabei handelt es sich um „Online-Casino-" oder „Online-Lotterie-Websites", die in der Regel eine Zahlung verlangen, bevor der Benutzer bei Online-Roulette, Poker, Black Jack oder ähnlichen Spielen um Geld spielen kann. Einige von ihnen sind seriös, d. h. es besteht eine Gewinnchance, andere sind betrügerisch, d. h. es besteht keine Gewinnchance. Außerdem werden „Gewinntipps und Betrugs-Websites" aufgespürt, die beschreiben, wie man mit Glücksspielen Geld verdienen kann, sowie Online-Lotterie-Websites.

Beispiel: *http://www.888.com*

Web Applikationen

Foren

Zu dieser Kategorie gehören Foren, Diskussionsforen und Websites, auf denen Fragen gestellt und beantwortet werden können.

Diese Kategorie umfasst nicht die speziellen Bereiche auf Unternehmenswebsites, in denen Kundenfragen gestellt werden.

Beispiel: *http://stackoverflow.com*

Video-Portale

Diese Kategorie umfasst Webseiten, auf denen verschiedene Videos oder Fotos zu finden sind, die entweder von Nutzern hochgeladen oder von verschiedenen Inhaltsanbietern bereitgestellt werden. Dazu gehören Websites wie Youtube, Metacafe, Google Video und Fotoseiten wie Picasa oder Flickr. Es werden auch Videos erkannt, die in andere Websites oder Blogs eingebettet sind.

Beispiel: *http://www.youtube.com*

Online-Radio-Stationen

Diese Kategorie umfasst Websites, die Internet-Musik-Streaming-Dienste anbieten, von Online-Radiosendern bis hin zu Websites, die (kostenlose oder kostenpflichtige) Audioinhalte auf Abruf bereitstellen.

Beispiel: *http://grooveshark.com*

Chat und Instant-Messaging

Diese Kategorie umfasst die Instant-Messaging- und Chat-Websites, die es den Benutzern ermöglichen, in Echtzeit zu chatten. Es werden auch yahoo.com und gmail.com erkannt, da beide einen eingebetteten Instant-Messenger-Dienst enthalten.

Beispiel: *http://www.meebo.com*

Suchmaschinen

In diese Kategorie fallen die Suchmaschinen-Websites wie Google, Yahoo, Bing usw.

Beispiel: *http://www.google.com*

Online-Nachrichten-Portale

Zu dieser Kategorie gehören Websites, die Informationen aus mehreren Quellen und verschiedenen Bereichen zusammenfassen und in der Regel Funktionen wie Suchmaschinen, E-Mail, Nachrichten und Unterhaltungsinformationen anbieten.

Beispiel: *http://www.yahoo.com*

Soziale Medien

Diese Kategorie umfasst die Websites der sozialen Netzwerke. Dazu gehören MySpace.com, Facebook.com, Bebo.com, usw. Soziale Netzwerke für spezielle Zwecke wie Youtube werden jedoch in der Kategorie Video/Foto aufgeführt.

Beispiel: *http://www.myspace.com*

Webmail

In diese Kategorie fallen Websites, die E-Mail-Funktionen als Webanwendung anbieten.

Beispiel: *http://mail.google.com*

Online-Foto-Portale

TODO: Keine Beschreibung in Entwicklerdoku

Beispiel: *http:/www.gettyimages.com*

Software

Diese Kategorie umfasst die Websites, die Computersoftware anbieten, in der Regel entweder Open Source, Freeware oder Shareware. Sie kann auch einige Online-Software-Shops umfassen.

Beispiel: *http://www.bitdefender.com*

Webhosting

Diese Kategorie umfasst kostenlose und kommerzielle Website-Hosting-Dienste, die es privaten Benutzern und Organisationen ermöglichen, Webseiten zu erstellen und zu veröffentlichen.

Beispiel: *http://www.godaddy.com*

Dating

Diese Kategorie umfasst die kostenpflichtigen und kostenlosen Online-Dating-Websites, auf denen Nutzer anhand bestimmter Kriterien nach Personen suchen können. Sie können auch ihre Profile veröffentlichen, damit andere sie suchen können. Zu dieser Kategorie gehören sowohl kostenlose als auch kostenpflichtige Online-Dating-Websites.

Da die meisten beliebten sozialen Netzwerke als Online-Dating-Websites genutzt werden können, werden einige beliebte Websites wie Facebook ebenfalls in dieser Kategorie erfasst. Es wird empfohlen, diese Kategorie zusammen mit der Kategorie *Soziale Medien* auf Seite 161 zu verwenden.

Beispiel: *http://www.match.com*

Blogs

Diese Kategorie umfasst sowohl persönliche Websites als auch alle Arten von Blogs: individuelle, Gruppen- und sogar Unternehmensblogs. Ein Blog ist ein im World Wide Web veröffentlichtes Journal, das aus Einträgen („Posts“) besteht, die in der Regel in umgekehrter chronologischer Reihenfolge angezeigt werden, so dass der neueste Beitrag zuerst erscheint.

Beispiel: *http://blog.wordpress.com*

Job-Suche

Diese Kategorie umfasst Websites, die Stellenbörsen, berufsbezogene Kleinanzeigen und Karrieremöglichkeiten anbieten, sowie Aggregatoren solcher Dienste. Sie umfasst keine Personalvermittlungsagenturen oder Jobseiten auf den regulären Unternehmenswebsites.

Beispiel: *http://monster.com*

Shopping

Online-Handel

Diese Kategorie umfasst die bekannten Online-Shops. Eine Website gilt als Online-Shop, wenn sie Waren oder Dienstleistungen online verkauft.

Beispiel: *http://www.bestbuy.com*

Finanzen

Online-Bezahlung & Geldtransfer

Diese Kategorie umfasst die Websites, die Online-Zahlungen oder Geldüberweisungen anbieten. Sie erkennt die beliebten Zahlungsseiten wie PayPal oder Moneybookers. Es erkennt auch heuristisch die Webseiten auf den regulären Websites, die nach Kreditkarteninformationen fragen, und ermöglicht so die Erkennung von versteckten, unbekannten oder illegalen Online-Shops.

Beispiel: *http://www.paypal.com*

Banken & Finanzinstitute

Diese Kategorie umfasst die Websites aller Banken auf der ganzen Welt, die den Online-Zugang anbieten. Einige Kreditgenossenschaften und andere Finanzinstitute sind ebenfalls erfasst. Einige lokale Banken könnten jedoch nicht erfasst sein.

Beispiel: *http://bankofamerica.com*

Religionen & Kulte

Religionen & Kulte

Diese Kategorie umfasst die Websites, die für eine Religion oder Sekte werben. Sie umfasst auch die Diskussionsforen, die sich auf eine oder mehrere Religionen beziehen.

Beispiel: *http://www.scientology.com*

Information

Bildung

Diese Kategorie umfasst die Websites offizieller Bildungseinrichtungen, auch solche außerhalb der .edu-Domäne. Sie umfasst auch die Bildungswebsites wie Enzyklopädien.

Beispiel: *http://lp.edu.ua*

Staatliche Einrichtungen

Diese Kategorie umfasst die Websites der Regierung, einschließlich der Websites von Regierungseinrichtungen, Botschaften und Ämtern.

Beispiel: *http://www.mid.ru*

Nachrichten

Diese Kategorie umfasst Nachrichten-Websites, die Text- und Videonachrichten anbieten. Es wird angestrebt, sowohl globale als auch lokale Nachrichten-Websites abzudecken, wobei einige kleine, sehr lokale Nachrichten-Websites möglicherweise nicht abgedeckt werden.

Beispiel: *http://www.cnn.com*

Unternehmens-Websites

Dies ist eine Sammelkategorie für Unternehmenswebsites, die normalerweise in keine andere Kategorie fallen.

Beispiel: *http://www.shell.com*

Gesundheit & Medizin

In diese Kategorie fallen Websites, die mit medizinischen Einrichtungen in Verbindung stehen, Websites, die sich mit der Vorbeugung und Behandlung von Krankheiten befassen, Websites, die Informationen oder Produkte über Gewichtsabnahme, Diäten, Steroide, Anabolika oder HGH-Produkte anbieten, sowie Websites mit Informationen über plastische Chirurgie.

Beispiel: *http://www.webmd.com*

Freizeit

Boulevard

Diese Kategorie ist hauptsächlich für Softpornografie und Promi-Klatschseiten gedacht. Viele Nachrichtenseiten im Stil von Boulevardzeitungen können hier Unterkategorien haben. Die Erkennung in dieser Kategorie basiert ebenfalls auf Heuristiken.

Beispiel: *http://www.celebrity-gossip.net*

Unterhaltung

Diese Kategorie umfasst Websites, die Informationen über künstlerische Aktivitäten, Museen sowie Websites, die Inhalte wie Filme, Musik oder Kunst bewerten, bereitstellen.

Beispiel: *http://www.imdb.com*

Ablenkung

In diese Kategorie fallen Websites, auf denen sich Personen lange Zeit aufhalten. Dazu können auch Websites aus anderen Kategorien wie soziale Netzwerke, Unterhaltung usw. gehören.

Beispiel: *http://www.9gag.com*

Alkohol & Tabak

Diese Kategorie umfasst die „Medizin / Alkohol / Tabak"-Websites, die den Gebrauch oder den Verkauf von (legalen) medizinischen Drogen oder Utensilien, Alkohol oder Tabakprodukten diskutieren.

Beachten Sie, dass die illegalen Drogen in der Kategorie *Betäubungsmittel* auf Seite 157 erfasst sind.

Beispiel: *http://www.cigar.com*

Reisen

Diese Kategorie umfasst Websites, die Reiseangebote, Reiseausrüstung sowie Bewertungen und Rezensionen von Reisezielen präsentieren.

Beispiel: *http://www.tripadvisor.com*

Sport

Diese Kategorie umfasst Websites, die Sportinformationen, Nachrichten und Anleitungen anbieten.

Beispiel: *http://www.eurosport.com*

Hobbies

In diese Kategorie fallen Websites, die Ressourcen zu Aktivitäten anbieten, die typischerweise in der Freizeit ausgeübt werden, wie z. B. Sammeln, Basteln, Radfahren usw.

Beispiel: *http://www.stamps.org*

Waffen & Jagd

Diese Kategorie umfasst die Websites, die Waffen zum Verkauf oder Tausch, zur Herstellung oder Verwendung anbieten. Sie deckt auch die Jagdressourcen und die Verwendung von Luft- und Luftdruckwaffen sowie Nahkampfwaffen ab.

Beispiel: *http://hyattguns.com*

BPJM

BPJM

Diese Kategorie umfasst die Websites, die über das BPJM-Modul der Bundeszentrale für Kinder- und Jugendmedienschutz gesperrt werden.

3.4.6 Benutzerauthentifizierung

In den Einstellungen für die **Benutzerauthentifizierung** bestimmen Sie die Liste der Benutzer, die zur Verwendung Ihrer Netzwerkressourcen (z. B. Internetzugang, Überschreiben des Contentfilters und VPN-Tunnel) autorisiert werden können. Außerdem können Sie mit diesen Einstellungen lokale Benutzer einrichten und Ihre LANCOM R&S®Unified Firewall mit einem externen Verzeichnisdienst verbinden, aus dem einzelne Benutzer und Benutzergruppen abgerufen werden können. Damit legen Sie Firewall-Regeln nicht nur für Computer, sondern auch für einzelne Benutzer an. Auch VPN-Profile für den LANCOM Advanced VPN Client können Sie gezielt für einzelne Benutzer zur Verfügung stellen.

Navigieren Sie zu **Benutzerauthentifizierung**, um die Liste der derzeit im System angelegten Benutzer in der Objektleiste anzuzeigen.

In den folgenden Abschnitten finden Sie weiterführende Informationen zur Benutzerauthentifizierung.

3.4.6.1 Technischer Hintergrund und Vorbereitungen

Zweck der Benutzerauthentifizierung

Durch die Benutzerauthentifizierung können Benutzern Firewall-Regeln zugewiesen werden, wenn diese sich anmelden. Pro IP-Adresse darf nur ein Benutzer angemeldet sein.Wenn sich ein Benutzer von einer IP-Adresse aus anmeldet, die bereits für eine Sitzung verwendet wird, wird der zuvor angemeldete Benutzer ausgeloggt und der neue Benutzer angemeldet.

Einloggen auf der Firewall

Die LANCOM R&S®Unified Firewall betreibt einen gesonderten Webserver, der ausschließlich Benutzer-Logins verarbeitet. Dieser empfängt Benutzernamen und Passwort. Mithilfe einer Benutzerdatenbank, die lokal auf Ihrer LANCOM R&S®Unified Firewall erstellt wird, verifiziert ein Authentifizierungsdient zunächst, ob Benutzername und Passwort zulässig sind. Falls dieses Login fehlschlägt und ein Microsoft Active Directory Server oder ein openLDAP Server in der LANCOM R&S®Unified Firewall konfiguriert sind, ruft der Authentifizierungsdienst diese Directory-Server via Kerberos-Protokoll zusätzlich an, um zu überprüfen, ob der Benutzer authentifiziert werden kann. Ist die Authentifizierung erfolgt, werden die Firewall-Regeln dieses Benutzers den IP-Adressen zugewiesen, von denen die Anfrage geschickt wurde. Es ist außerdem möglich, Microsoft

Azure oder Keycloak als separaten Identity Provider (IdP) anzubinden und damit Single Sign-On mittels SAML zu unterstützen.

Benutzer, die in der lokalen Datenbank Ihrer LANCOM R&S®Unified Firewall registriert sind, können ihre Passwörter über den Webserver ändern. Das Passwort kann aus bis zu 248 Zeichen bestehen. Längere Passwörter werden akzeptiert, jedoch automatisch verkürzt.

Einige Computer, wie z. B. Terminalserver, an denen viele Benutzer gleichzeitig arbeiten, oder Server, auf denen sich nur Administratoren einloggen können, können von der Benutzerauthentifizierung ausgeschlossen werden. In diesem Fall akzeptieren Webserver und Authentifizierungsdienst keine Benutzeranmeldungen von den IP-Addressen dieser Computer.

Da alle Benutzer eines Terminalservers die gleiche IP-Adresse haben, kann Ihre LANCOM R&S®Unified Firewall in diesem Fall nicht die einzelnen Benutzer im Netzwerk identifizieren. Um dies zu umgehen, bietet Microsoft die sogenannte Remotedesktop-IP-Virtualisierung für Server 2008 R2 und neuere Versionen an. Mit dieser Anwendung erhält jeder Benutzer seine eigene IP-Adresse aus einem Pool von IP-Adressen, ähnlich wie bei DHCP.

Authentifizierungsserver

Für kleine Unternehmen ohne zentrale Benutzerverwaltung bietet Ihre LANCOM R&S®Unified Firewall die Möglichkeit einer lokalen Benutzerverwaltung. Sie können jederzeit die lokale Benutzerdatenbank verwenden. Sie können allerdings auch einen externen Verzeichnisdienst wie etwa den Microsoft Active Directory-Server oder einen openLDAP-Server verwenden. Darüber hinaus können Microsoft Azure oder Keycloak als IdP mit Single Sign-On genutzt weden. Sowohl Microsoft Active Directory als auch openLDAP verwenden das Protokoll Kerberos für die Verifizierung aller Login-Daten, die von Benutzerauthentifizierungs-Clients bereitgestellt werden. Microsoft Azure und Keycloak verwenden SAML für die Authentifizierung, so dass die Authentifizierung direkt zwischen Client-Browser und IdP erfolgt. Die Firewall wird hier nur über das Ergebnis benachrichtigt.

Active Directory- oder IdP-Gruppen

Wenn Sie einen Microsoft Active Directory-Server für die Authentifizierung verwenden, werden die Active Directory-Gruppen auch in der Objektleiste unter Benutzerauthentifizierung geführt. Active Directory-Gruppen sind eine effektive Möglichkeit, Sicherheitseinstellungen für einzelne Benutzer einzurichten und aufrechtzuerhalten. Beispielsweise können Sie Active Directory-Benutzer zu bestimmten Active Directory-Gruppen hinzufügen und mit Ihrer LANCOM R&S®Unified Firewall Firewall-Regeln für diese bestimmten Gruppen einrichten. Gleiches gilt für aus einem IdP importierte Gruppen.

3.4.6.2 Einloggen

Es bestehen drei verschiedene Möglichkeiten, sich auf LANCOM R&S®Unified Firewalls einzuloggen:

- *Login über Web-Browser*
- *Login über den LANCOM R&S® Unified Firewall Benutzerauthentifizierungs-Client*
- *Login über den LANCOM R&S® Unified Firewall Single Sign-On-Client*

Login über Web-Browser

Wenn Benutzer als Desktop-Objekte eingerichtet wurden und Firewall-Regeln für diese Benutzer konfiguriert wurden, können sie mithilfe der sogenannten Landingpage den Regeln entsprechend agieren. Das Einloggen über einen Webbrowser ist mit jedem Browser möglich und erfolgt SSL-verschlüsselt.

Gehen Sie wie folgt vor, um sich über einen Webbrowser auf Ihrer LANCOM R&S®Unified Firewall einzuloggen:

1. Starten Sie einen Webbrowser.
2. Stellen Sie sicher, dass Cookies aktiviert sind.
3. Geben Sie die IP-Adresse Ihrer LANCOM R&S®Unified Firewall, z. B. `https://192.168.12.1` (Standardport 443), in die Adresszeile ein.

Eine spezielle Webseite mit der LANCOM R&S®Unified Firewall Landingpage erscheint.

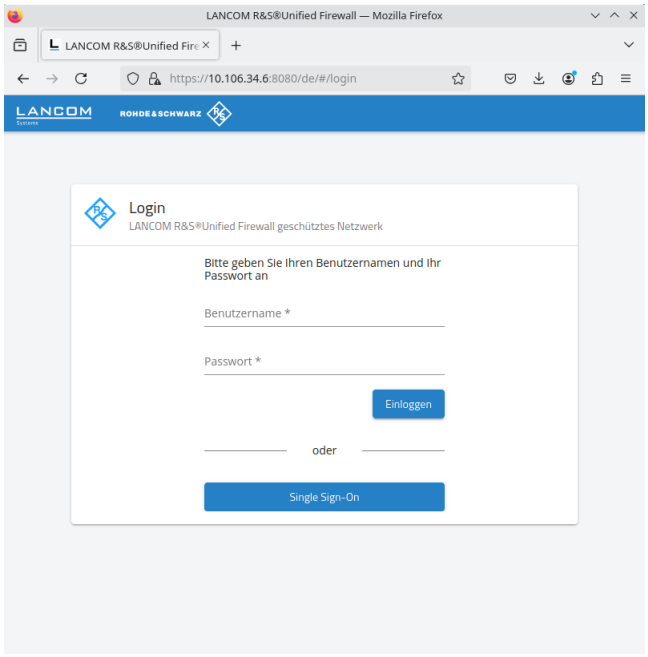


Abbildung 32: Benutzerauthentifizierung über einen Webbrowser

4. Wird ein IdP konfiguriert, steht Single Sign-On als alternative Login-Methode zur Verfügung. In diesem Fall klicken Sie auf **Single Sign-On**. Sie werden zum IdP weitergeleitet und können sich dort authentifizieren. Sollten Sie bereits authentifiziert sein, dann wird sofort die Seite nach der Anmeldung geöffnet.

   Geben Sie im Feld **Name** Ihren Benutzernamen ein.

   Wenn es sich um einen LDAP-Benutzer handelt, muss der Login-Name des Benutzers exakt mit dem Benutzernamen im sAMAccountName-Attribut des Benutzers übereinstimmen. Andernfalls entspricht der Name in den benutzerspezifischen Firewall-Regeln nicht dem Namen des sich am Client anmeldenden Benutzers und die Regeln stimmen nicht überein.
5. Geben Sie das **Kennwort** ein.
6. Klicken Sie auf **Anmelden**.

Die Authentifizierung wird ausgeführt.

Das Browserfenster, das zum Einloggen genutzt wurde, muss aus Sicherheitsgründen während der gesamten Sitzung geöffnet bleiben. Andernfalls wird der Benutzer nach einer Minute automatisch ausgeloggt. Dies verhindert, dass Unbefugte Zugriff auf die Firewall erlangen können, falls ein Benutzer sich aus Versehen nicht ausgeloggt hat.

Login über den LANCOM R&S®Unified Firewall Benutzerauthentifizierungs-Client

Der auf Windows basierende LANCOM R&S®Unified Firewall Benutzerauthentifizierungs-Client befindet sich im Verzeichnis `UA Client` auf dem USB-Flash-Laufwerk.

Gehen Sie wie folgt vor, um sich über den LANCOM R&S®Unified Firewall Benutzerauthentifizierungs-Client auf Ihrer LANCOM R&S®Unified Firewall einzuloggen:

1. Installieren Sie den LANCOM R&S®Unified Firewall Benutzerauthentifizierungs-Client.

2. Starten Sie den LANCOM R&S®Unified Firewall Benutzerauthentifizierungs-Client.

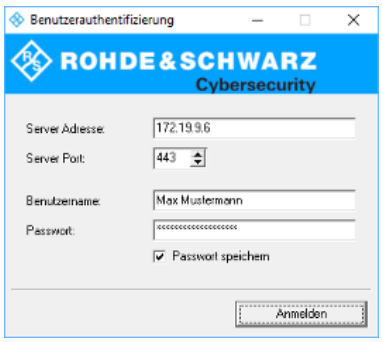


Abbildung 33: LANCOM R&S®Unified Firewall Benutzerauthentifizierungs-Client

3. Geben Sie unter **Server-Adresse** die IP-Adresse Ihrer LANCOM R&S®Unified Firewall ein.
4. Geben Sie im Feld **Benutzername** Ihren Benutzernamen ein.

> Wenn es sich um einen LDAP-Benutzer handelt, muss der Login-Name des Benutzers exakt mit dem Benutzernamen im sAMAccountName-Attribut des Benutzers übereinstimmen. Andernfalls entspricht der Name in den benutzerspezifischen Firewall-Regeln nicht dem Namen des sich am Client anmeldenden Benutzers und die Regeln stimmen nicht überein.

5. Geben Sie das **Kennwort** ein.
6. Optional: Setzen Sie den Haken im Kontrollkästchen **Passwort speichern**, um das Passwort für zukünftige Logins zu speichern.
7. Optional: Passen Sie unter **Einstellungen** das Zeitfenster für die Neuverbindung an, indem Sie mit der rechten Maustaste auf das Symbol im Benachrichtigungsfeld der Windows-Taskleiste klicken.

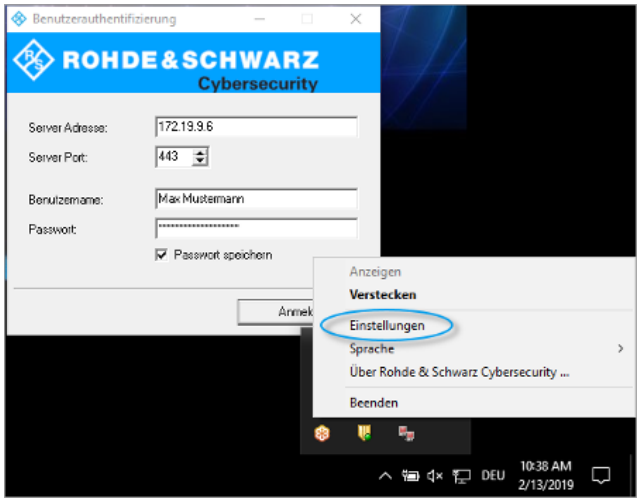


Abbildung 34: LANCOM R&S®Unified Firewall Benutzerauthentifizierungs-Client-Einstellungen

8. Klicken Sie auf **Anmelden**.

   Die Authentifizierung wird ausgeführt.

> Aus Sicherheitsgründen wird empfohlen, den LANCOM R&S®Unified Firewall Benutzerauthentifizierungs-Client stets auf die neueste verfügbare Version zu aktualisieren. Es ist allerdings möglich, einen Kompatibilitätsmodus

zu aktivieren, über den ältere Versionen des LANCOM R&S®Unified Firewall Benutzerauthentifizierungs-Clients ab Version 10 des LCOS FX arbeiten können. Weitere Informationen finden Sie unter *Einstellungen* auf Seite 176.

Login über den LANCOM R&S®Unified Firewall Single Sign-On-Client

Bei Verwendung von Single-Sign-On (SSO) loggen sich Active Directory-Domänenbenutzer auf einem Windows-Client ein. Die auf Ihrer LANCOM R&S®Unified Firewall konfigurierten Regeln, die diese Benutzer betreffen, werden dann automatisch angewandt.

Um SSO mit LANCOM R&S®Unified Firewall in einer Active Directory-Umgebung zu verwenden, müssen folgende Voraussetzungen erfüllt werden:

1. Da Kerberos zeitgebunden ist, stellen Sie sicher, dass für alle SSO-Komponenten (Domain Controller, Windows-Client und LANCOM R&S®Unified Firewall) die gleiche Uhrzeit und der gleiche NTP-Server eingestellt ist.
2. Erstellen des Benutzers `gpLogin`

   Im Active Directory muss in der Benutzerverwaltung unter „CN=Users" ein normaler Domänenbenutzer erstellt werden. Diesem Benutzer wird dann ein sogenannter Service Principal Name (SPN) zugewiesen, der für die Authentifizierung Ihrer LANCOM R&S®Unified Firewall beim Server notwendig ist. Der Benutzer benötigt keine besonderen Rechte.

   a. Öffnen Sie den Domain Controller.

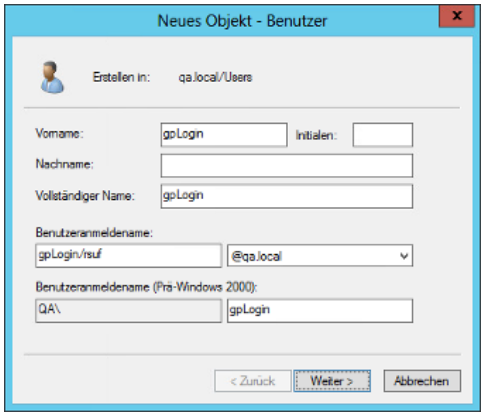


Abbildung 35: Benutzer anlegen

   b. Geben Sie unter **Vorname** `gpLogin` ein.

   Mit diesem Namen ist es später einfacher, den Benutzer in der Benutzerübersicht zu finden.

   c. Geben Sie unter **Benutzeranmeldename** `gpLogin/<firewall name>` ein.

   Im oberen Beispiel lautet der Hostname (`<firewall name>`) Ihrer LANCOM R&S®Unified Firewall `rsuf`, folglich lautet der Login-Name des Benutzers `gpLogin/rsuf`.

   d. Geben Sie unter **Benutzeranmeldename (Prä-Windows 2000)** `gpLogin` ein.

   e. Klicken Sie auf **Weiter**.

f. Geben Sie ein Passwort für den Benutzer ein und bestätigen Sie es.

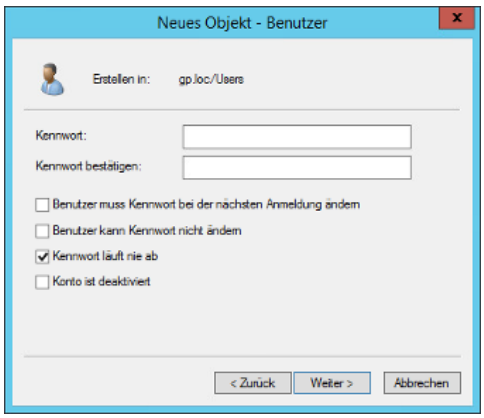


Abbildung 36: Benutzerpasswort eingeben

g. Setzen Sie den Haken im Kontrollkästchen **Passwort läuft nie ab**.

h. Klicken Sie auf **Weiter**.

i. Um die Details zum neuen Benutzer zu überprüfen, klicken Sie auf **Beenden**.

Der Benutzer `gpLogin` wird erstellt.

3. Login mit dem Benutzer `gpLogin` zur Abfrage des Active Directory.

Geben Sie im Eingabefeld **Benutzername** unter **Authentifizierungs-Server** `gpLogin` ein.

4. Konfigurieren des Service Principal Name (SPN).

Weisen Sie dem neu erstellten Benutzer einen SPN zu, sodass Ihre LANCOM R&S®Unified Firewall den Domain Controller als vertrauenswürdig erkennen kann. Führen Sie hierzu den folgenden Befehl im Domain Controller aus:
`setspn -A gpLogin/rsuf gpLogin`

5. Erzeugen eines Kerberos-Schlüssels

Mithilfe des LANCOM R&S®Unified Firewall Single Sign-On-Client kann ein Benutzerlogin auf der Windows-Domäne an Ihre LANCOM R&S®Unified Firewall weitergeleitet werden. Mit dem Kerberos-Schlüssel kann Ihre LANCOM R&S®Unified Firewall die weitergeleiteten Informationen prüfen und die benutzerspezifischen Firewall-Regeln aktivieren. Gehen Sie wie folgt vor, um einen Kerberos-Schlüssel zu erzeugen:

a. Loggen Sie sich auf Ihrer LANCOM R&S®Unified Firewall ein.

b. Navigieren Sie zu **Benutzerauthentifizierung** > **LDAP/AP**.

c. Klicken Sie im Tab **Kerberos** auf die Schaltfläche **Kerberos-Schlüssel erstellen**, um den Kerberos-Schlüssel zu erzeugen.

Das Active Directory wird abgefragt, um den spezifizierten AD-Benutzer zu validieren und relevante Informationen wie beispielsweise die Versionsnummer des Kerberos-Schlüssels zu erhalten. Mit diesen Informationen kann Ihre LANCOM R&S®Unified Firewall lokal einen gültigen Kerberos-Schlüssel erzeugen.

6. Aktivieren von SSO auf Ihrer LANCOM R&S®Unified Firewall

Gehen Sie wie folgt vor, um SSO auf Ihrer LANCOM R&S®Unified Firewall zu aktivieren:

a. Setzen Sie den Haken im Kontrollkästchen **Aktiv** im Tab **Kerberos**.

b. Klicken Sie auf**Speichern**, um Ihre Einstellungen zu speichern.

7. Vorbereiten des Windows-Clients.

Das ZIP-Archiv mit dem Windows Installer für den Single-Sign-On-Client finden Sie auf:

https://www.lancom-systems.de/downloads/

Es gibt drei Möglichkeiten, den LANCOM R&S®Unified Firewall Single-Sign-On-Client zu installieren:

- Kopieren Sie die eigenständige Anwendung `UAClientSSO.exe` an den gewünschten Zielort.
- Führen Sie das Setupprogramm `UAClientSSOSetup.exe` aus und installieren Sie die eigenständige Anwendung `UAClientSSO.exe` im folgenden Pfad:

  `C:\Program Files\R&S Cybersecurity\UA Client\3.0\`
- Installieren Sie den Client über die Domain und verwenden Sie dabei den Microsoft-Installer `UAClientSSO.msi` in einem Gruppenrichtlinienobjekt.

In allen Fällen wird die eigenständige Anwendung `UAClientSSO.exe` auf dem Windows-PC installiert. Sie kann daraufhin ausgeführt werden, wenn die folgenden Parameter gegeben sind:

- Hostname der LANCOM R&S®Unified Firewall (weitere Informationen finden Sie unter *Einstellungen* auf Seite 176).
- IP-Adresse der LANCOM R&S®Unified Firewall im Netzwerk des Client-Computers.

Beispiel: Der Hostname Ihrer LANCOM R&S®Unified Firewall ist „rsuf". Die IP-Adresse im Netzwerk des Client-Computers ist 192.168.0.1. Der Zielpfad für die Installation des LANCOM R&S®Unified Firewall Single-Sign-On-Clients ist demnach:

`C:\Program Files\R&S Cybersecurity\UA Client\3.0\UAClientSSO.exe rsuf 192.168.0.1`.

3.4.6.3 LDAP/AD

Hier können Sie die Verbindungsparameter für den Verzeichnisserver angeben, der zur Verwaltung der LDAP-Benutzer in Ihrem Netzwerk genutzt wird.

Im Tab **Authentifizierungs-Server** können Sie angeben, welchen Datenbanktyp Sie benutzen wollen. Sie können die lokale Benutzer-Datenbank in der LANCOM R&S®Unified Firewall unabhängig benutzen, oder zusätzlich zum Microsoft-Active-Directory-Server oder zum openLDAP-Server mit Kerberos als externe Benutzer-Datenbank.

Wenn Sie `Microsoft Active Directory Server` auswählen, können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Host	Geben Sie den Hostnamen oder die IP-Adresse des Directory-Servers ein. Wenn Sie den Hostnamen des Directory-Servers eingeben, müssen Sie die DNS-Einstellungen konfigurieren. Andernfalls kann der Name nicht aufgelöst werden.
Port	Geben Sie die Port-Nummer des Directory-Servers ein, die für die Kommunikation genutzt werden soll. Sie können die Port-Nummer auch über Pfeil nach oben / nach unten auswählen.
Benutzername	Geben Sie den Namen eines leseberechtigten Benutzers ein, um die Liste der Domänenbenutzer aus dem Active Directory abzurufen. Dieses Eingabefeld muss mit dem Benutzerattribut sAMAccountName übereinstimmen. Der Benutzer muss in „CN=Users" eingeordnet sein. Weitere Informationen finden Sie unter *Login über den LANCOM R&S®Unified Firewall Single Sign-On-Client* auf Seite 168.

Eingabefeld	Beschreibung
Kennwort	Geben Sie das Passwort des leseberechtigten Benutzers ein. Es ist empfohlen, einen dedizierten Benutzer für diesen Zweck zu erstellen.
Domainname	Geben Sie den Domänennamen des Active Directorys ein.
StartTLS	Um die Verbindungssicherheit zum openLDAP- oder Microsoft-Active-Directory-Server zu gewährleisten können Sie das Protokoll **StartTLS** aktivieren. Geben Sie in diesem Fall auch die zu verwendende **Server-CA** an.

Um die konfigurierten Einstellungen für Microsoft Active Directory Server zu prüfen, klicken Sie auf **AD-Einstellungen testen**.

Wenn Sie `OpenLDAP Server` auswählen, können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Server-Adresse	Geben Sie den Hostnamen oder die IP-Adresse des Directory-Servers ein. Wenn Sie den Hostnamen des Directory-Servers eingeben, müssen Sie die DNS-Einstellungen konfigurieren. Andernfalls kann der Name nicht aufgelöst werden.
Port	Geben Sie die Port-Nummer des Directory-Servers ein, die für die Kommunikation genutzt werden soll. Sie können die Port-Nummer auch über Pfeil nach oben / nach unten auswählen.
User-DN	Geben Sie den Benutzerdomänennamen eines leseberechtigten Kontos ein. Es ist nicht erforderlich, den kompletten Benutzerdomänennamen einzugeben. Wenn Sie auf **Speichern** klicken, fügt das System die Domain Components vom **Base-DN**-Eintrag automatisch hinzu.
Kennwort	Geben Sie das Passwort des leseberechtigten Benutzers ein.
Base-DN	Geben Sie einen eindeutigen Namen (Base-DN) als Abfolge von Relative Distinguished Names (RDN, Relative Eindeutige Namen) und verbunden durch Kommas ein, zum Beispiel drei Domain Components: `dc=ldap,dc=example,dc=com`, um den Ort im Verzeichnis festzulegen, von dem aus die Verzeichnissuche starten soll.
User-Query	Optional: Geben Sie den Filter an, der verwendet werden soll, um die Liste der Benutzer abzurufen.
User-ID	Optional: Legen Sie die Attribute fest, von denen aus das Benutzer-Identifizierungszeichen abgerufen wird. Der im Webclient angezeigte Benutzername kommt aus diesem Attribut des LDAP-Benutzers. Das Benutzer-Identifizierungszeichen wird standardmäßig aus dem Attribut `sAMAccountName` abgerufen.
User-Name	Optional: Legen Sie das Attribut fest, aus dem der Benutzername abgerufen wird.
User-Gruppe	Optional: Legen Sie das Attribut fest, aus dem die Benutzergruppe abgerufen wird.
User-Primary-Group	Optional: Legen Sie das Attribut fest, aus dem die primäre Benutzergruppe abgerufen wird.
Mail-Query	Optional: Geben Sie den Filter an, der verwendet werden soll, um die E-Mail-Liste abzurufen.
Mail-Name	Optional: Legen Sie das Attribut fest, aus dem der E-Mail-Name abgerufen wird.
Group-Query	Optional: Geben Sie den Filter an, der verwendet werden soll, um die Liste der Gruppen abzurufen.

Eingabefeld	Beschreibung
Group-Name	Optional: Legen Sie das Attribut fest, aus dem der E-Mail-Name abgerufen wird.
Group-ID	Optional: Legen Sie das Attribut fest, aus dem das Gruppen-Identifizierungszeichen abgerufen wird.
Group-Primary-ID	Optional: Legen Sie das Attribut fest, aus dem das primäre Gruppen-Identifizierungszeichen abgerufen wird.
Group-Parent	Optional: Legen Sie das Attribut fest, aus dem die übergeordnete Gruppe abgerufen wird.
StartTLS	Um die Verbindungssicherheit zum openLDAP- oder Microsoft-Active-Directory-Server zu gewährleisten können Sie das Protokoll **StartTLS** aktivieren. Geben Sie in diesem Fall auch die zu verwendende **Server-CA** an.

Wenn Sie auf **Speichern** klicken, ergänzt das System mit standardmäßigen Werten alle optionalen Felder, in denen Sie nichts angegeben haben.

Wenn Sie bei Single-Sign-On Kerberos verwenden möchten, muss der Benutzername `gpLogin` sein. Der Hostname und die Domain Ihrer Firewall wird aus den allgemeinen Einstellungen entnommen. Siehe *Allgemeine Einstellungen* auf Seite 35. Weitere Informationen finden Sie unter *Einloggen* auf Seite 165.

Im Tab **Kerberos** :

Eingabefeld	Beschreibung
Aktiv	Wählen Sie dieses Kontrollkästchen, um den Kerberos-Dienst zu aktivieren.
Kerberos-Schlüssel	Zeigt den Dienstnamen, den Hostnamen und den Domänennamen bezüglich des userPrincipalName des zuletzt erzeugten Kerberos-Schlüssels an, auch Keytab genannt. Weitere Informationen finden Sie unter *Einloggen* auf Seite 165.

3.4.6.4 Externes Portal

Das externe Benutzer-Portal erlaubt es dem Administrator, einzelnen oder mehreren Benutzern den beschränkten Zugriff auf die Firewall einzurichten. Über diesen Zugriff haben diese die Möglichkeit, bereitgestellte Dateien oder Information direkt zu erhalten. Dies sind z. B. IPsec-Konfigurations-Dateien, die für die Konfiguration des LANCOM Advanced VPN Client zur Herstellung einer VPN-Verbindung zu Ihrer LANCOM R&S®Unified Firewall benötigt werden.

Hierzu sind die folgenden Konfigurationsschritte notwendig:

- Erstellen Sie ein Zertifikat für den Zugriff über HTTPS.

  Für das externe Portal empfiehlt sich ein Zertifikat einer vetrauenswürdingen Zertifizierungsstelle!

- Erstellen Sie lokale Benutzer oder konfigurieren Sie den Zugrif zu einem Directory Server (openLDAP oder Microsoft Active Directory).
- Erstellen Sie eine IPsec-Client-to-Site-Verbindung.
- Konfigurieren Sie unter **Benutzerauthentifizierung** > **Externes Portal** > **Einstellungen** das externe Portal.
- Erstellen Sie unter **Benutzerauthentifizierung** > **Externes Portal** > **VPN-Profile** ein neues Profil und weisen Sie damit die VPN-Verbindung den Benutzern zu.

Anschließend können sich die Benutzer über die konfigurierte Adresse bei der Firewall einloggen.

3.4.6.4.1 Einstellungen

Mit den **Einstellungen** des externen Portals können Sie die Benutzerauthentifizierung für externe Benutzer generell aktivieren oder deaktivieren.

Das externe Portal verwendet zur Bereitstellung des Web-Zugriffs das Reverse-Proxy-System, so dass die Einstellungen analog zu den Einstellungen für ein Reverse-Proxy-Frontend sind mit folgenden Unterschieden:

- SSL ist immer aktiviert
- Kein „Outlook Anywhere“, Proxy-Pfade oder Blockierte Pfade
- Für das externe Portal wird im Backend ein separates Reverse-Proxy-Backend erstellt, aber nicht in der Backend-Liste aufgeführt.
- Die Einstellungen für das externe Portal erscheinen auch nicht in der Liste der Frontends, werden aber bei der Validierung von Einstellungen wie ein Frontend behandelt.

Navigieren Sie zu **Benutzerauthentifizierung** > **Externes Portal** > **Einstellungen**, um ein Bearbeitungsfenster zu öffnen, in dem Sie die generellen Einstellungen für die Benutzerauthentifizierung erstellen können.

Im Bearbeitungsfenster **Externes Portal** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
I/0	Ein Schiebeschalter gibt an, ob das externe Portal derzeit aktiv (**I**) oder inaktiv (**0**) ist. Indem Sie auf den Schiebeschalter klicken, können Sie den Status der Benutzerauthentifizierung ändern. Die Benutzerauthentifizierung ist standardmäßig deaktiviert.
Domäne oder IP-Adresse	Geben Sie den Namen der Domain oder die IP-Adresse ein, der das externe Portal zugewiesen ist.
Cookie-Domain für Reverse-Proxy-Authentifizierung	Für die Reverse-Proxy-Authentifizierung (vgl. *Reverse-Proxy* auf Seite 147) werden Cookies verwendet. Damit diese Cookies unter den korrekten Bedingungen vom Browser an den Server gesendet werden, kann es nötig sein, das `domain` Attribut des Cookies enstprechend zu setzen. Ist dieses Feld leer, dann wird die Cookie-Domain nicht explizit gesetzt und entspricht der Domain- oder IP-Angabe des externen Portals. Wurde der Wert vom Benutzer nicht angepasst, wird ein sinnvoller Standard-Wert vewendet: › Keine Cookie-Domain bei Angabe einer IP-Adresse. › Die angegebene Domain, falls es sich um eine Second Level Domain handelt (sie also direkt unterhalb einer TLD liegt, wie example.com). › Die nächsthöhere Domain, falls es es sich um eine Subdomain handelt. Also für portal.example.com dann z. B. example.com. Die Cookie-Domain ist wichtig, damit eine erfolgreiche Authentifizierung am externen Portal, das zum Beispiel unter portal.example.com gehostet wird, auch für weitere Dienste auf anderen Subdomains effektiv ist, wie zum Beispiel webmail.example.com oder intranet.example.com. Für besondere Fälle kann die Cookie Domain manuell auf einen eigenen Wert gesetzt werden. **Wichtiger Sicherheitshinweis:** Das Setzen einer Cookie-Domain veranlasst den Browser, diesen Cookie bei Anfragen an die angegebene Domain an den Zielserver zu schicken. Bei dem Cookie für die Reverse-Proxy-Authentifizierung handelt es sich um eine sensible Information, die dem Besitzer den Zugriff auf per Reverse Proxy freigegebene Ressourcen ermöglicht. Es sollten nur Cookie-Domains angegeben werden, die uneingeschränkt vertrauenswürdig sind.
Verbindung	Wählen Sie eine Verbindung aus. Sie können sowohl eine Netzwerkverbindung, eine PPP-Verbindung als auch eine Wireguard-Verbindung auswählen.
Port	Konfigurieren Sie den extern erreichbaren Listen-Port für das externe Portal.
Let's Encrypt verwenden	Verwendet ein Let's Encrypt-Zertifikat. Siehe *Let's Encrypt* auf Seite 215. Eine Einschränkung bei der Verwendung von Let's Encrypt ist, dass keine IP-Adressen im Feld **Domäne oder IP-Adresse** verwendet werden können, sondern ausschließlich Domänennamen.

3.4.6.4.2 VPN-Profile

Die VPN-Profile dienen zur Erstellung und Bereitstellung der VPN-Konfigurationsdateien für die konfigurierten Benutzer. Die VPN-Konfigurationsdateien gleichen den Zip-Dateien, die der Benutzer erhält, wenn er die IPsec-Verbindung über

die Export-Schaltfläche erzeugt, mit der Ausnahme, dass diese Konfigurationsdateien nicht durch ein Passwort geschützt sind.

Im Bearbeitungsfenster **VPN-Profile** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Name	Geben Sie dieser Vorlage einen aussagekräftigen Namen.
IPsec-Verbindung	Hier wird die IPsec-Verbindung gewählt, die als Konfigurations-Datei dem Benutzer im externen Portal zur Verfügung gestellt werden soll.
Gateway	Zu dieser Adresse baut der LANCOM Advanced VPN Client die Verbindung auf.
Remote Zertifikat	Zertifikat der Gegenstelle.
Schlüssel-Passwort	Geben Sie das Passwort zum Entschlüsseln des Private Key des Client Zertifikats an.
Transport-Passwort	Geben Sie das Passwort zum Verschlüsseln des p12 Transport Containers an.
Benutzer	Geben Sie die Benutzer an, für die dieses Profil gelten soll. Die Zuordnung von mehreren Benutzern zu einer IPsec-Verbindung ist nur sinnvoll in Verbindung mit XAuth oder EAP. Im Portal sehen Benutzer nur die Ihnen zugeordneten Profile.

3.4.6.4.3 SAML / Single Sign-On

Das externe Portal unterstützt Single Sign-On an ausgewählten Identity Providern (IdP) mittels SAML. Unterstützt werden Microsoft Azure und Keycloak.

Navigieren Sie zu **Benutzerauthentifizierung** > **Externes Portal** > **SAML**, um ein Bearbeitungsfenster zu öffnen, in dem Sie die Einstellungen für SAML bearbeiten können.

Im Bearbeitungsfenster **SAML** können Sie die folgenden Elemente konfigurieren:

IdP-Synchronisation

Diese Einstellungen sind notwendig für die Verbindung der Firewall mit dem IdP. Über diese Verbindung können dann Listen der dem IdP bekannten Benutzer und Gruppen abgerufen werden.

Eingabefeld	Beschreibung
I/**0**	Ein Schiebeschalter gibt an, ob die SAML-Anbindung derzeit aktiv (**I**) oder inaktiv (**0**) ist. Indem Sie auf den Schiebeschalter klicken, können Sie den Status ändern. Die SAML-Anbindung ist standardmäßig deaktiviert.
IdP-Typ	Azure oder Keycloak. Abhängig vom Typ ergeben sich unterschiedliche Angaben.
Basis-URL	Die URL, unter der die IdP-API erreicht werden kann. Bei Keycloak ist das der Hostname bzw. die IP-Adresse und der Port des Keycloak-Servers. Bei Azure setzt sich die URL aus dem Hostnamen (z. B. „https://sts.windows.net/“) und der Tenant-ID zusammen. Z. B. „https://sts.windows.net/ac564d8f-3367-c9a1-31dd-68e35de484ac“
IdP-Zertifikat (PEM)	Optional. Falls die Verbindung der Firewall zum IdP ein Zertifikat verwendet, dem die Firewall nicht vertraut, kann dieses hier hinterlegt werden, so dass eine sichere Verbindung aufgebaut werden kann. Das ist z. B. für selbst-signierte Zertifkate hilfreich. Es kann in Textform eingegeben werden oder aus einer Datei importiert werden.
IdP-Typ Azure	
Tenant-ID	Azure Tenant ID.
Client-ID	ID des auf dem IdP konfigurierten Klienten, unter dem die Abfragen durchgeführt werden.
Client-Geheimnis	Azure Client-Geheimnis.
Grant-Typ	Immer „Client-Zugangsdaten“.
IdP-Typ Keycloak	

Eingabefeld	Beschreibung
Client-ID	ID des auf dem IdP konfigurierten Klienten, unter dem die Abfragen durchgeführt werden.
Grant-Typ	Immer „Passwort“.
Master-Realm	Der Keycloak Master Realm.
Realm	Der Realm, für den die User und Gruppen abgefragt werden sollen.
Benutzername	Nutzername für die Anmeldung an der Keycloak API.
Passwort	Passwort für die Anmeldung an der Keycloak API.
Synchronisations-Intervall	Intervall zwischen dem Beginn zweier Synchronisations-Vorgängen. Ein Synchronisations-Vorgang wird nur gestartet, wenn der vorherige Synchronisations-Vorgang abgeschlossen ist. Läuft er noch, wird nichts unternommen. Nachdem das Intervall erneut verstrichen ist, wird diese Prüfung wiederholt und ggf. ein neuer Synchronisations-Vorgang gestartet.
Letzte Synchronisation	Zeit des letzten Synchronisations-Vorgangs. Über **Jetzt synchronisieren** kann ein Synchronisations-Vorgang manuell im Hintergrund gestartet werden.

IdP-SAML-Einstellungen

Die IdP-SAML-EInstellungen werden aus der sogenannten „Federation Metadata“-XML-Datei importiert. Diese Datei kann aus dem IdP exportiert werden. Ihr Inhalt hängt von den jeweiligen Einstellungen im IdP ab. Sind noch keine Metadaten importiert worden, zeigt das Formular die dafür vorgesehene Schaltfläche **IdP-Metadaten importieren**. Nach dem Import werden die übernommenen Einstellungen hier angezeigt. Geänderte IdP-Metadaten können mit der Schaltfläche **IdP-Metadaten importieren** am unteren Rand des Editor-Fensters auch später noch importiert werden.

SP-SAML-Einstellungen

Die SP-SAML-Einstellungen beschreiben, wo und wie der auf der Firewall laufende Service Provider für die SAML-Authentifizierung erreicht werden kann. Die Service Provider-Einstellungen können als XML-Datei exportiert werden. Diese XML-Datei kann dann im IdP importiert werden, um die relevanten Einstellungen zu übernehmen.

Eingabefeld	Beschreibung
Identität	Ein frei wählbarer Identifikator für den Service Provider. Z. B. der Firewall Name.
Beschreibung	Eine optionale Bescheibung.
Zertifikat	Das Zertifikat. Bei Azure werden durch eine Limitation von Azure nur Zertifikate mit einer Schlüsselgröße von 2048 Bits unterstützt.
Private-Key-Passwort	Das Passwort für den Private Key des verwendeten Zertifikats.
Antworten signieren	Bei aktivierter Option werden Antworten der Firewall signiert.
Authn-Requests signiert	Bei aktivierter Option werden nur korrekt signierte Authn-Requests akzeptiert.
Logout-Requests signiert	Bei aktivierter Option werden nur korrekt signierte Logout-Requests akzeptiert.
Host	Host-Adresse, unter der der Client den Service Provider erreichen kann. Die Host-Angabe und der Port entsprechen den Einstellungen für das externe Portal (**Benutzerauthentifizierung** > **Externes Portal** > **Einstellungen**, **Domäne oder IP-Adresse** bzw. **Port**). Anpassungen sind nicht möglich.
Assertion Consumer Service POST URL	URL, zu welcher der Client-Browser im Rahmen des Login-Prozesses weitergeleitet wird. Ergibt sich aus der Host-Adresse.
Logout Service Redircect URL	URL, zu der der Client-Browser im Rahmen des Logout-Prozesses weitergeleitet wird. Ergibt sich aus der Host-Adresse.

Nutzer des IdP für das externe Portal

Die Nutzer und Gruppen, die vom für das externe Portal eingerichteten IdP geladen wurden, können zur Anmeldung am externen Portal der Firewall verwendet werden. Entsprechend können diese Nutzer und Gruppen für

- VPN Profile (**Benutzerauthentifizierung** > **Externes Portal** > **VPN-Profile**) und
- Zugangsbeschränkungen zu Reverse Proxy Frontends (**UTM** > **Reverse-Proxy** > **HTTP(S)-Frontends**)

verwendet werden.

3.4.6.5 Internes Portal

Das interne Benutzer-Portal erlaubt es, Benutzern Firewall-Regeln zuzuweisen, wenn diese sich anmelden. Außerdem dient es zur Bereitstellung und Verwaltung von Content-Filter-Codes, um Ausnahmeregelungen zu erlauben.

Pro IP-Adresse darf nur ein Benutzer angemeldet sein.Wenn sich ein Benutzer von einer IP-Adresse aus anmeldet, die bereits für eine Sitzung verwendet wird, wird der zuvor angemeldete Benutzer ausgeloggt und der neue Benutzer angemeldet.

3.4.6.5.1 Einstellungen

Mit den **Einstellungen** des internen Portals können Sie die Benutzerauthentifizierung für interne Benutzer generell aktivieren oder deaktivieren.

Navigieren Sie zu **Benutzerauthentifizierung** > **Internes Portal** > **Einstellungen**, um ein Bearbeitungsfenster zu öffnen, in dem Sie die generellen Einstellungen für die Benutzerauthentifizierung erstellen können.

Im Bearbeitungsfenster **Internes Portal** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
I/**0**	Ein Schiebeschalter gibt an, ob die Benutzer-Authentifizierung derzeit aktiv (**I**) oder inaktiv (**0**) ist. Indem Sie auf den Schiebeschalter klicken, können Sie den Status der Benutzerauthentifizierung ändern. Die Benutzerauthentifizierung ist standardmäßig deaktiviert.
Anmeldungen protokollieren	Aktivieren Sie dieses Kontrollkästchen, wenn Sie alle Logins an der LANCOM R&S®Unified Firewall protokollieren wollen. Unter **Monitoring & Statistiken** > **Protokolle** > **Systemprotokoll** können Sie alle Anmeldeereignisse einsehen.
Anmelde-Modus	Wählen Sie eine der folgenden vier Optionen aus: › **Einfache Anmeldung (weitere Anmeldung verhindern)** – Kein Benutzer kann aus mehr als einer IP-Adresse gleichzeitig angemeldet sein. › **Einfache Anmeldung (vorherige Anmeldung trennen)** – Alle früheren Anmeldungen werden abgemeldet,wenn der Benutzer sich von einer anderen IP-Adresse anmeldet. › **Mehrfache Anmeldung** – Benutzer können sich von bis zu 254 verschiedenen IP-Adressen gleichzeitig anmelden. › **Mehrfache Anmeldung (mit Warnung im Bericht)** – Benutzer können sich von bis zu 254 verschiedenen IP-Adressen gleichzeitig anmelden und Warnmeldungen werden im Bericht ausgegeben.
Web-Login-Port	Legen Sie den HTTPS-Port für die Webanmeldung fest, indem Sie über Pfeil nach oben / nach unten navigieren oder Sie die Portnummer eingeben. Die Standardeinstellung ist Port `443`.
Kompatibilitäts-Modus	Aktivieren Sie dieses Kontrollkästchen, wenn Sie für die Anmeldung bei der LANCOM R&S®Unified Firewall Benutzerauthentifizierung-Clients verwenden, die älter sind als Version 3.0.0.

Eingabefeld	Beschreibung
	Indem Sie dieses Kontrollkästchen aktivieren, bringen Sie ihre Netzwerksicherheit in Gefahr. Weitere Informationen finden Sie unter *Benutzerauthentifizierung* auf Seite 164.
Landing Page anzeigen	Optional: Aktivieren Sie dieses Kontrollkästchen, um eine Landingpage anzuzeigen, wenn ein unberechtigter Benutzer versucht, auf das Internet zuzugreifen.

Für jede IP-Adresse wird eine einzige Benutzeranmeldung unterstützt, auch wenn der Modus **Mehrfache Anmeldung** aktiviert ist.

3.4.6.5.2 SAML / Single Sign-On

Das interne Portal unterstützt Single Sign-On an ausgewählten Identity Providern (IdP) mittels SAML. Unterstützt werden Microsoft Azure und Keycloak.

Navigieren Sie zu **Benutzerauthentifizierung** > **Internes Portal** > **SAML**, um ein Bearbeitungsfenster zu öffnen, in dem Sie die Einstellungen für SAML anpassen können.

Im Bearbeitungsfenster **SAML** können Sie die folgenden Elemente konfigurieren:

IdP-Synchronisation

Diese Einstellungen sind notwendig für die Verbindung der Firewall mit dem IdP. Über diese Verbindung können dann Listen der dem IdP bekannten Benutzer und Gruppen abgerufen werden.

Eingabefeld	Beschreibung
I/**0**	Ein Schiebeschalter gibt an, ob die SAML-Anbindung derzeit aktiv (**I**) oder inaktiv (**0**) ist. Indem Sie auf den Schiebeschalter klicken, können Sie den Status ändern. Die SAML-Anbindung ist standardmäßig deaktiviert.
IdP-Typ	Azure oder Keycloak. Abhängig vom Typ ergeben sich unterschiedliche Angaben.
Basis-URL	Die URL, unter der die IdP-API erreicht werden kann. Bei Keycloak ist das der Hostname bzw. die IP-Adresse und der Port des Keycloak-Servers. Bei Azure setzt sich die URL aus dem Hostnamen (z. B. „https://sts.windows.net/“) und der Tenant-ID zusammen. Z. B. „https://sts.windows.net/ac564d8f-3367-c9a1-31dd-68e35de484ac“
IdP-Zertifikat (PEM)	Optional. Falls die Verbindung der Firewall zum IdP ein Zertifikat verwendet, dem die Firewall nicht vertraut, kann dieses hier hinterlegt werden, so dass eine sichere Verbindung aufgebaut werden kann. Das ist z. B. für selbst-signierte Zertifkate hilfreich. Es kann in Textform eingegeben werden oder aus einer Datei importiert werden.
IdP-Typ Azure	
Tenant-ID	Azure Tenant ID.
Client-ID	ID des auf dem IdP konfigurierten Klienten, unter dem die Abfragen durchgeführt werden.
Client-Geheimnis	Azure Client-Geheimnis.
Grant-Typ	Immer „Client-Zugangsdaten“.
IdP-Typ Keycloak	
Client-ID	ID des auf dem IdP konfigurierten Klienten, unter dem die Abfragen durchgeführt werden.
Grant-Typ	Immer „Passwort“.
Master-Realm	Der Keycloak Master Realm.

Eingabefeld	Beschreibung
Realm	Der Realm, für den die User und Gruppen abgefragt werden sollen.
Benutzername	Nutzername für die Anmeldung an der Keycloak API.
Passwort	Passwort für die Anmeldung an der Keycloak API.
Synchronisations-Intervall	Intervall zwischen dem Beginn zweier Synchronisations-Vorgängen. Ein Synchronisations-Vorgang wird nur gestartet, wenn der vorherige Synchronisations-Vorgang abgeschlossen ist. Läuft er noch, wird nichts unternommen. Nachdem das Intervall erneut verstrichen ist, wird diese Prüfung wiederholt und ggf. ein neuer Synchronisations-Vorgang gestartet.
Letzte Synchronisation	Zeit des letzten Synchronisations-Vorgangs. Über **Jetzt synchronisieren** kann ein Synchronisations-Vorgang manuell im Hintergrund gestartet werden.

IdP-SAML-Einstellungen

Die IdP-SAML-EInstellungen werden aus der sogenannten „Federation Metadata"-XML-Datei importiert. Diese Datei kann aus dem IdP exportiert werden. Ihr Inhalt hängt von den jeweiligen Einstellungen im IdP ab. Sind noch keine Metadaten importiert worden, zeigt das Formular die dafür vorgesehene Schaltfläche **IdP-Metadaten importieren**. Nach dem Import werden die übernommenen Einstellungen hier angezeigt. Geänderte IdP-Metadaten können mit der Schaltfläche **IdP-Metadaten importieren** am unteren Rand des Editor-Fensters auch später noch importiert werden.

SP-SAML-Einstellungen

Die SP-SAML-Einstellungen beschreiben, wo und wie der auf der Firewall laufende Service Provider für die SAML-Authentifizierung erreicht werden kann. Die Service Provider-Einstellungen können als XML-Datei exportiert werden. Diese XML-Datei kann dann im IdP importiert werden, um die relevanten Einstellungen zu übernehmen.

Eingabefeld	Beschreibung
Identität	Ein frei wählbarer Identifikator für den Service Provider. Z. B. der Firewall Name.
Beschreibung	Eine optionale Bescheibung.
Zertifikat	Das Zertifikat. Bei Azure werden durch eine Limitation von Azure nur Zertifikate mit einer Schlüsselgröße von 2048 Bits unterstützt.
Private-Key-Passwort	Das Passwort für den Private Key des verwendeten Zertifikats.
Antworten signieren	Bei aktivierter Option werden Antworten der Firewall signiert.
Authn-Requests signiert	Bei aktivierter Option werden nur korrekt signierte Authn-Requests akzeptiert.
Logout-Requests signiert	Bei aktivierter Option werden nur korrekt signierte Logout-Requests akzeptiert.
Host	Host-Adresse, unter der der Client den Service Provider erreichen kann. Der Port entspricht immer dem **Web-Login-Port** des internen Portals (**Benutzerauthentifizierung** > **Internes Portal** > **Einstellungen**). Der Host-Anteil kann frei gewählt werden. Hier sollte eine IP-Adresse oder ein entsprechend auflösender Hostname angegeben werden, die / der zu einem Intranet-Interface der Firewall gehört. Nur auf diesen Interfaces ist das interne Portal und der Service Provider erreichbar.
Assertion Consumer Service POST URL	URL, zu welcher der Client-Browser im Rahmen des Login-Prozesses weitergeleitet wird. Ergibt sich aus der Host-Adresse.
Logout Service Redircect URL	URL, zu der der Client-Browser im Rahmen des Logout-Prozesses weitergeleitet wird. Ergibt sich aus der Host-Adresse.

Nutzer des IdP für das interne Portal

Die Nutzer und Gruppen, die vom für das interne Portal eingerichteten IdP geladen wurden, können zur Anmeldung am internen Portal der Firewall verwendet werden. Entsprechend können diese Nutzer und Gruppen für

- die Verwaltung von Content-Filter-Ausnahme-Codes (**UTM** > **URL-/Contentfilter** > **Einstellungen**),
- das Regelwerk auf dem Desktop (Benutzer- und Gruppen-Objekte, sowohl einfache als auch die VPN-Varianten) und
- die Wake-on-LAN-Funktion (**Benutzerauthentifizierung** > **Internes Portal** > **Wake on LAN**)

verwendet werden.

3.4.6.5.3 Wake-on-LAN

Starten Sie Geräte, sobald sich ein Benutzer am internen Portal anmeldet, um Firewall-Regeln zu aktivieren.

Im Bearbeitungsfenster **Wake On LAN** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Benutzer	Wählen Sie im linken Bereich einen Benutzer aus.
MAC-Adresse	Geben Sie im rechten Bereich eine oder mehrere MAC-Adressen an. Sobald sich der Benutzer am internen Portal anmeldet, um Firewall-Regeln zu aktivieren, werden Wake-on-LAN-Pakete an diese MAC-Adresse geschickt, um das entsprechende Gerät zu starten.

Klicken Sie auf **Exportieren**, um Ihre Benuterz-MAC-Adressen in das Dateisystem zu exportieren. Klicken Sie auf **Importieren**, um Benutzer-MAC-Adressen zu importieren.

3.4.6.6 Benutzer

Wie Computer können auch Benutzer und LDAP-Gruppen auf dem Desktop als einzelne Benutzer oder Benutzergruppen eingerichtet werden.

Für diese Desktop-Objekte können Sie dann Regeln bestimmen, die den Benutzern zugewiesen werden, sobald sie sich einloggen.Wenn ein Benutzer sich von einem Computer aus einloggt, dem bestimmte Regeln zugewiesen sind, werden dem Benutzer die Regeln dieses Computers zusammen mit seinen benutzerspezifischen Regeln zugewiesen. Sie können Benutzer und LDAP-Gruppen aus der lokalen Benutzerdatenbank Ihrer LANCOM R&S®Unified Firewall und aus dem openLDAP- oder Active Directory-Authentifizierungsserver auswählen und sie den Benutzergruppen auf dem Desktop hinzufügen. Es gibt auch eine spezielle **Standard-Benutzergruppe**, die auf dem Desktop ausgewählt werden kann. Zu dieser Benutzergruppe kann kein Benutzer hinzugefügt werden. Sie besteht aus allen Benutzern, die sich einloggen können, jedoch noch nicht als einzelne Benutzer oder Mitglieder einer anderen Benutzergruppe auf dem Desktop eingerichtet wurden. Wenn eine Standard-Benutzergruppe auf dem Desktop eingerichtet ist, der Sie Regeln zugewiesen haben, werden Benutzer, die nachträglich auf dem Active-Directory-Server erstellt werden, automatisch zu dieser Standard-Benutzergruppe hinzugefügt. Nach dem Login werden diesen neuen Benutzern die Standard-Regeln ohne weiteren Verwaltungsaufwand automatisch zugewiesen.

3.4.6.7 LDAP-Benutzer

Es ist möglich, Ihre LANCOM R&S®Unified Firewall über das Lightweight Directory Access Protocol (LDAP) mit einem externen Verzeichnisserver zu verbinden, um von dort Benutzer abzurufen. Diese Benutzer können dann in benutzerspezifische Firewall-Regeln eingebunden werden.

Außerdem können Sie LDAP verwenden, um auf Verzeichnisdienste zuzugreifen und um Benutzerdaten zu verwalten.

Verbinden Sie sich wie unter *LDAP/AD* auf Seite 170 beschrieben mit einem Verzeichnisserver.

Navigieren Sie zu **Benutzerauthentifizierung** > **LDAP-Benutzer**, um die Liste der derzeit im Verzeichnisserver angelegten LDAP-Benutzer in der Objektleiste anzuzeigen.

Um die hier aufgelisteten LDAP-Benutzer für Verbindungen und gruppenspezifische Firewall-Regeln zur Verfügung stellen zu können, müssen die Gruppen einem Benutzer-Desktopobjekt zugewiesen werden. Weitere Informationen finden Sie unter *Benutzergruppen* auf Seite 122.

3.4.6.8 LDAP-Gruppen

Es ist möglich, Ihre LANCOM R&S®Unified Firewall über das Lightweight Directory Access Protocol (LDAP) mit einem externen Verzeichnisserver zu verbinden, um Benutzergruppen abzurufen. Sie können diese Benutzergruppen in gruppenspezifische Firewall-Regeln einbinden.

Außerdem können Sie LDAP verwenden, um auf Verzeichnisdienste zuzugreifen und um Benutzerdaten zu verwalten.

Verbinden Sie sich wie unter *LDAP/AD* auf Seite 170 beschrieben mit einem Verzeichnisserver.

Navigieren Sie zu **Benutzerauthentifizierung** > **LDAP-Gruppen**, um die Liste der derzeit im Verzeichnisserver angelegten LDAP-Gruppen in der Objektleiste anzuzeigen.

Um die hier aufgelisteten LDAP-Gruppen für Verbindungen und gruppenspezifische Firewall-Regeln zur Verfügung stellen zu können, müssen die Gruppen einem Benutzergruppen-Desktopobjekt zugewiesen werden. Weitere Informationen finden Sie unter *Benutzergruppen* auf Seite 122.

3.4.6.9 Lokale Benutzer

Ihre LANCOM R&S®Unified Firewall bietet eine lokale Benutzeradministration für kleinere Unternehmen ohne zentrale Administration. Nutzen Sie die Einstellungen unter **Lokale Benutzer**, um Benutzernamen und Passwörter anzugeben. Auf diese Weise können Sie Benutzer verwalten und definieren.

Navigieren Sie zu **Benutzerauthentifizierung** > **Lokale Benutzer**, um die Liste der derzeit im System angelegten lokalen Benutzer in der Objektleiste anzuzeigen.

In der erweiterten Ansicht werden in den Tabellenspalten der **Name** des lokalen Benutzers und zusätzlich eine **Beschreibung** angezeigt, sofern diese eingegeben wurde. Mit den Schaltflächen in der letzten Spalte können Sie die Einstellungen eines lokalen Benutzers einsehen und anpassen, einen neuen Benutzer ausgehend von einer Kopie des vorhandenen lokalen Benutzers anlegen, oder einen Benutzer aus dem System löschen.

Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28.

Unter **Benutzerauthentifizierung** > **Lokale Benutzer** können Sie einen neuen Benutzer hinzufügen oder einen vorhandenen lokalen Benutzer bearbeiten.

Im Bearbeitungsfenster **Lokale Benutzer-Authentifizierung** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Benutzername	Geben Sie einen eindeutigen Namen für den lokalen Benutzer ein. Dieser Name dient als Anmeldename. Der Anmeldename des Benutzers muss exakt mit dem **Benutzername** übereinstimmen (Groß- und Kleinschreibung ist zu beachten). Andernfalls entspricht der Name in den benutzerspezifischen Firewall-Regeln nicht dem Namen des sich am Client anmeldenden Benutzers und die Regeln stimmen nicht überein.
Beschreibung	Optional: Die hier erfolgten Angaben dienen nur der internen Nutzung durch den Administrator.
Kennwort	Geben Sie ein Passwort für den Benutzer ein und bestätigen Sie es. Das Passwort muss aus mindestens sechs Zeichen bestehen.
Zeige Passwort	Optional: Setzen Sie den Haken in diesem Kontrollkästchen, um das Passwort zu verifizieren.
Kennwort-Änderung erforderlich nach nächster Anmeldung	Optional: Wenn Sie den Haken in diesem Kontrollkästchen setzen, muss der Benutzer sein Passwort nach der nächsten Anmeldung ändern. Hierzu leitet der Webserver den Benutzer von der Anmeldeseite auf eine Seite weiter, auf der das Passwort geändert werden kann.

Die Schaltflächen rechts unten im Bearbeitungsfeld hängen davon ab, ob Sie einen neuen lokalen Benutzer hinzufügen oder einen bestehenden Benutzer bearbeiten. Klicken Sie für einen neu konfigurierten lokalen Benutzer auf **Erstellen**, um den neuen Benutzer zur Liste der verfügbaren lokalen Benutzer hinzuzufügen, oder auf **Abbrechen**, um die Erstellung zu verwerfen.

Wenn Sie Änderungen vorgenommen haben, können Sie diese mit den Schaltflächen unten rechts im Bearbeitungsfenster speichern (**Speichern**), oder verwerfen (**Zurücksetzen**). Andernfalls können Sie das Fenster schließen (**Schließen**).

Die hier definierten lokalen Benutzer stehen zur Verwendung in Desktopobjekten wie beispielsweise VPN-Benutzern zur Verfügung.

3.4.6.10 Nicht zugewiesene Benutzer

Navigieren Sie zu **Benutzerauthentifizierung** > **Nicht zugewiesen**, um LDAP-Benutzer anzuzeigen, die Benutzerobjekten auf dem Desktop zugewiesen sind, aber nicht mehr im Verzeichnisdienst aufgerufen werden können.

3.4.6.11 Anwendungsbeispiele

In einer Windows-Domain

Wenn Sie über eine Windows-Domain verfügen, können Sie die Benutzerauthentifizierung mit dem Windows Domain Controller verbinden.

Gehen Sie wie folgt vor, um die Benutzerauthentifizierung mit dem Windows Domain Controller zu verbinden:

1. Navigieren Sie zu **Benutzerauthentifizierung** > **Einstellungen**.
2. Klicken Sie auf **Authentifizierungs-Server**.
3. Geben Sie die Daten ihres Domain-Controllers ein.

   Alle Benutzer in der angegebenen Domain werden in der Benutzerliste angezeigt.
4. Ziehen Sie die Benutzersymbole in das Konfigurationsdesktop und weisen Sie ihnen Regeln zu.

   Um sich einzuloggen, müssen Benutzer die URL mit `https://` und der IP-Adresse der Firewall in der Adressleiste ihres Browsers eingeben. Eine Loginseite erscheint. Nach erfolgreichem Login werden den angegebenen IP-Adressen die Firewall-Regeln des Benutzers zugewiesen. Wenn das Browserfenster geschlossen wird, läuft der Sitzungscookie ab und die Regeln sind nicht mehr gültig.

Den Terminalserver von der Benutzerauthentifizierung ausschließen

Wenn Sie einen Terminalserver verwenden, sollten Sie diesen von der Benutzerauthentifizierung ausschließen. Andernfalls werden alle bisherigen Benutzer ausgeloggt, wenn sich ein neuer Benutzer einloggt.

Gehen Sie wie folgt vor, um den Terminalserver von der Benutzerauthentifizierung auszuschließen.

1. Klicken Sie auf das Hostgruppen-Symbol in der Symbolleiste im oberen Bereich des Desktops.

2. Entfernen Sie den Haken im Kontrollkästchen in der Spalte **Login erlaubt**.

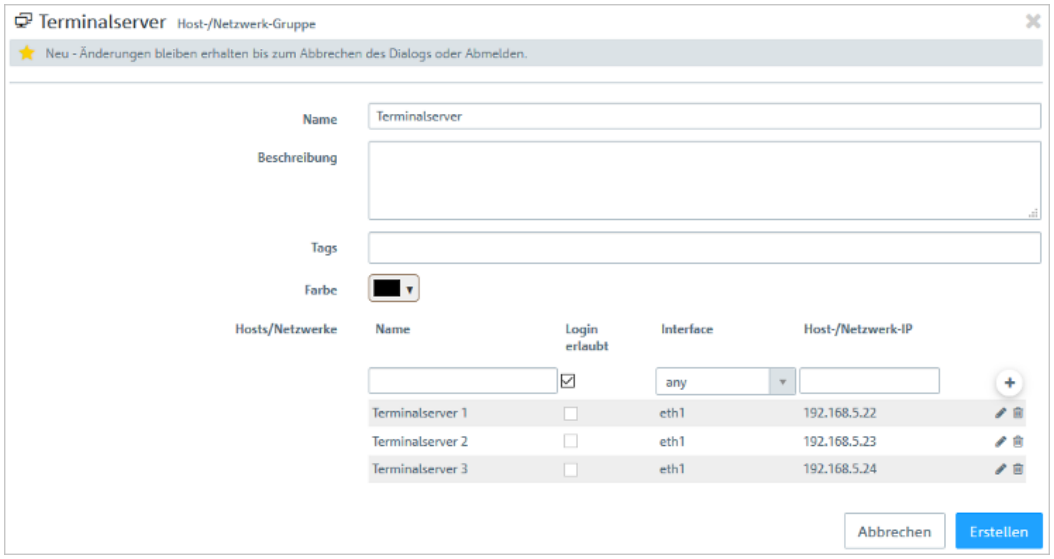


Abbildung 37: Objekteinstellungen – Terminalserver

Falls Ihre Benutzer eine Authentifizierung im Terminalserver benötigen, können Sie Remote-desktop-IP-Virtualisierung im Terminalserver aktivieren. Hierdurch wird allen Benutzern während einer Sitzung eine eigene IP-Adresse zugewiesen.

3.4.7 VPN

Mit den Einstellungen unter **VPN** können Sie Ihre LANCOM R&S®Unified Firewall für die Verwendung als Virtual Private Network-Server konfigurieren, um Client-to-Site (C2S)-VPN-Verbindungen zur Verfügung zu stellen. So können Computer an einem anderen Ort mittels IPsec und VPN-SSL sicher auf Ressourcen im lokalen Netzwerk zugreifen. Durch ein *Site-to-Site* (S2S) VPN-Gateway kann über das Internet mittels IPsec und VPN-SSL ein sicherer Kommunikationskanal zwischen zwei Remote-Netzwerken aufgebaut werden.

Client-to-Site VPN-Verbindungen

Durch eine Client-to-Site VPN-Verbindung kann das Unternehmensnetzwerk von außen erreicht werden. Die Authentifizierung erfolgt entweder über IPsec mit ausgestellten Zertifikaten, mittels eines so genannten PSK (Pre-Shared Key) oder über VPN-SSL mit Zertifikaten.

Client-to-Site-Verbindungen über IPsec und VPN-SSL können abhängig von den Client-Einstellungen in einem von zwei Modi betrieben werden:

- Im *Split-Tunnel-Modus* wird nur die Kommunikation zwischen dem Client und dem internen Netzwerk (z. B. einem Unternehmensnetzwerk) durch die Firewall geleitet. Clients können Geräte im internen Netzwerk über den Tunnel erreichen. Für andere Ziele (wie das Internet) vorgesehene Pakete werden nicht durch die LANCOM R&S®Unified Firewall geroutet.

  Beispiel: Ein Benutzer wählt sich mithilfe eines VPN-Software-Clients per Fernzugriff aus dem Drahtlosnetzwerk eines Hotels in ein Unternehmensnetzwerk ein. Durch Split Tunneling kann der Benutzer sich über die VPN-Verbindung mit Dateiservern, Datenbankenservern, Mailservern und anderen Diensten im Unternehmensnetzwerk verbinden. Verbindet sich der Benutzer mit Internetressourcen (Websites, FTP-Seiten etc.), wird die Verbindungsanfrage direkt über das Gateway des Hotelnetzwerks abgesendet.

- Im *Full-Tunnel-Modus* wird der gesamte Datenverkehr zurück zu Ihrer LANCOM R&S®Unified Firewall geleitet, einschließlich der Kommunikation mit Internetseiten.

Full Tunneling erlaubt es dem Benutzer beispielsweise nicht, über Hotelnetzwerke direkt auf das Internet zuzugreifen. Jeglicher Datenverkehr, der vom Client ausgesendet wird, während die VPN-Verbindung aktiv ist, wird an die Firewall gesendet.

C2S-Verbindungen über IPsec werden mithilfe eines gewöhnlichen VPN-Clients hergestellt, z. B. dem LANCOM Advanced VPN Client. Weitere Informationen finden Sie unter *IPsec-Verbindungs-Einstellungen* auf Seite 194.

VPN-SSL C2S-Verbindungen werden mithilfe eines gewöhnlichen VPN-Clients hergestellt. Weitere Informationen finden Sie unter *VPN-SSL-Verbindungseinstellungen* auf Seite 201.

Site-to-Site VPN-Verbindungen

Bei einer Site-to-Site-Verbindung werden zwei Standorte über einen verschlüsselten Tunnel miteinander zu einem virtuellen Netzwerk verbunden und tauschen durch diesen Tunnel Daten aus. Die beiden Standorte können feste IP-Adressen haben. Die Authentifizierung erfolgt entweder über IPsec mit ausgestellten Zertifikaten, mittels eines so genannten PSK (Pre-Shared Key) oder über VPN-SSL mit Zertifikaten.

IPsec

IPsec (Internet Protocol Security) ist ein Satz von Protokollen, der auf Ebene der Vermittlungsschicht oder der Sicherungsschicht arbeitet und den Austausch von Paketen über nicht vertrauenswürdige Netzwerke (bspw. das Internet) sichert, indem er jedes IP-Paket einer Kommunikationssitzung authentifiziert und verschlüsselt. IPsec erfüllt die höchsten Sicherheitsanforderungen.

VPN-SSL

VPN über SSL bietet eine schnelle und sichere Möglichkeit, eine Roadwarrior-Verbindung einzurichten. Der größte Vorteil an VPN-SSL ist, dass der gesamte Datenverkehr über einen TCP- oder UDP-Port läuft und im Gegensatz zu IPsec keine weiteren speziellen Protokolle benötigt werden.

Stellen Sie vor der Einrichtung von VPN-Verbindungen sicher, dass Sie die notwendigen Zertifikate installiert haben, wie unter *Zertifikatsverwaltung* auf Seite 205 beschrieben.

3.4.7.1 IPsec

Die IPsec-Protokollsuite (Internet Protocol Security) arbeitet auf der Ebene der Vermittlungsschicht und nutzt die Authentifizierung und Verschlüsselung von IP-Paketen, um die Kommunikation in nicht vertrauenswürdigen Netzwerken abzusichern.

Für eine Site-to-Site-Verbindung über IPsec benötigen Sie zwei VPN-IPsec-fähige Server. Für eine Client-to-Site-Verbindung benötigen Sie separate Client-Software.

Ihre LANCOM R&S®Unified Firewall ist in der Lage, mithilfe der IPsec-Protokollsuite sichere Verbindungen aufzubauen und zu nutzen. Ermöglicht wird dies durch ESP im Tunnel-Modus. Der Schlüsselaustausch kann mithilfe von Version 1 des IKE-Protokolls oder des neueren IKEv2 erfolgen. Nach Wahl werden Pre-shared Keys oder Zertifikate nach dem X.509-Standard verwendet. Mit IKEv1 ist auch eine Authentifizierung über XAUTH möglich. Beu IKEv2 gibt es die zusätzliche Authentifizierungsmöglichkeit über EAP.

3.4.7.1.1 IPsec-Einstellungen

Unter **VPN** > **IPsec** > **IPsec-Einstellungen** können Sie IPsec aktivieren und die Einstellungen konfigurieren:

Tabelle 7: Allgemein

Eingabefeld	Beschreibung
I/0	Ein Schiebeschalter gibt an, ob IPSec aktiv (**I**) oder inaktiv (**0**) ist. Mit einem Klick auf den Schiebeschalter ändern Sie den Status dieser Option.
Ausgenommene Interfaces	Auswahlliste, in der Interfaces ausgewählt werden können, die nicht vom IPsec-Dienst verwendet werden sollen. Wenn hier nichts eingetragen ist, dann werden alle Interfaces auf dem System ausgenommen – auch solche die neu erstellt oder automatisch erzeugt werden. Normalerweise werden ausgenomme Interfaces und die ausgenommenen IP-Adressen benötigt, wenn der gesamte Traffic über einen IPsec-Tunnel in die Zentrale geschickt wird. In einem solchen Fall muss man aufpassen, dass die lokalen Netze weiter erreichbar bleiben. Standardmäßig hat IPsec eine höhere Priorität als normale Routen und somit würden selbst Pakete, die für lokale Netze gedacht sind, stattdessen in den VPN-Tunnel geschickt. Im Normalfall bleiben also durch die Voreinstellung, alle lokalen Interfaces auszunehmen, die lokalen Netze immer erreichbar.
Ausgenommene IP-Adressen	Tragen Sie hier IP-Adressen im CIDR-Format ein. Pakete zu diesen Netzen werden unter keinen Umständen in einen Tunnel weitergeleitet, selbst dann nicht, wenn ein Tunnel für die Zieladresse konfiguriert ist. Klicken Sie rechts auf ⊕, um Ihren Eintrag zur Liste der IP-Adressen hinzuzufügen.
Proxy-ARP	Ist diese Option aktiv, dann antwortet die Firewall auf ARP-Anfragen aus lokalen Netzen für virtuelle IP-Adressen, die an IPsec-Clients vergeben wurden, mit der eigenen MAC-Adresse.

Tabelle 8: DHCP-Server

Eingabefeld	Beschreibung
Aktiv	IPsec kann einen DHCP-Server verwenden, um den verbundenen IPsec-Clients virtuelle IP-Adressen zuzuweisen. Hier können Sie diese Funktion aktiveren. Zur Verwendung wählen Sie in einer IPsec-Verbindung bei **Virtueller IP-Pool** die Option **DHCP Virtual-IP pool** aus.
IP-Adresse	Geben Sie hier die IP-Adresse des zu verwendenden DHCP-Servers ein. Dies kann entweder die Adresse eines DHCP-Servers sein oder eine Broadcast-Adresse eines Netzwerks.

Tabelle 9: RADIUS-Server

Eingabefeld	Beschreibung
Aktiv	IPsec kann in Verbindung mit EAP oder XAUTH die Benutzerverwaltung eines RADIUS-Servers verwenden, um die Verbindung zu authentifizieren. Ausserdem können auch IP-Adressen vom RADIUS-Server an IPsec-Clients zugewiesen werden. Dafür wählen Sie in einer IPsec-Verbindung bei **Virtueller IP-Pool** die Option **RADIUS Virtual-IP pool** aus. Hier können Sie diese Funktion aktiveren.
IP-Adresse	IP-Adresse des RADIUS-Servers.
Port	Port des RADIUS-Servers.
Passwort	Passwort für den Zugriff auf den Radius-Server.

Wenn Sie Änderungen vorgenommen haben, können Sie diese mit den Schaltflächen unten rechts im Bearbeitungsfenster speichern (**Speichern**) oder verwerfen (**Zurücksetzen**). Andernfalls können Sie das Fenster schließen (**Schließen**).

Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

3.4.7.1.2 Sicherheits-Profile

Unter **VPN** > **IPsec** > **Sicherheits-Profile** finden Sie eine Liste von vordefinierten Profilen, die Sie mit selbst erstellten Profilen erweitern können.

Die vordefinierten Profile können weder bearbeitet noch gelöscht werden.

Werden verwendete Sicherheits-Profile geändert, können in der erweiterten Listbar alle zugehörigen Verbindungen neugestartet werden. Sicherheits-Profile werden in Vorlagen und Verbindungen gewählt.

Klicken Sie auf ⊕, um ein neues Sicherheitsprofil hinzuzufügen.

Tabelle 10: Allgemeine Einstellungen

Eingabefeld	Beschreibung
Name	Geben Sie diesem Sicherheitsprofil einen aussagekräftigen Namen.
Verwendet in	Zeigt an, in welchen IPsec-Verbindungen dieses Profil aktuell verwendet wird.
Datenkomprimierung	Wenn man hier Datenkomprimierung wählt, dann wird diese für alle Verbindungen aktiviert, die dieses Profil verwenden. Man spart dadurch zwar Bandbreite, erhöht aber auch die CPU-Last. Wenn Sie Datenkomprimierung aktivieren, dann muss diese auch auf der Gegenstelle aktiviert sein.

ISAKMP (IKE)

In diesem Tab können Sicherheits-Einstellungen für die IKE-Phase definiert werden. IKE definiert, wie Sicherheitsparameter vereinbart und gemeinsame Schlüssel ausgetauscht werden

Tabelle 11: ISAKMP (IKE)

Eingabefeld	Beschreibung
IKE-Version	Wählen Sie IKEv1 oder IKEv2
Verschlüsselungsalgorithmen	Wählen Sie aus der Liste der verfügbaren Verschlüsselungsalgorithmen diejenigen aus, die Sie verwenden wollen. IKEv1: › 3DES-EDE-CBC 168 bit (3des) (veraltet) › AES-CBC 128 bit (aes128) › AES-CBC 192 bit (aes192) › AES-CBC 256 bit (aes256) › Blowfish-CBC 128 bit (blowfish128) (veraltet) › Blowfish-CBC 192 bit (blowfish192) (veraltet) › Blowfish-CBC 256 bit (blowfish256) (veraltet) › Serpent-CBC 128 bit (serpent128) › Serpent-CBC 192 bit (serpent192) › Serpent-CBC 256 bit (serpent256) › Twofish-CBC 128 bit (twofish128) › Twofish-CBC 192 bit (twofish192) › Twofish-CBC 256 bit (twofish256) IKEv2:

Eingabefeld	Beschreibung
	> 3DES-EDE-CBC 168 bit (3des) (veraltet) > AES-CBC 128 bit (aes128) > AES-CBC 192 bit (aes192) > AES-CBC 256 bit (aes256) > AES-CCM 128 bit with 64 bit ICV (aes128ccm8) > AES-CCM 128 bit with 96 bit ICV (aes128ccm12) > AES-CCM 128 bit with 128 bit ICV (aes128ccm16) > AES-CCM 192 bit with 64 bit ICV (aes192ccm8) > AES-CCM 192 bit with 96 bit ICV (aes192ccm12) > AES-CCM 192 bit with 128 bit ICV (aes192ccm16) > AES-CCM 256 bit with 64 bit ICV (aes256ccm8) > AES-CCM 256 bit with 96 bit ICV (aes256ccm12) > AES-CCM 256 bit with 128 bit ICV (aes256ccm16) > AES-COUNTER 128 bit (aes128ctr) > AES-COUNTER 192 bit (aes192ctr) > AES-COUNTER 256 bit (aes256ctr) > AES-GCM 128 bit with 64 bit ICV (aes128gcm8) > AES-GCM 128 bit with 96 bit ICV (aes128gcm12) > AES-GCM 128 bit with 128 bit ICV (aes128gcm16) > AES-GCM 192 bit with 64 bit ICV (aes192gcm8) > AES-GCM 192 bit with 96 bit ICV (aes192gcm12) > AES-GCM 192 bit with 128 bit ICV (aes192gcm16) > AES-GCM 256 bit with 64 bit ICV (aes256gcm8) > AES-GCM 256 bit with 96 bit ICV (aes256gcm12) > AES-GCM 256 bit with 128 bit ICV (aes256gcm16) > Blowfish-CBC 128 bit (blowfish128) (veraltet) > Blowfish-CBC 192 bit (blowfish192) (veraltet) > Blowfish-CBC 256 bit (blowfish256) (veraltet) > Camellia-CBC 128 bit (camellia128) > Camellia-CBC 192 bit (camellia192) > Camellia-CBC 256 bit (camellia256) > Camellia-CCM 128 bit with 64 bit ICV (camellia128ccm8) > Camellia-CCM 128 bit with 96 bit ICV (camellia128ccm12) > Camellia-CCM 128 bit with 128 bit ICV (camellia128ccm16) > Camellia-CCM 192 bit with 64 bit ICV (camellia192ccm8) > Camellia-CCM 192 bit with 96 bit ICV (camellia192ccm12) > Camellia-CCM 192 bit with 128 bit ICV (camellia192ccm16) > Camellia-CCM 256 bit with 64 bit ICV (camellia256ccm8) > Camellia-CCM 256 bit with 96 bit ICV (camellia256ccm12) > Camellia-CCM 256 bit with 128 bit ICV (camellia256ccm16) > Camellia-COUNTER 128 bit (camellia128ctr) > Camellia-COUNTER 192 bit (camellia192ctr) > Camellia-COUNTER 256 bit (camellia256ctr) > CAST-CBC 128 bit (cast128) (veraltet) > ChaCha20/Poly1305 256 bit with 128 bit ICV (chacha20poly1305)

Eingabefeld	Beschreibung
Authentifizierungsalgorithmen	Wählen Sie aus der Liste der verfügbaren Authentifizierungsalgorithmen diejenigen aus, die Sie verwenden wollen. IKEv1: › MD5 HMAC 96 bit (md5) › SHA1 HMAC 96 bit (sha1) › SHA2_256 HMAC 128 bit (sha2_256) › SHA2_384 HMAC 192 bit (sha2_384) › SHA2_512 HMAC 256 bit (sha2_512) IKEv2: › AES CMAC 96 bit (aesmac) › AES XCBC 96 bit (aesxcbc) › MD5 HMAC 96 bit (md5) › SHA1 HMAC 96 bit (sha1) › SHA2_256 HMAC 128 bit (sha2_256) › SHA2_384 HMAC 192 bit (sha2_384) › SHA2_512 HMAC 256 bit (sha2_512)
DH-Gruppen	Wählen Sie aus der Liste der verfügbaren Diffie-Hellmann-Gruppen diejenigen aus, die Sie verwenden wollen. › DH Group 02 (modp1024) (veraltet) › DH Group 05 (modp1536) (veraltet) › DH Group 14 (modp2048) › DH Group 15 (modp3072) › DH Group 16 (modp4096) › DH Group 17 (modp6144) › DH Group 18 (modp8192) › DH Group 19 NIST Elliptic Curve (ecp256) › DH Group 20 NIST Elliptic Curve (ecp384) › DH Group 21 NIST Elliptic Curve (ecp521) › DH Group 25 NIST Elliptic Curve (ecp192) (veraltet) › DH Group 26 NIST Elliptic Curve (ecp224) › DH Group 27 Brainpool Ellipcic Curve (ecp224bp) › DH Group 28 Brainpool Ellipcic Curve (ecp256bp) › DH Group 29 Brainpool Ellipcic Curve (ecp384bp) › DH Group 30 Brainpool Ellipcic Curve (ecp512bp) › DH Group 31 Ellipcic Curve 25519 (x25519)
SA-Lebensdauer	Geben Sie die gewünschte SA-Lebensdauer in Sekunden an.
Mobile IKE (nur IKEv2)	Diese nur für IKEv2 verfügbare Option erlaubt das Wechseln der IP-Adressen ohne Verbindungsabbruch.

Die Verschlüsselungsalgorithmen, Authentifizierungsalgorithmen und DH-Gruppen, die hier definier werden, werden beim Aufbau der IPsec-Verbindung verwendet, um eine Verschlüsselungs-Authentifizierungs-Kombination mit der Gegenstelle auszuhandeln. Je mehr Einträge hier definiert werden, desto höher sind die Kombinationsmöglichkeiten.

Die Anzahl der Kombinationsmöglichkeiten ist bei Verwendung von IKEv1 auf etwas über 200 begrenzt. Bei IKEv2 gibt es keine Beschränkung.

IPsec (ESP)

Encapsulating Security Payload (ESP) stellt Mechanismen zur Sicherstellung der Authentizität, Integrität und Vertraulichkeit der übertragenen IP-Pakete bereit. Diese Einstellungen bestimmen somit die Verschlüsselungs- und Authentifizierungsalgorithmen der eigentlichen IP-Pakete.

Tabelle 12: IPsec (ESP)

Eingabefeld	Beschreibung
Verschlüsselungsalgorithmen	Wählen Sie aus der Liste der verfügbaren Verschlüsselungsalgorithmen diejenigen aus, die Sie verwenden wollen. › 3DES-EDE-CBC 168 bit (3des) (veraltet) › AES-CBC 128 bit (aes128) › AES-CBC 192 bit (aes192) › AES-CBC 256 bit (aes256) › AES-CCM 128 bit with 64 bit ICV (aes128ccm8) › AES-CCM 128 bit with 96 bit ICV (aes128ccm12) › AES-CCM 128 bit with 128 bit ICV (aes128ccm16) › AES-CCM 192 bit with 64 bit ICV (aes192ccm8) › AES-CCM 192 bit with 96 bit ICV (aes192ccm12) › AES-CCM 192 bit with 128 bit ICV (aes192ccm16) › AES-CCM 256 bit with 64 bit ICV (aes256ccm8) › AES-CCM 256 bit with 96 bit ICV (aes256ccm12) › AES-CCM 256 bit with 128 bit ICV (aes256ccm16) › AES-COUNTER 128 bit (aes128ctr) › AES-COUNTER 192 bit (aes192ctr) › AES-COUNTER 256 bit (aes256ctr) › AES-GCM 128 bit with 64 bit ICV (aes128gcm8) › AES-GCM 128 bit with 96 bit ICV (aes128gcm12) › AES-GCM 128 bit with 128 bit ICV (aes128gcm16) › AES-GCM 192 bit with 64 bit ICV (aes192gcm8) › AES-GCM 192 bit with 96 bit ICV (aes192gcm12) › AES-GCM 192 bit with 128 bit ICV (aes192gcm16) › AES-GCM 256 bit with 64 bit ICV (aes256gcm8) › AES-GCM 256 bit with 96 bit ICV (aes256gcm12) › AES-GCM 256 bit with 128 bit ICV (aes256gcm16) › Blowfish-CBC 128 bit (blowfish128) (veraltet) › Blowfish-CBC 192 bit (blowfish192) (veraltet) › Blowfish-CBC 256 bit (blowfish256) (veraltet) › Camellia-CBC 128 bit (camellia128) › Camellia-CBC 192 bit (camellia192) › Camellia-CBC 256 bit (camellia256) › CAST-CBC 128 bit (cast128) (veraltet) › ChaCha20/Poly1305 256 bit with 128 bit ICV (chacha20poly1305) › Serpent-CBC 128 bit (serpent128) › Serpent-CBC 192 bit (serpent192) › Serpent-CBC 256 bit (serpent256)

Eingabefeld	Beschreibung
	› Twofish-CBC 128 bit (twofish128) › Twofish-CBC 192 bit (twofish192) › Twofish-CBC 256 bit (twofish256)
Authentifizierungsalgorithmen	Wählen Sie aus der Liste der verfügbaren Authentifizierungsalgorithmen diejenigen aus, die Sie verwenden wollen. › AES XCBC 96 bit (aesxcbc) › MD5 HMAC 96 bit (md5) › MD5 HMAC 128 bit (md5_128) › SHA1 HMAC 96 bit (sha1) › SHA1 HMAC 160 bit (sha1_160) › SHA2_256 HMAC 128 bit (sha2_256) › SHA2_384 HMAC 192 bit (sha2_384) › SHA2_512 HMAC 256 bit (sha2_512)
DH-Gruppen	Wählen Sie aus der Liste der verfügbaren Diffie-Hellmann-Gruppen diejenigen aus, die Sie verwenden wollen. › DH Group 02 (modp1024) (veraltet) › DH Group 05 (modp1536) (veraltet) › DH Group 14 (modp2048) › DH Group 15 (modp3072) › DH Group 16 (modp4096) › DH Group 17 (modp6144) › DH Group 18 (modp8192) › DH Group 19 NIST Elliptic Curve (ecp256) › DH Group 20 NIST Elliptic Curve (ecp384) › DH Group 21 NIST Elliptic Curve (ecp521) › DH Group 25 NIST Elliptic Curve (ecp192) (veraltet) › DH Group 26 NIST Elliptic Curve (ecp224) › DH Group 27 Brainpool Ellipcic Curve (ecp224bp) › DH Group 28 Brainpool Ellipcic Curve (ecp256bp) › DH Group 29 Brainpool Ellipcic Curve (ecp384bp) › DH Group 30 Brainpool Ellipcic Curve (ecp512bp) › DH Group 31 Ellipcic Curve 25519 (x25519)
SA-Lebensdauer	Geben Sie die gewünschte SA-Lebensdauer in Sekunden an.

Klicken Sie auf **Erstellen**.

Der Dialog **Sicherheits-Profil** schließt sich. Das neue Sicherheits-Profil wird zur Liste der verfügbaren Sicherheits-Profile in der Objektleiste hinzugefügt.

3.4.7.1.3 Virtuelle IP-Pools

Virtuelle IP-Pools können verwendet werden, um verbundenen Clients IP-Adressen-Konfigurationen zu schicken. Die virtuellen IP-Pools können in den Vorlagen und Verbindungen unter dem Tab **Tunnel** ausgewählt werden.

Unter **VPN** > **IPsec** > **Virtuelle IP-Pools** finden Sie zum einen die vordefinierten und nicht veränderbaren virtuellen IP-Pools für DHCP- und RADIUS-Server, zum anderen den **Default Virtual-IP pool**, den Sie bearbeiten können. Alternativ klicken Sie auf ⊕, um einen neuen virtuellen IP-Pool hinzuzufügen.

Die vordefinierten Profile können weder bearbeitet noch gelöscht werden.

Tabelle 13: Virtueller IP-Pool

Eingabefeld	Beschreibung
Name	Geben Sie diesem virtuellem IP-Pool einen aussagekräftigen Namen.
Verwendet in	Zeigt an, in welchen IPsec-Verbindungen dieser virtuelle IP-Pool aktuell verwendet wird.
IP-Pool	Netzwerk-Adresse, aus der IP-Adressen an die Clients geschickt werden.
Bevorzugter DNS-Server	IP-Adresse des bevorzugten DNS-Servers.
Alternativer DNS-Server	IP-Adresse des alternativen DNS-Servers.
Bevorzugter WINS-Server	IP-Adresse des bevorzugten WINS-Servers.
Alternativer WINS-Server	IP-Adresse des alternativen WINS-Servers.
DNS-Suchdomänen	Liste an DNS-Suchdomänen. Klicken Sie rechts auf ⊕, um Ihren Eintrag zur Liste der DNS-Suchdomänen hinzuzufügen.

Klicken Sie auf **Erstellen**.

Der Dialog **Virtueller IP-Pool** schließt sich. Der neue Pool wird zur Liste der verfügbaren virtuellen IP-Pools in der Objektleiste hinzugefügt.

Werden verwendete IP-Pools geändert, können in der erweiterten Listbar alle zugehörigen Verbindungen neu gestartet werden.

3.4.7.1.4 Vorlagen

Die Verbindungs-Vorlagen können verwendet werden, um Werte für Verbindungen vorzudefinieren, die häufig verwendet werden. Alle Werte außer dem Vorlagen-Namen sind optional und füllen das entsprechende Feld einer auf Basis dieser Vorlage erstellten VPN-Verbindung aus.

Es sind verschiedene Vorlagen vordefiniert, wie z. B. die Vorlage „LANCOM Advanced VPN Client“, um IPsec-Verbindungen mit diesem Client zu vereinfachen. Die Vorlage „(empty)“ kann verwendet werden, falls die Werte einer vorhandenen Verbindungen gelöscht werden sollen.

Die vordefinierten Vorlagen können weder bearbeitet noch gelöscht werden.

Unter **VPN** > **IPsec** > **Vorlagen** können Sie das Fenster **IPsec Verbindugs-Vorlage** öffnen. Im Fenster **IPsec Verbindungs-Vorlage** können Sie die folgenden Informationen einsehen und konfigurieren:

Tabelle 14: IPsec Verbindungs-Vorlage

Eingabefeld	Beschreibung
Name	Geben Sie dieser Vorlage einen aussagekräftigen Namen.
Sicherheits-Profil	Wählen Sie eines der vordefinierten Sicherheitsprofile aus.

Im Tab **Verbindung** können Sie Vorgaben für die folgenden Felder einstellen:

Tabelle 15: Verbindung

Eingabefeld	Beschreibung
Verbindung	Eine Netzwerk- oder Internet-Verbindung kann gewählt werden, deren IP-Adressen für die IPsec-Verbindung verwendet werden soll.
Listening-IP-Adressem	Alternativ zur **Verbindung** können auch benutzerdefinierte IP-Adressen eingetragen werden. Sind hier IP-Adressen gesetzt, so wird die Einstellung **Verbindung** ignoriert. Werden weder **Verbindung** noch **Listening-IP-Adressen** gesetzt, dann verwendet der IPsec-Dienst automatisch eine der konfigurierten IP-Adressen aller Verbindungen.
Remote Gateways	Diese Adresse bzw. Liste von Adressen ist für die Option **Verbindung aufbauen** notwendig, um die Adresse der Gegenstelle zu bestimmen.
Verbindung aufbauen	Von der Firewall wird eine Verbindung zur im Feld **Remote Gateway** angegebenen Adresse aufgebaut.
NAT-T erzwingen	Normalerweise wird NAT-T automatisch gesetzt, wenn die Verbindung es erfordert. Wenn dieser Automatismus nicht greift, dann kann über diese Option NAT-T für den Aufbau einer Verbindung erzwungen werden.

Im Tab **Tunnel** können Sie Vorgaben für die folgenden Felder einstellen:

Tabelle 16: Tunnel

Eingabefeld	Beschreibung
Lokale Netzwerke	Lokale Netzwerke, die mit der Gegenstelle verbunden werden sollen.
Remote Netzwerke	Remote-Netzwerke, die mit den lokalen Netzwerken verbunden werden sollen. Es werden alle konfigurierten lokalen mit allen konfigurierten entfernten (Remote) Netzwerken verbunden. Bei IKEv1-Verbindungen und IKEv2-Verbindungen mit aktivierter Option **IKEv2-Kompatibilitätsmodus** ist die maximale Anzahl an Kombinationen auf 25 begrenzt, bei IKEv2 mit inaktiver Option **IKEv2-Kompatibilitätsmodus** gibt es keine Begrenzung.
Virtueller IP-Pool	Der Gegenstelle wird eine IP-Adresse aus dem konfigurierten IP-Pool zugewiesen.
IKEv2-Kompatibilitätsmodus	Anstatt alle konfigurierten lokalen und entfernten Netze durch einen einzigen Tunnel zu schicken wird wie bei IKEv1 für jede Verbindung zwischen zwei Netzen ein einzelner Tunnel angelegt. Diese Option ist nur für IKEv2-Verbindungen gültig.

Im Tab **Authentifizierung** können Sie Vorgaben für die folgenden Felder einstellen:

Tabelle 17: Authentifizierung

Eingabefeld	Beschreibung
Authentifizierungstyp	Geben Sie den Authentifizierungstyp an. Mögliche Werte: › Zertifikat – die Authentifizierung wird über ein lokales und ein Remote-Zertifikat durchgeführt. › Certificate Authority – die Authentifizierung wird über ein lokales und ein Remote-Zertifikat durchgeführt, das von der ausgewählten CA signiert wurde. › PSK (Preshared Key) – die Authentizierung erfolgt über ein Passwort. › LTA – bei dem Modus LANCOM Trusted Access wird immer ein Clientzertifikat erwartet und aus diesem Clientzertifikat werden die Gruppen des sich verbindenden Benutzers gelesen, um die dazu passenden Regeln zu aktivieren.
PSK (Preshared Key)	Nur bei Authentifizierungstyp PSK (Preshared Key) – Geben Sie das zu verwendende Passwort an.

Eingabefeld	Beschreibung
Lokales Zertifikat	Das Zertifikat der Firewall zur Authentifizierung. Dieses muss einen Private Key beinhalten.
Lokaler Identifier	Ist diese Feld leer, wird bei PSK-Authentifizierung automatisch die ausgehende IP-Adresse der Firewall verwendet und bei Zertifikat-Authentifizierung der Distinguished Name (DN) des ausgewählten lokalen Zertifikats. › Bei PSK-Authentifizierung sind die folgenden Werte erlaubt: IP-Adressen, Fully Qualified Domain Names (FQDN), E-Mail Adressen (FQUN) und freier Text zwischen Anführungszeichen ("). › Bei Zertifikat-Authentifizierung sind die folgenden Werte erlaubt: Den Distinguished Name (DN) des ausgewählten Zertifikats, Wildcard DN – Alle DN Elemente müssen (in korrekter Reihenfolge) vorhanden sein, dürfen aber als Wildcard (z.B. CN=*) angegeben werden – eventuelle Subject Alternative Names (SAN) des ausgewählten Zertifikats.
Erweiterte Authentifizierung	Aktiviert die optionale Verwendung einer zusätzlichen Benutzer-Authentifizierung. Sobald Sie ein Sicherheitsprofil ausgewählt haben, stehen Ihnen die folgenden Optionen zur Verfügung: › **Keine erweiterte Authentifizierung** – Keine erweiterte Authentifizierung durchführen. › **XAUTH (IKEv1)** – Es wird entweder die lokale Benutzerdatenbank oder ein RADIUS-Server verwendet (je nachdem, ob in den IPSec-Einstellungen RADIUS aktiv ist oder nicht). › **EAP First Round** – Es wird ein externer RADIUS-Server verwendet, der in den IPSec-Einstellungen aktiviert sein muss. Die Konfiguration für den RADIUS-Server wird in den IPSec-Einstellungen vorgenommen. Die Einstellungen im Bereich **Lokal** dienen zur Authentifizierung der Firewall bei der Gegenstelle. Die Gegenstelle authentifiziert sich lediglich per EAP. › **EAP Second Round** – Es wird ein externer RADIUS-Server verwendet, der in den IPSec-Einstellungen aktiviert sein muss. Die Konfiguration für den RADIUS-Server wird in den IPSec-Einstellungen vorgenommen. Die Einstellungen im Bereich **Lokal** dienen zur Authentifizierung der Firewall bei der Gegenstelle. Die Gegenstelle authentifiziert sich mit dem PSK oder einem Zertifikat bei der Firewall und führt danach eine EAP-Authentifizierung durch. › **EAP-TLS** – Entspricht der Variante **EAP First Round** mit dem Unterschied, dass ein TLS-Zertifikat zur EAP-Authentifizierung verwendet wird. ⓘ › Bei IKEv1 stehen unabhängig vom Authentifizierungstyp die Optionen **Keine erweiterte Authentifizierung** und **XAUTH (IKEv1)** zur Verfügung. › Bei IKEv2 mit Zertifikats- bzw. PSK-Authentifizierung stehen mit Ausnahme von **XAUTH (IKEv1)** alle Optionen zur Verfügung. › Bei IKEv2 mit CA-Authentifizierung stehen die Optionen **Keine erweiterte Authentifizierung** und **EAP Second Round** zur Verfügung.
Remote Zertifikat	Nur bei Authentifizierungstyp „Zertifikat": Zertifikat der Gegenstelle.
Certificate Authority	Nur bei Authentifizierungstyp „Certificate Authority": Eine CA, deren signierte Zertifikate für die Authentifizierung verwendet werden können.
Remote Identifier	Ist diese Feld leer, wird bei PSK-Authentifizierung automatisch die IP-Adresse des Remote Gateways verwendet, falls diese gesetzt wurde. Bei Zertifikat-Authentifizierung der Distinguished Name (DN) des ausgewählten remote Zertifikats. › Bei PSK-Authentifizierung sind die folgenden Werte erlaubt: IP-Adressen, Fully Qualified Domain Names (FQDN), E-Mail Adressen (FQUN) und freier Text zwischen Anführungszeichen ("). › Bei Zertifikat-Authentifizierung sind die folgenden Werte erlaubt: Den Distinguished Name (DN) des ausgewählten Zertifikats, Wildcard DN – Alle DN Elemente müssen (in korrekter Reihenfolge) vorhanden sein, dürfen aber als Wildcard (z.B. CN=*) angegeben werden – eventuelle Subject Alternative Names (SAN) des ausgewählten Zertifikats.

Im Tab **Routing** können Sie die folgenden Felder konfigurieren:

Tabelle 18: Routing

Eingabefeld	Beschreibung
Routen-basiertes IPsec	Diese Option erlaubt es, bei Aktivierung durch das ausschließlich manuelle Festlegen von Routing-Regeln und Routing-Tabellen (bzw. deren Einträgen), genau festzulegen, welcher Datenverkehr durch einen Tunnel geleitet werden soll. Das ist insbesondere dann hilfreich, wenn in der Verbindung verwendete Netze (lokale Netze oder remote Netze) sich auf unerwünschte Art mit weiteren auf dem Gerät definierten Netzen überschneiden. In den Dialogen zur Routing-Konfiguration (Routing-Regeln und -Tabellen) können an den Stellen, wo Quell- / Ziel-Interfaces ausgewählt werden können, nach Aktivierung dieser Option auch diejenigen IPSec-Verbindungen ausgewählt werden, für die **Routen-basiertes IPsec** aktiviert wurde. Zur einfacheren Unterscheidung von anderen Interfaces sind diese mit einem Vorhängeschloss markiert.
MTU	Hier können Sie die MTU (Maximum Transmission Unit), also die maximale Größe eines unfragmentierten Datenpakets einstellen. Standardmäßig liegt sie bei 1400.

Im Tab **Traffic-Shaping** können Sie die folgenden Felder konfigurieren:

Eingabefeld	Beschreibung
Traffic-Gruppe	Wählen Sie optional den Namen einer Traffic-Gruppe aus. Dadurch werden die für diese Gruppe definierten Regeln für den Datenverkehr auf dieser Verbindung angewendet. Siehe auch *Traffic Shaping* auf Seite 105. Falls es sich um einen Routen-basierten IPsec-Tunnel handelt, kann der Datenverkehr innerhalb eines Tunnels mit Hilfe einer eigenen Shaping-Konfiguration priorisiert werden.
DSCP ausgehend	Wählen Sie einen optionalen DSCP-Wert für ausgehenden Datenverkehr aus der Liste aus. Die Liste enthält die Bezeichnungen aus den relevanten RFCs (z. B. „CS0“) und der Gruppe (z. B. „Standard“). Zusätzlich wird der Wert ebenfalls in seiner numerischen Repräsentation zu verschiedenen Basen (binär, hexadezimal und dezimal) angezeigt. Die Liste kann entsprechend dieser Darstellungen durchsucht werden, so dass Sie unabhängig von der individuell bevorzugten Darstellung schnell den gewünschten Wert finden.

Klicken Sie auf **Erstellen**.

Der Dialog **IPsec Verbindugs-Vorlage** schließt sich. Die neue Vorlage wird zur Liste der verfügbaren Vorlagen in der Objektleiste hinzugefügt.

3.4.7.1.5 IPsec-Verbindungen

Mit Ihrer LANCOM R&S®Unified Firewall können Sie Remote-Clients über IPsec (IPsec Client-to-Site) VPN-Zugang verschaffen und einen sicheren Tunnel zwischen zwei Remote-Netzwerken erstellen (IPsec Site-to-Site).

Übersicht IPSec-Verbindungen

Navigieren Sie zu **VPN** > **IPsec** > **Verbindungen**, um die Liste der derzeit im System angelegten IPSec-Verbindungen in der Objektleiste anzuzeigen.

In der erweiterten Ansicht wird in den Tabellenspalten der **Name** und der **Status** der IPSec-Verbindung angezeigt. Des Weiteren zeigen die Spalten die für diese Verbindung gewählte Authentifizierungsmethode an. Mit den Schaltflächen in der letzten Spalte können Sie die Einstellungen für eine IPsec-Verbindung einsehen und anpassen oder eine Verbindung aus dem System löschen.

Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28.

IPsec-Verbindungs-Einstellungen

Unter **VPN** > **IPsec** > **Verbindungen** können Sie eine IPsec-Verbindung hinzufügen, oder eine vorhandene Verbindung bearbeiten.

Im Bearbeitungsfenster **Verbindung** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
I/0	Ein Schiebeschalter gibt an, ob die IPSec-Verbindung derzeit aktiv (**I**) oder inaktiv (**0**) ist. Mit einem Klick auf den Schiebeschalter können Sie den Status der Verbindung ändern. Eine neue Verbindung ist standardmäßig aktiviert.
Name	Geben Sie einen eindeutigen Namen für die Verbindung ein. Dieser muss aus einem bis 63 alphanumerischen Zeichen und Unterstrichen bestehen. Im Namen dürfen keine Umlaute verwendet werden.
Vorlage	Wählen Sie optional eine der vordefinierten Vorlagen aus. Alle Einstellungen werden entsprechend der gesetzten Werte aus der Vorlage verwendet. Werte die nicht in der Vorlage gesetzt wurden, werden zurückgesetzt. Daher kann die Vorlage „(empty)“ verwendet werden, um alle Werte zurückzusetzen.
Sicherheits-Profil	Wählen Sie eines der vordefinierten Sicherheitsprofile aus.

Im Tab **Verbindung** können Sie die folgenden Felder konfigurieren:

Tabelle 19: Verbindung

Eingabefeld	Beschreibung
Verbindung	Eine Netzwerk- oder Internet-Verbindung kann gewählt werden, deren IP-Adressen für die IPsec-Verbindung verwendet werden soll. Hier sind sowohl IPv4- als auch IPv6-Verbindungen möglich. Ist keine Verbindung ausgewählt, können unter **Listening-IP-Adressem** und **Remote Gateways** sowohl IPv4- als auch IPv6-Adressen gewählt werden. Anderfalls müssen diese dem Verbindungstypen entsprechen.
Listening-IP-Adressem	Alternativ zur **Verbindung** können auch benutzerdefinierte IP-Adressen eingetragen werden. Klicken Sie rechts auf ⊕, um Ihren Eintrag zur Liste hinzuzufügen. Sind hier IP-Adressen gesetzt, so wird die Einstellung **Verbindung** ignoriert. Werden weder **Verbindung** noch **Listening-IP-Adressen** gesetzt, dann verwendet der IPsec-Dienst automatisch eine der konfigurierten IP-Adressen aller Verbindungen.
Remote Gateways	Diese Adresse bzw. Liste von Adressen ist für die Option **Verbindung aufbauen** notwendig, um die Adresse der Gegenstelle zu bestimmen.
Verbindung aufbauen	Von der Firewall wird eine Verbindung zur im Feld **Remote Gateway** angegebenen Adresse aufgebaut.
NAT-T erzwingen	Normalerweise wird NAT-T automatisch gesetzt, wenn die Verbindung es erfordert. Wenn dieser Automatismus nicht greift, dann kann über diese Option NAT-T für den Aufbau einer Verbindung erzwungen werden.

Im Tab **Tunnel** können Sie die folgenden Felder konfigurieren:

Unter dem Tab **Tunnel** können nur IPv4-Werte, keine IPv6-Werte, verwendet werden.

Tabelle 20: Tunnel

Eingabefeld	Beschreibung
Lokale Netzwerke	Lokale Netzwerke, die mit der Gegenstelle verbunden werden sollen. Klicken Sie rechts auf ⊕, um Ihren Eintrag zur Liste hinzuzufügen.
Remote Netzwerke	Remote-Netzwerke, die mit den lokalen Netzwerken verbunden werden sollen. Klicken Sie rechts auf ⊕, um Ihren Eintrag zur Liste hinzuzufügen. Es werden alle konfigurierten lokalen mit allen konfigurierten entfernten (Remote) Netzwerken verbunden. Bei IKEv1-Verbindungen und IKEv2-Verbindungen mit aktivierter Option **IKEv2-Kompatibilitätsmodus** ist die maximale Anzahl an Kombinationen auf 25 begrenzt, bei IKEv2 mit inaktiver Option **IKEv2-Kompatibilitätsmodus** gibt es keine Begrenzung.
Virtueller IP-Pool	Der Gegenstelle wird eine IP-Adresse aus dem konfigurierten IP-Pool zugewiesen.
Virtuelle IP	Weisen Sie der Gegenstelle eine bestimmte IP-Adresse zu. Die Optionen **Remote-Netzwerke**, **Virtueller IP-Pool** und **Virtuelle IP** sollten nicht zusammen verwendet werden
IKEv2-Kompatibilitätsmodus	Anstatt alle konfigurierten lokalen und entfernten Netze durch einen einzigen Tunnel zu schicken wird wie bei IKEv1 für jede Verbindung zwischen zwei Netzen ein einzelner Tunnel angelegt. Diese Option ist nur für IKEv2-Verbindungen gültig.

Im Tab **Authentifizierung** können Sie die folgenden Felder konfigurieren:

Tabelle 21: Authentifizierung

Eingabefeld	Beschreibung
Authentifizierungstyp	Geben Sie den Authentifizierungstyp an. Mögliche Werte: › Zertifikat – die Authentifizierung wird über ein lokales und ein Remote-Zertifikat durchgeführt. › Certificate Authority – die Authentifizierung wird über ein lokales und ein Remote-Zertifikat durchgeführt, das von der ausgewählten CA signiert wurde. › PSK (Preshared Key) – die Authentizierung erfolgt über ein Passwort. › LTA – bei dem Modus LANCOM Trusted Access wird immer ein Clientzertifikat erwartet und aus diesem Clientzertifikat werden die Gruppen des sich verbindenden Benutzers gelesen, um die dazu passenden Regeln zu aktivieren.
PSK (Preshared Key)	Nur bei Authentifizierungstyp PSK (Preshared Key) – Geben Sie das zu verwendende Passwort an.
Lokales Zertifikat	Das Zertifikat der Firewall zur Authentifizierung. Dieses muss einen Private Key beinhalten.
Lokaler Identifier	Ist dieses Feld leer, wird bei PSK-Authentifizierung automatisch die ausgehende IP-Adresse der Firewall verwendet und bei Zertifikat-Authentifizierung der Distinguished Name (DN) des ausgewählten lokalen Zertifikats. › Bei PSK-Authentifizierung sind die folgenden Werte erlaubt: IP-Adressen, Fully Qualified Domain Names (FQDN), E-Mail Adressen (FQUN) und freier Text zwischen Anführungszeichen ("). › Bei Zertifikat-Authentifizierung sind die folgenden Werte erlaubt: Den Distinguished Name (DN) des ausgewählten Zertifikats, Wildcard DN – Alle DN Elemente müssen (in korrekter Reihenfolge) vorhanden sein, dürfen aber als Wildcard (z.B. CN=*) angegeben werden – eventuelle Subject Alternative Names (SAN) des ausgewählten Zertifikats.
Erweiterte Authentifizierung	Aktiviert die optionale Verwendung einer zusätzlichen Benutzer-Authentifizierung. Sobald Sie ein Sicherheitsprofil ausgewählt haben, stehen Ihnen die folgenden Optionen zur Verfügung:

Eingabefeld	Beschreibung
	› **Keine erweiterte Authentifizierung** – Keine erweiterte Authentifizierung durchführen. › **XAUTH (IKEv1)** – Es wird entweder die lokale Benutzerdatenbank oder ein RADIUS-Server verwendet (je nachdem, ob in den IPSec-Einstellungen RADIUS aktiv ist oder nicht). › **EAP First Round** – Es wird ein externer RADIUS-Server verwendet, der in den IPSec-Einstellungen aktiviert sein muss. Die Konfiguration für den RADIUS-Server wird in den IPSec-Einstellungen vorgenommen. Die Einstellungen im Bereich **Lokal** dienen zur Authentifizierung der Firewall bei der Gegenstelle. Die Gegenstelle authentifiziert sich lediglich per EAP. › **EAP Second Round** – Es wird ein externer RADIUS-Server verwendet, der in den IPSec-Einstellungen aktiviert sein muss. Die Konfiguration für den RADIUS-Server wird in den IPSec-Einstellungen vorgenommen. Die Einstellungen im Bereich **Lokal** dienen zur Authentifizierung der Firewall bei der Gegenstelle. Die Gegenstelle authentifiziert sich mit dem PSK oder einem Zertifikat bei der Firewall und führt danach eine EAP-Authentifizierung durch. › **EAP-TLS** – Entspricht der Variante **EAP First Round** mit dem Unterschied, dass ein TLS-Zertifikat zur EAP-Authentifizierung verwendet wird. ⓘ › Bei IKEv1 stehen unabhängig vom Authentifizierungstyp die Optionen **Keine erweiterte Authentifizierung** und **XAUTH (IKEv1)** zur Verfügung. › Bei IKEv2 mit Zertifikats- bzw. PSK-Authentifizierung stehen mit Ausnahme von **XAUTH (IKEv1)** alle Optionen zur Verfügung. › Bei IKEv2 mit CA-Authentifizierung stehen die Optionen **Keine erweiterte Authentifizierung** und **EAP Second Round** zur Verfügung.
Remote Zertifikat	Nur bei Authentifizierungstyp „Zertifikat“: Zertifikat der Gegenstelle.
Certificate Authority	Nur bei Authentifizierungstyp „Certificate Authority“: Eine CA, deren signierte Zertifikate für die Authentifizierung verwendet werden können.
Remote Identifier	Ist dieses Feld leer, wird bei PSK-Authentifizierung automatisch die IP-Adresse des Remote Gateways verwendet, falls diese gesetzt wurde. Bei Zertifikat-Authentifizierung der Distinguished Name (DN) des ausgewählten remote Zertifikats. › Bei PSK-Authentifizierung sind die folgenden Werte erlaubt: IP-Adressen, Fully Qualified Domain Names (FQDN), E-Mail Adressen (FQUN) und freier Text zwischen Anführungszeichen ("). › Bei Zertifikat-Authentifizierung sind die folgenden Werte erlaubt: Den Distinguished Name (DN) des ausgewählten Zertifikats, Wildcard DN – Alle DN Elemente müssen (in korrekter Reihenfolge) vorhanden sein, dürfen aber als Wildcard (z.B. CN=*) angegeben werden – eventuelle Subject Alternative Names (SAN) des ausgewählten Zertifikats.

Im Tab **Routing** können Sie die folgenden Felder konfigurieren:

Tabelle 22: Routing

Eingabefeld	Beschreibung
Routen-basiertes IPsec	Diese Option erlaubt es, bei Aktivierung durch das ausschließlich manuelle Festlegen von Routing-Regeln und Routing-Tabellen (bzw. deren Einträgen), genau festzulegen, welcher Datenverkehr durch einen Tunnel geleitet werden soll. Das ist insbesondere dann hilfreich, wenn in der Verbindung verwendete Netze (lokale Netze oder remote Netze) sich auf unerwünschte Art mit weiteren auf dem Gerät definierten Netzen überschneiden. In den Dialogen zur Routing-Konfiguration (Routing-Regeln und -Tabellen) können an den Stellen, wo Quell- / Ziel-Interfaces ausgewählt werden können, nach Aktivierung dieser Option auch diejenigen IPSec-Verbindungen ausgewählt werden, für die **Routen-basiertes IPsec**

Eingabefeld	Beschreibung
	aktiviert wurde. Zur einfacheren Unterscheidung von anderen Interfaces sind diese mit einem Vorhängeschloss markiert.
MTU	Hier können Sie die MTU (Maximum Transmission Unit), also die maximale Größe eines unfragmentierten Datenpakets einstellen. Standardmäßig liegt sie bei 1400.

Im Tab **Traffic-Shaping** können Sie die folgenden Felder konfigurieren:

Eingabefeld	Beschreibung
Traffic-Gruppe	Wählen Sie optional den Namen einer Traffic-Gruppe aus. Dadurch werden die für diese Gruppe definierten Regeln für den Datenverkehr auf dieser Verbindung angewendet. Siehe auch *Traffic Shaping* auf Seite 105. Falls es sich um einen Routen-basierten IPsec-Tunnel handelt, kann der Datenverkehr innerhalb eines Tunnels mit Hilfe einer eigenen Shaping-Konfiguration priorisiert werden.
DSCP ausgehend	Wählen Sie einen optionalen DSCP-Wert für ausgehenden Datenverkehr aus der Liste aus. Die Liste enthält die Bezeichnungen aus den relevanten RFCs (z. B. „CS0“) und der Gruppe (z. B. „Standard“). Zusätzlich wird der Wert ebenfalls in seiner numerischen Repräsentation zu verschiedenen Basen (binär, hexadezimal und dezimal) angezeigt. Die Liste kann entsprechend dieser Darstellungen durchsucht werden, so dass Sie unabhängig von der individuell bevorzugten Darstellung schnell den gewünschten Wert finden.

Die Schaltflächen rechts unten im Bearbeitungsfeld hängen davon ab, ob Sie eine neue VPN-IPsec-Verbindung hinzufügen oder eine bestehende Verbindung bearbeiten. Klicken Sie für eine neu konfigurierte Netzwerkverbindung auf **Erstellen**, um die Verbindung zur Liste der verfügbaren IPSec-Netzwerkverbindungen hinzuzufügen, oder auf **Abbrechen**, um die Erstellung einer neuen Netzwerkverbindung abzubrechen.

Wenn Sie Änderungen vorgenommen haben, können Sie diese mit den Schaltflächen unten rechts im Bearbeitungsfenster speichern (**Speichern**) oder verwerfen (**Zurücksetzen**). Andernfalls können Sie das Fenster schließen (**Schließen**).

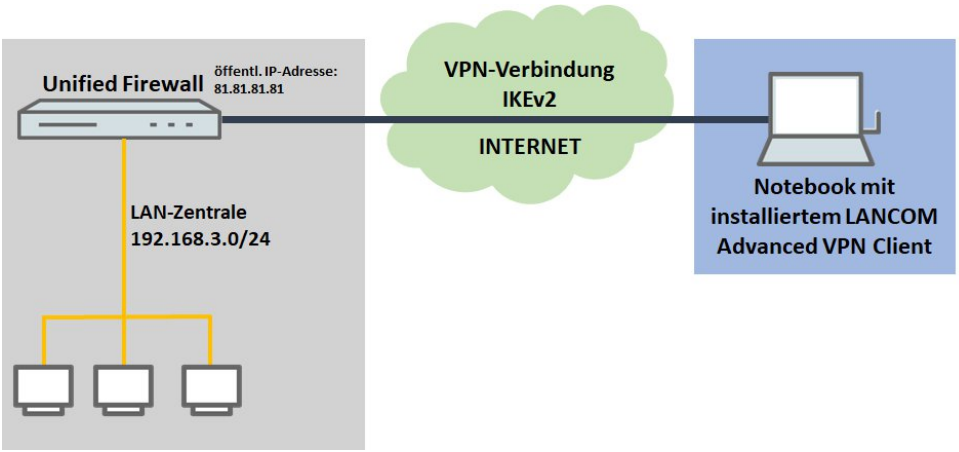
Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

Einrichtung einer IKEv2 VPN-Verbindung mit dem LANCOM Advanced VPN-Client

Szenario: Die LANCOM R&S®Unified Firewall ist direkt mit dem Internet verbunden und verfügt über eine öffentliche IPv4-Adresse:

- Ein Unternehmen möchte seinen Außendienst-Mitarbeitern den Zugriff auf das Firmennetzwerk per IKEv2 Client-To-Site Verbindung ermöglichen.
- Dazu ist auf den Notebooks der Außendienst-Mitarbeiter der LANCOM Advanced VPN Client installiert.
- Die Firmenzentrale verfügt über eine LANCOM R&S®Unified Firewall als Gateway und eine Internetverbindung mit der festen öffentlichen IP-Adresse 81.81.81.81.

› Das lokale Netzwerk der Zentrale hat den IP-Adressbereich 192.168.3.0/24.



Neben anderen Szenarien ist dieses eines der in der *LANCOM Support Knowledge Base* erläuterten Szenarien. Über den folgenden Link finden Sie eine Schritt-für-Schritt-Anleitung:

https://knowledgebase.lancom-systems.de/pages/viewpage.action?pageId=37454451

3.4.7.2 VPN-SSL

VPN über SSL bietet eine schnelle und sichere Möglichkeit, eine Roadwarrior-Verbindung einzurichten. Der größte Vorteil von VPN-SSL ist, dass der gesamte Datenverkehr über einen TCP- oder UDP-Port läuft und keine weiteren speziellen Protokolle benötigt werden.

Ihre LANCOM R&S®Unified Firewall ermöglicht es Ihnen, Remote-Clientcomputern einen VPN-Zugang zu gewähren (C2S, „Client-to-Site"), eine sichere Verbindung zwischen zwei Remote-Netzwerken (S2S, „Site-to-Site") oder eine Bridge-Verbindung über das VPN-SSL-Protokoll herzustellen.

3.4.7.2.1 VPN-SSL-Einstellungen

Unter **VPN** > **VPN-SSL** > **VPN-SSL-Einstellungen** können Sie VPN-SSL aktivieren und die allgemeinen Einstellungen dazu konfigurieren:

Eingabefeld	Beschreibung
I/0	Ein Schiebeschalter gibt an, ob VPN-SSL aktiv (**I**) oder inaktiv (**0**) ist. Mit einem Klick auf den Schiebeschalter ändern Sie den Status dieser Option.
Host-Zertifikat	Wählen Sie ein Hostzertifikat aus, das Ihre LANCOM R&S®Unified Firewall für alle VPN-SSL-Verbindungen nutzt.
DNS	Optional: Geben Sie einen DNS-Server ein, der von Clients für Client-to-Site-Verbindungen verwendet werden soll, während die Verbindung besteht.
WINS	Optional: Geben Sie einen WINS-Server ein, der von Clients für Client-to-Site-Verbindungen verwendet werden soll, während die Verbindung besteht.
Timeout	Geben Sie die Zeitüberschreitung in Sekunden ein. Der Tunnel wird getrennt, wenn bis zur Zeitüberschreitung kein Datenfluss vorliegt. Die Standardeinstellung beträgt `0`. Der Tunnel wird also permanent aufrechterhalten.
Log-Level	Legen Sie die Ereignisprotokollstufe fest. Für Troubleshooting empfiehlt sich die Ereignisprotokollstufe `5` .
Routen	Geben Sie Routen für die VPN-SSL-Tunnel ein, die von den Clients oder dem entfernten Verbindungsende erstellt werden sollen. Diese Routen werden dann für alle VPN-SSL-Verbindungen verwendet.

Eingabefeld	Beschreibung
	Klicken Sie auf **Hinzufügen**, um die Route zur Liste hinzuzufügen. Sie können einzelne Einträge in der Liste bearbeiten oder löschen, indem Sie auf die entsprechende Schaltfläche neben einem Eintrag klicken. Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28. Wenn Sie einen Eintrag bearbeiten, erscheint auf der rechten Seite des Eintrags ein Haken. Klicken Sie auf den Haken, um Ihre Änderungen zu übernehmen.

Im Tab **Client-to-Site** :

Eingabefeld	Beschreibung
Protokoll	Wählen Sie das zu verwendende Protokoll aus, indem Sie die entsprechende Optionsschaltfläche auswählen. In der Standard-Einstellung ist **UDP** ausgewählt.
Port	Geben Sie die Nummer des VPN-SSL Listening Port an, der für eingehende Verbindungen verwendet werden soll. Die gleiche Port-Nummer muss auch in der Client-Software angegeben werden.
Adressbereich	Geben Sie den Adressbereich an, aus dem IP-Adressen an Clients vergeben werden. Der Adressbereich darf sich nicht mit Ihren lokalen Netzwerken überschneiden.
Verschlüsselungs-Algorithmus	Wählen Sie aus der Drop-down-Liste den Verschlüsselungsalgorithmus aus, der für C2S-Verbindungen über VPN-SSL verwendet werden soll. Die folgenden Verschlüsselungsalgorithmen können ausgewählt werden: › AES 128 (Standard-Einstellung) › AES 192 › AES 256 › 3DES › Blowfish › Cast5
Erneute Verhandlung des Schlüssels	Um die Sicherheit zu erhöhen, erneuert eine VPN-SSL-Verbindung den Sitzungsschlüssel, während die Verbindung besteht. Geben Sie das Intervall für diese Schlüsselerneuerung in Sekunden an.
Kompression	Optional: Setzen Sie dieses Häkchen, um LZO (Lempel-Ziv-Oberhumer, ein Algorithmus für verlustfreie Datenkompression) zu aktivieren. Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Im Tab **Site-to-Site** :

Eingabefeld	Beschreibung
Protokoll	Wählen Sie das zu verwendende Protokoll aus, indem Sie die entsprechende Optionsschaltfläche auswählen. In der Standard-Einstellung ist **UDP** ausgewählt.
Port	Geben Sie die Nummer des VPN-SSL Listening Port an, der für eingehende Verbindungen verwendet werden soll. Dieselbe Portnummer muss am entfernten Verbindungsende angegeben werden.
Adressbereich	Geben Sie den Adressbereich an, aus dem IP-Adressen für S2S-Verbindungen verwendet werden sollen. Der Adressbereich darf sich nicht mit Ihren lokalen Netzwerken überschneiden.
Verschlüsselungs-Algorithmus	Wählen Sie aus der Drop-down-Liste den Verschlüsselungsalgorithmus aus, der für S2S-Verbindungen über VPN-SSL verwendet werden soll.

Eingabefeld	Beschreibung
	Die folgenden Verschlüsselungsalgorithmen können ausgewählt werden: › AES 128 (Standard-Einstellung) › AES 192 › AES 256 › 3DES › Blowfish › Cast5
Erneute Verhandlung des Schlüssels	Um die Sicherheit zu erhöhen, erneuert eine VPN-SSL-Verbindung den Sitzungsschlüssel, während die Verbindung besteht. Geben Sie das Intervall für diese Schlüsselerneuerung in Sekunden an.
Kompression	Optional: Setzen Sie dieses Häkchen, um LZO (Lempel-Ziv-Oberhumer, ein Algorithmus für verlustfreie Datenkompression) zu aktivieren. Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Im Tab **Bridging** geben Sie die Einstellungen für die VPN SSL Serververbindung an:

Eingabefeld	Beschreibung
Protokoll	Wählen Sie das zu verwendende Protokoll aus, indem Sie die entsprechende Optionsschaltfläche auswählen. In der Standard-Einstellung ist **UDP** ausgewählt.
Port	Geben Sie die Nummer des VPN-SSL Listening Port an, der für Bridging verwendet werden soll. Dieselbe Portnummer muss am entfernten Verbindungsende angegeben werden.
Verschlüsselungs-Algorithmus	Wählen Sie aus der Drop-down-Liste den Verschlüsselungsalgorithmus aus, der für Bridging über VPN-SSL verwendet werden soll. Die folgenden Verschlüsselungsalgorithmen können ausgewählt werden: › AES 128 (Standard-Einstellung) › AES 192 › AES 256 › 3DES › Blowfish › Cast5
Erneute Verhandlung des Schlüssels	Um die Sicherheit zu erhöhen, erneuert eine VPN-SSL-Verbindung den Sitzungsschlüssel, während die Verbindung besteht. Geben Sie das Intervall für diese Schlüsselerneuerung in Sekunden an.
Kompression	Optional: Setzen Sie dieses Häkchen, um LZO (Lempel-Ziv-Oberhumer, ein Algorithmus für verlustfreie Datenkompression) zu aktivieren. Dieses Kontrollkästchen ist standardmäßig deaktiviert.

Wenn Sie Änderungen vorgenommen haben, können Sie diese mit den Schaltflächen unten rechts im Bearbeitungsfenster speichern (**Speichern**) oder verwerfen (**Zurücksetzen**). Andernfalls können Sie das Fenster schließen (**Schließen**).

Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

3.4.7.2.2 VPN-SSL-Verbindungen

Unter **VPN** > **VPN-SSL** > **VPN-SSL-Verbindungen** können Sie VPN-SSL-Verbindungen erstellen und verwalten.

Mit Ihrer LANCOM R&S®Unified Firewall können Sie Remote-Clients über VPN-SSL (Client-to-Site) VPN-Zugang verschaffen und einen sicheren Tunnel zwischen zwei Remote-Netzwerken erstellen (Site-to-Site).

Übersicht VPN-SSL-Verbindungen

Navigieren Sie zu **VPN** > **VPN-SSL** > **VPN-SSL-Verbindungen**, um die Liste der derzeit im System angelegten VPN-SSL-Verbindungen in der Objektleiste anzuzeigen.

In der erweiterten Ansicht wird in den Tabellenspalten der **Name** der VPN-SSL-Verbindung, das für die Verbindung verwendete **Zertifikat** sowie der **Typ** und der **Status** der Verbindung angezeigt. Mit den Schaltflächen in der letzten Spalte können Sie die Einstellungen für eine VPN-SSL-Verbindung einsehen, anpassen, exportieren oder eine Verbindung aus dem System löschen.

Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28.

VPN-SSL-Verbindungseinstellungen

Unter **VPN** > **VPN-SSL** > **VPN-SSL-Verbindungen** können Sie eine VPN-SSL-Verbindung hinzufügen, oder eine vorhandene Verbindung bearbeiten.

Mit den Einstellungen unter **VPN-SSL-Verbindungen** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
I/0	Ein Schiebeschalter gibt an, ob die VPN-SSL-Verbindung derzeit aktiv (**I**) oder inaktiv (**0**) ist. Mit einem Klick auf den Schiebeschalter können Sie den Status der Verbindung ändern. Neu angelegte Verbindungen sind standardmäßig aktiviert.
Name	Geben Sie einen eindeutigen Namen für die Verbindung ein. Der Name muss aus alphanumerischen Zeichen bestehen (erlaubt sind Buchstaben mit Ausnahme von ä, ö, ü und ß sowie Zahlen und Sonderzeichen).
Zertifikat	Wählen Sie das Serverzertifikat für VPN-SSL-Verbindungen aus der Drop-Down-Liste aus. Eine CA und von dieser abgeleitete Zertifikate werden dabei als „Empfohlen“ angezeigt. D.h. mit der Verwendung der CA können nun mehrere Verbindungen exportiert werden, die auf der Firewall nur einmal definiert werden müssen. Dafür kann im Export-Dialog von VPN-SSL-Verbindungen über **Remote-Zertifikat** ein CA-Zertifikat ausgewählt werden. Das VPN-Zertifikat muss an allen Standorten von der gleichen Zertifizierungsstelle (Certificate Authority, CA) signiert werden. Es empfiehlt sich daher, die VPN-Zertifizierungsstelle und die VPN-Zertifikate an einem Standort zu verwalten und die VPN-Zertifikate von dort an alle weiteren Standorte zu exportieren.
Verbindungstyp	Wählen Sie den Typ der Verbindung und die Funktion der LANCOM R&S®Unified Firewall aus, indem Sie die entsprechende Optionsschaltfläche auswählen. Sie können aus den folgenden Typen auswählen: › **Client-to-Site** – Es wird eine C2S-Verbindung hergestellt (z. B. für Full Tunneling). Dieser Verbindungstyp kann z. B. mit dem herkömmlichen OpenVPN-Client verwendet werden, um vor allem mobile Clients mit Ihrem lokalen Netzwerk zu verbinden. › **Site-to-Site (Server)** – Es wird eine S2S-Verbindung hergestellt, bei der Ihre LANCOM R&S®Unified Firewall als Server dient. › **Site-to-Site (Client)** – Es wird eine S2S-Verbindung hergestellt. Ihre LANCOM R&S®Unified Firewall dient als Client. › **Bridge (Server)** – Es wird eine Bridge-Server-Verbindung hergestellt. Es können mehrere Bridge-Server-Verbindungen erstellt werden; alle Verbindungen müssen aber die gleiche Bridge verwenden, so dass z. B. mehrere Standorte zu einem Netz zusammengefasst werden können. Andere Einstellungen werden nicht benötigt. › **Bridge (Client)** – Es wird eine Bridge-Client-Verbindung hergestellt. Sobald eine Verbindung hergestellt wurde, erscheint in der Portliste der verwendeten Bridge ein automatisch erzeugtes TAP-Interface. Dieses TAP-Interface

Eingabefeld	Beschreibung
	kann nicht aus der Bridge entfernt werden, kann aber in Desktop-verbindungen wie normale Interfaces verwendet werden, um damit Regeln zu definieren.

Die angezeigten Elemente in den Einstellungen hängen vom gewählten Verbindungstyp ab:

Bei Client-to-Site-Verbindungen können Sie die folgende Elemente konfigurieren:

Eingabefeld	Beschreibung
Standard Gateway setzen	Setzen Sie den Haken in diesem Kontrollkästchen, um den VPN-SSL-Tunnel als Standard-Route zu verwenden (z. B. für Full Tunneling).
Client IP	Optional: Geben Sie die IP-Adresse ein, unter der der Client erreichbar ist.
Zusätzliche Server-Netzwerke	Die Angabe der lokalen Netzwerke, zu denen der Client Verbindungsrouten erstellen soll, muss in gültiger CIDR-Notation erfolgen (IP-Adresse gefolgt von einem Schrägstrich „/" und der Anzahl der in der Subnetzmaske festgelegten Bits, z. B. `192.168.1.0/24`). Klicken Sie auf **Hinzufügen**, um ein Netzwerk zur Liste hinzuzufügen. Sie können einzelne Einträge in der Liste bearbeiten oder löschen, indem Sie auf die entsprechende Schaltfläche neben einem Eintrag klicken. Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28. Wenn Sie einen Eintrag bearbeiten, erscheint auf der rechten Seite des Eintrags ein Haken. Klicken Sie auf den Haken, um Ihre Änderungen zu übernehmen.

Bei Site-to-Site-Verbindungenn, bei denen Ihre LANCOM R&S®Unified Firewall als Server dient, können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Adressbereich	Geben Sie den Adressbereich an, aus dem IP-Adressen für diese Verbindung verwendet werden. Der Adressbereich ist in den Einstellungen für VPN-SSL angegeben. Weitere Informationen finden Sie unter *VPN-SSL* auf Seite 198.
Remote-IP	Optional: Geben Sie die IP-Adresse des entfernten Verbindungsendes ein.
Fremde Netzwerke	Geben Sie die Netzwerke an, die dem entfernten Verbindungsende zur Verfügung stehen. Nachdem die Verbindung erfolgreich hergestellt wurde, erstellt der Server Routen in diesen Netzwerken. Klicken Sie auf **Hinzufügen**, um ein Netzwerk zur Liste hinzuzufügen. Sie können einzelne Einträge in der Liste bearbeiten oder löschen, indem Sie auf die entsprechende Schaltfläche neben einem Eintrag klicken. Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28. Wenn Sie einen Eintrag bearbeiten, erscheint auf der rechten Seite des Eintrags ein Haken. Klicken Sie auf den Haken, um Ihre Änderungen zu übernehmen.
Zusätzliche eigene Netzwerke	Geben Sie zusätzliche lokale Netzwerke an. Nachdem die Verbindung erfolgreich hergestellt wurde, erstellt der Server Routen in diesen Netzwerken. Klicken Sie auf **Hinzufügen**, um ein Netzwerk zur Liste hinzuzufügen. Sie können einzelne Einträge in der Liste bearbeiten oder löschen, indem Sie auf die entsprechende Schaltfläche neben einem Eintrag klicken. Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28. Wenn Sie einen Eintrag bearbeiten, erscheint auf der rechten Seite des Eintrags ein Haken. Klicken Sie auf den Haken, um Ihre Änderungen zu übernehmen.

Bei Site-to-Site-Verbindungen, bei denen Ihre LANCOM R&S®Unified Firewall als Client dient, können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Adressbereich	Geben Sie den Adressbereich an, aus dem IP-Adressen für diese Verbindung verwendet werden. Der Adressbereich ist in den Einstellungen für VPN-SSL angegeben. Weitere Informationen finden Sie unter *VPN-SSL* auf Seite 198.
Remote-Adressen	Geben Sie die IP-Adresse ein, unter der das entfernte Verbindungsende erreichbar ist. Klicken Sie auf **Hinzufügen**, um ein Netzwerk zur Liste hinzuzufügen. Wenn Sie mehr als ein Netzwerk hinzufügen, wird eine automatische Ausfallsicherung ausgelöst, falls das erste Netzwerk nicht erreichbar ist. Ihre LANCOM R&S®Unified Firewall versucht in diesem Fall, nacheinander die übrigen Netzwerke in der Liste zu erreichen, bis ein Netzwerk erreichbar ist. Sie können einzelne Einträge in der Liste bearbeiten oder löschen, indem Sie auf die entsprechende Schaltfläche neben einem Eintrag klicken. Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28. Wenn Sie einen Eintrag bearbeiten, erscheint auf der rechten Seite des Eintrags ein Haken. Klicken Sie auf den Haken, um Ihre Änderungen zu übernehmen.
Remote-Port	Geben Sie die Port-Nummer ein, die am entfernten Verbindungsende für diese Verbindung verwendet wird.
Verbindungsversuche für	Geben Sie die Zeitüberschreitung in Minuten an, nach deren Ablauf keine weiteren Verbindungsversuche unternommen werden. Wenn diese Option auf 0 eingestellt ist, werden die Verbindungsversuche ohne Unterbrechung fortgesetzt.

Bei Bridge-Server-Verbindungen können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Bridge	Wählen Sie eine Bridge aus den vorkonfigurierten Bridges aus. Weitere Informationen finden Sie unter *VPN-SSL* auf Seite 198.

Bei Bridge-Client-Verbindungen können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Bridge	Wählen Sie eine Bridge aus den vorkonfigurierten Bridges aus. Weitere Informationen finden Sie unter *VPN-SSL* auf Seite 198.
Remote-Adressen	Geben Sie die IP-Adresse ein, unter der das entfernte Verbindungsende erreichbar ist. Klicken Sie auf **Hinzufügen**, um ein Netzwerk zur Liste hinzuzufügen. Wenn Sie mehr als ein Netzwerk hinzufügen, wird eine automatische Ausfallsicherung ausgelöst, falls das erste Netzwerk nicht erreichbar ist. Ihre LANCOM R&S®Unified Firewall versucht in diesem Fall, nacheinander die übrigen Netzwerke in der Liste zu erreichen, bis ein Netzwerk erreichbar ist. Sie können einzelne Einträge in der Liste bearbeiten oder löschen, indem Sie auf die entsprechende Schaltfläche neben einem Eintrag klicken. Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28. Wenn Sie einen Eintrag bearbeiten, erscheint auf der rechten Seite des Eintrags ein Haken. Klicken Sie auf den Haken, um Ihre Änderungen zu übernehmen.
Remote-Port	Geben Sie die Port-Nummer ein, die am entfernten Verbindungsende für diese Verbindung verwendet wird.
Verbindungsversuche für	Geben Sie die Zeitüberschreitung in Minuten an, nach deren Ablauf keine weiteren Verbindungsversuche unternommen werden. Wenn diese Option auf 0 eingestellt ist, werden die Verbindungsversuche ohne Unterbrechung fortgesetzt.

Die Schaltflächen rechts unten im Bearbeitungsfeld hängen davon ab, ob Sie eine neue VPN-SSL-Verbindung hinzufügen oder eine bestehende Verbindung bearbeiten. Klicken Sie für eine neu konfigurierte Verbindung auf **Erstellen**, um die Verbindung zur Liste der verfügbaren VPN-SSL-Verbindungen hinzuzufügen, oder auf **Abbrechen**, um Ihre Änderungen zu verwerfen.

Wenn Sie Änderungen vorgenommen haben, können Sie diese mit den Schaltflächen unten rechts im Bearbeitungsfenster speichern (**Speichern**) oder verwerfen (**Zurücksetzen**). Andernfalls können Sie das Fenster schließen (**Schließen**).

Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

3.4.7.3 WireGuard

Richten Sie unter **VPN** > **WireGuard** per WireGuard gesicherte VPN-Verbindungen ein.

WireGuard funktioniert aktuell nur auf Unified Firewalls mit einer Internet-Verbindung korrekt. Auf einer Unified Firewall mit mehr als einer Internet-Verbindung ist keine Daten-Übertragung über die WireGuard-Verbindung möglich, da die Unified Firewall die Antwort-Pakete über eine andere Internet-Verbindung sendet als eingehende Pakete.

3.4.7.3.1 WireGuard-Verbindung

Unter **VPN** > **WireGuard** können Sie WireGuard VPN-Verbindungen verwalten.

Eingabefeld	Beschreibung
I/0	Ein Schiebeschalter gibt an, ob diese WireGuard-Verbindung aktiv (**I**) oder inaktiv (**0**) ist. Mit einem Klick auf den Schiebeschalter ändern Sie den Status dieser Option.
Name	Geben Sie dieser WireGuard-Verbindung einen Namen.
Interface	Auswahlliste, in der WireGuard-Interfaces ausgewählt werden können. Siehe *WireGuard-Interfaces* auf Seite 104.
Adresse	Geben Sie hier die IP-Adresse des WireGuard-Interfaces an. Dies kann sowohl eine implizite IP-Adresse (/32 Präfix-Länge) als auch eine IP-Adresse mit Präfix-Länge kleiner als 32 sein.
Port	Port auf der Firewall, über den die WireGuard-Verbindung von der Gegenstelle aufgebaut werden kann. Für die erste Verbindung wird der Standard-Port 51820 vorgeschlagen, danach wird für jede weitere Verbindung hochgezählt bzw. der nächste nicht verwendete Port vorgeschlagen.

Unter dem Reiter **Peers** können Gegenstellen konfiguriert werden. Klicken Sie auf ⊕, um den Peer-Dialog zu öffnen.

Tabelle 23: Peers

Eingabefeld	Beschreibung
Name	Geben Sie dieser Gegenstelle einen Namen.
Remote-Adresse	Optionale externe und somit über das Internet erreichbare Adresse der Gegenstelle. Kann auch ein Domainname sein. Wenn angegeben, dann wird die Firewall versuchen, die Verbindung zu initiieren. Die Angabe wird benötigt, wenn ein Remote-Port angegeben ist.
Remote-Port	Optionaler Port, über den die Verbindung aufgebaut werden soll. Wird benötigt, wenn eine Remote-Adresse angegeben ist.
Public-Key	Der Base64-kodierte Public-Key der Gegenstelle.
Keep-Alive	Intervall in Sekunden zum Senden von Paketen zur Aufrechterhaltung der Verbindung, Default 25, bei einem Wert von 0 wird die Verbindung nur bei Bedarf hergestellt.
Routen erstellen	Wenn aktiviert, dann werden alle IP-Adressen unter **Erlaubte IP-Adressen** automatisch in die Routing-Tabelle 201 eingetragen. Sonst müssen Sie die Routen manuell erstellen.

Eingabefeld	Beschreibung
Erlaubte IP-Adressen	IP-Adressen oder Netze mit Subnetzmaske, die über die WireGuard-Verbindung erreichbar sein sollen.

Unter dem Reiter **Authentifizierung** kann ein Private- / Public-Key-Paar erzeugt werden. Diese werden bei WireGuard anstelle von Zertifikaten verwendet.

Tabelle 24: Authentifizierung

Eingabefeld	Beschreibung
Private-Key ändern	Diese Option soll verhindern, dass ein bereits eingegebener Key überschrieben wird. Das Aktivieren dieses Hakens aktiviert auch die Schaltfläche **Schlüsselpaar erzeugen**.
Private-Key	Geben Sie entweder einen Base64-String als Private-Key ein oder lassen Sie das Feld leer.
Public-Key	Der Public Key zum Private Key. Generieren Sie ihn ggfs. mittels **Schlüsselpaar erzeugen**.
Schlüsselpaar erzeugen	Mit einem Klick auf diese Schaltfläche erezugen Sie ein Private- / Public-Key-Paar. Falls bereits ein **Private-Key** existiert, dann erhalten Sie eine Sicherheitsabfrage.
Public-Key erzeugen	Mit einem Klick auf diese Schaltfläche erezugen Sie einen Public-Key zu einem bereits eingetragenen Private-Key.
Public-Key kopieren	Kopieren Sie den Public Key in die Zwischenablage. Der kopierte Schlüssel kann dann auf der Gegenstelle eingetragen werden, oder an den Admin der Gegenstelle versendet werden.

Die Schaltflächen rechts unten im Bearbeitungsfeld hängen davon ab, ob Sie eine neue Verbindung hinzufügen oder eine bestehende bearbeiten. Klicken Sie für eine neu konfigurierte Verbindung auf **Erstellen**, um sie zur Liste der verfügbaren Verbindungdn hinzuzufügen, oder auf **Abbrechen**, um Ihre Änderungen zu verwerfen. Zum Bearbeiten einer vorhandenen Verbindung klicken Sie auf **Speichern**, um die neu konfigurierte Verbindung zu speichern, oder auf **Zurücksetzen**, um Ihre Änderungen zu verwerfen.

3.4.8 Zertifikatsverwaltung

Mit den Einstellungen unter ✹ **-Zertifikatsverwaltung** können Sie die vom Webclient, vom eingebauten SSL-Proxy und vom OpenVPN-Server verwendeten Zertifikate verwalten, Vorlagen erstellen, die die Erstellung von Zertifikaten vereinfachen und Ihre Proxy-CAs verwalten.

3.4.8.1 Zertifikate

Mit den Einstellungen unter **Zertifikate** können Sie die Zertifikate verwalten, die der LANCOM R&S®Unified Firewall-Webclient, der integrierte SSL-Proxy und der OpenVPN-Server nutzen.

Um verschlüsselte Verbindungen abzusichern, nutzt Ihre LANCOM R&S®Unified Firewall digitale Zertifikate, wie im X.509-Standard beschrieben.

Die LANCOM R&S®Unified Firewall selbst agiert als Zertifizierungsstelle (Certification Authority). Daher ist ein so genanntes CA-Zertifikat erforderlich. Um die Verwaltung der Zertifikate zu zentralisieren, ist es empfehlenswert, ein CA-Zertifikat in einer zentralen Firewall zu erstellen und es direkt für die Signatur aller für die Anwendung genutzten Zertifikate zu verwenden. Dies wird als einstufige Zertifizierungskette bezeichnet.

Alle Zertifikate für Anwendungen müssen von der zentralen Firewall signiert werden. Wenn ein Zertifikat für eine andere Firewall benötigt wird, müssen Sie darauf eine Anforderung erstellen. Diese Anforderung muss von der zentralen Firewall signiert werden. Die signierte Anforderung, die Sie erstellt haben, muss von den anderen Firewalls importiert werden, um genutzt werden zu können.

Um die anderen Firewalls dazu zu befähigen, Zertifikate zu erstellen, die zwar hauptsächlich lokalen Zwecken dienen, aber dennoch in Ihrer gesamten Organisation als gültig anerkannt werden, können Sie mehrstufige Zertifizierungsketten einsetzen. Dafür benötigen Sie in Ihrer zentralen Firewall ein so genanntes Root-CA-Zertifikat, mit dem Sie die untergeordneten CA-Zertifikate signieren können. Sie müssen für diese untergeordneten CA-Zertifikate Anforderungen

auf Ihren anderen Firewalls erstellen. Nachdem Sie die signierten CA-Zertifikate importiert haben, sind die anderen Firewalls selbst in der Lage, Zertifikate für Anwendungen zu signieren. Um diese Hierarchien übersichtlich darzustellen, werden sie in einer Baumansicht angezeigt.

3.4.8.1.1 Übersicht Zertifikate

Navigieren Sie zu **Zertifikatsverwaltung** > **Zertifikate**, um die Liste der derzeit im System angelegten Zertifikate in einem Baumdiagramm nach Zertifizierungsstellen im rechten Bereich anzuzeigen.

Mit den Schaltflächen oberhalb der Liste können Sie Äste ein bzw. ausklappen, ein Zertifikat aus einer Datei importieren (➔]) bzw. eine Zertifikatsignierungsanforderung signieren oder ein neues Zertifikat erstellen.

Nach dem ersten Hochfahren und nach einer erneuten Installation werden die folgenden Zertifikate standardmäßig, teilweise allerdings erst nach Auswahl im Setup-Assistent, angelegt:

Tabelle 25: Bereits angelegte Zertifikate

Name des Zertifikats	Beschreibung
LCOS FX Default Root CA	Oberste Zertifizierungsstelle zur Erstellung von untergeordneten Zertifizierungsstellen und Zertifikaten.
LCOS FX Default HTTPS Proxy CA	Zertifizierungsstelle zur Erstellung von untergeordneten Zertifikaten zur Verwendung durch den HTTPS Proxy.
LCOS FX Default Appfilter Certificate	Vorkonfiguriertes Zertifikat für das Application Management.
LCOS FX Default Mail Proxy CA	Zertifizierungsstelle zur Erstellung von untergeordneten Zertifikaten zur Verwendung durch den Mailproxy.
LCOS FX Default Mail Proxy Certificate	Vorkonfiguriertes Zertifikat für den Mailproxy.
LCOS FX Default Web Portal Certificate	Vorkonfiguriertes Zertifikat für das Web Portal.
LCOS FX Default Webserver Certificate	Vorkonfiguriertes Zertifikat für den Webserver.

In der Liste werden der Name des jeweiligen Zertifikats und durch die Baumstruktur auch dessen Abhängigkeiten angezeigt. Die Schaltflächen hinter den jeweiligen Zertifikaten zeigen den Gültigkeitsstatus:

- ✔ – Zertifikat ist gültig
- ✔ – Zertifikat läuft in 8 bis 30 Tagen ab
- ✔ – Zertifikat läuft in einem bis 7 Tagen ab
- ⚠ – Zertifikat ist abgelaufen
- ⛔ – Zertifikat wurde revoziert
- ↻ – Zertifikat wurde ersetzt

Zudem wird angezeigt, ob ein privater Schlüssel für das Zertifikat vorhanden ist (🔑) und über ein „CA“, ob das Zertifikat eine Zertifizierungsstelle ist. Außerdem können Sie mithilfe der Schaltflächen Details zu jedem Zertifikat anzeigen lassen (👁), ein Zertifikat exportieren ([➔), die Gültigkeit eines Zertifikats oder erneuern (↻), das Zertifikat revozieren (⊘) und das Zertifikat oder nur den zugehörigen privaten Schlüssel löschen (🗑).

Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28.

Zertifikatsansicht filtern

Sie können die Zertifikatsansicht mithilfe der Filterfunktion im Eingabefeld **Zertifikats-Filter** um verschiedene Suchkriterien und -optionen eingrenzen.

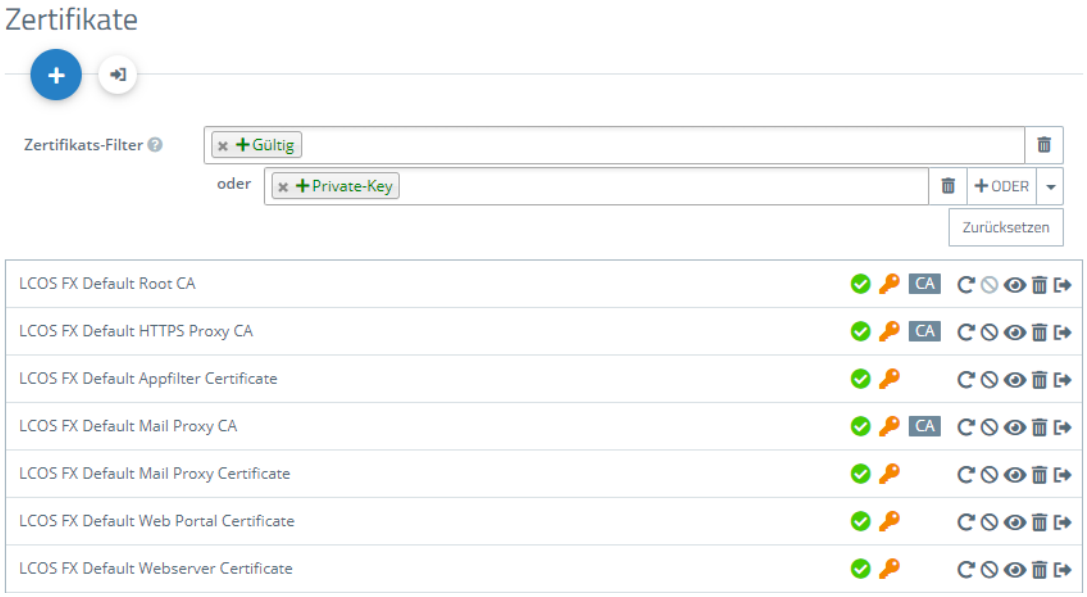


Abbildung 38: Zertifikate mit angewandtem Filter

Um einen Filter zu erstellen, gehen Sie wie folgt vor:

1. Klicken Sie in das Eingabefeld.

   Der Webclient zeigt Filtervorschläge an.

2. Wählen Sie einen der vorgeschlagenen Filter aus der Drop-down-Liste aus oder geben Sie einen beliebigen Suchtext ein, um weitere Vorschläge zu erhalten. Vordefinierte Filter sind:

   - Status
     - Gültige Zertifikate
     - Abgelaufene Zertifikate
     - Revozierte Zertifikate
     - Weniger als eine Woche gültige Zertifikate
     - Weniger als einen Monat gültige Zertifikate
     - Noch nicht gültige Zertifikate
   - Eigenschaft
     - Mit Private-Key
     - Ist eine Certificate Authority
     - Ist ein Request
     - Wurde mit Hilfe eines der folgenden Schlüssel-Algorithem generiert: RSA, NIST Curves, ED448, ED25519
     - NIST-Kurventypen: secp224r1, secp256r1, secp384r1, secp521r1, secp256k1
     - Schlüsselgröße: 1024, 1536, 2048, 3072, 4096, 6144 und 8192
     - Schlüsselverwendung: Inhaltsverpflichtung, CRL-Signierung, Datenverschlüsselung, Nur Entschlüsselung, Digitale Signatur, Nur Verschlüsselung, Schlüsselvereinbarung, Schlüsselzertifikats-Signierung, Schlüsselverschlüsselung
     - Erweiterte Schlüsselverwendung: Beliebige erweiterte Schlüsselverwendung, Client-Authentifizierung, Code-Signierung, E-Mail-Schutz, OCSP-Signierung, Server-Authentifizierung, Zeitstempel
     - Hash-Algorithmen: sha1, sha224, sha256, sha384, sha512

- Revozierungsgründe: Nicht spezifiziert, Schlüssel gefährdet, CA gefährdet, Zugehörigkeit geändert, Ersetzt, Geschäftsaufgabe, Recht entzogen, Attribut-Authorität gefährdet

Sobald ein Text eingegeben wird, werden weitere Filter-Eigenschaften angeboten:

- Text
  - Common Name enthält eingegebenen Text
  - Subjekt enthält eingegebenen Text
  - Subjekt des Ausstellers enthält eingegeben Text
- Hexadezimal-Notation (Bindestriche und Doppelpunkte werden ignoriert, d. h. Sie können z. B. „dddd" eingeben und sowohl „dd-dd" als auch „dd:dd" werden als gültig angesehen)
  - Fingerabdruck enthält eingegebenen Text
  - Signatur enthält eingegebenen Text

Für jeden Vorschlag können Sie auswählen, ob dieser als Inklusionsfilter (+ / UND-Verknüpfung) oder Exklusionsfilter (⊘ / UND-NICHT-Verknüpfung) verwendet werden soll.

Nach der Auswahl wird der Filtervorschlag als Suchkriterium in das Eingabefeld eingefügt.

Die Liste der Zertifikate passt sich an die Suchabfrage an.

Wiederholen Sie die obigen Schritte, bis Sie die gewünschten Filterkriterien zu Ihrer Suchanfrage hinzugefügt haben.

Es werden nur Einträge angezeigt, die mit allen Filterkriterien übereinstimmen.

Um ein Filterkriterium in einer Suchabfrage zu löschen, klicken Sie auf ✖.

Sie können mehrere Zeilen zu Ihrer Suchanfrage hinzufügen, indem Sie neben dem Eingabefeld auf **+ ODER** klicken. Sie können wählen, ob Sie eine neue leere Zeile einfügen, oder die zuletzt angelegte Zeile kopieren möchten. Jede Zeile ist in sich eine eigene Suchabfrage, die mit den anderen Zeilen ODER-verknüpft wird.

Löschen Sie die Zeile, indem Sie neben der Zeile auf 🗑 klicken.

Zertifikat oder Zertifikats-Request erstellen

Mit der Plus-Schaltfläche ⊕ oberhalb der Liste mit den Elementen können Sie neue Zertifikate und Signierungsanfragen erzeugen. Für die Erstellung können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Zertifikatstyp	Wählen Sie zwischen den Optionen **Zertifikat** zur Erstellung eines Zertifikats bzw. einer Zertifizierungsstelle (CA) und einem **Zertifikats-Request**. Mit letzterem erstellen Sie eine Zertifizierungsanfrage für ein Zertifikat oder eine untergeordnete CA, welches dann von einer übergeordneten CA signiert werden muss, damit es gültig wird. Bei Auswahl der Option **Zertifikats-Request** können weder **Gültigkeit** noch die **Signierende CA** ausgewählt werden, da diese bei der Signierung des Zertifikats festgelegt werden. Der erstellte Request erscheint in dem Zertifikatsbaum im Anschluss an die Zertifikate in einem gesonderten Zweig **Ausstehende Zertifikatssignierungsanforderungen**.
Common Name (CN)	Legen Sie einen Namen für das Zertifikat fest.
Private-Key-Passwort	Obligatorisch: Geben Sie ein Passwort ein, um den privaten Schlüssel abzusichern.
Passwort anzeigen	Optional: Setzen Sie den Haken im Kontrollkästchen, um das Passwort zur Überprüfung anzuzeigen.

Eingabefeld	Beschreibung
Gültigkeit	Legen Sie den anfänglichen Zeitraum fest, für den das Zertifikat gültig sein soll. Die Eingabefelder sind bereits mit dem aktuellen Datum als Erstellungsdatum und dem gleichen Tag ein Jahr später im Falle eines Zertifikats bzw. 5 Jahre später bei einer Certificate Authority als Ablaufdatum ausgefüllt. Um einen anderen Zeitraum festzulegen, wählen Sie eine der vorgegebenen Optionen aus oder selektieren Sie im angezeigten Kalender das Start- und Enddatum. Das Start- und Enddatum wird in folgendem Format angezeigt: MM/DD/JJJJ - MM/DD/JJJJ (z. B. `04/18/2021 - 04/18/2031`).
Vorlage	Optional: Wählen Sie eine der unter *Vorlagen* auf Seite 213 vorhandenen Vorlagen aus, um die Felder im Bereich „Optionen“ und „Subject und SAN“ aus der Vorlage zu übernehmen. Bei Auswahl einer Vorlage werden bereits vorgenommene Einstellungen überschrieben!
Signierende CA	Wählen Sie die signierende CA aus.
CA-Passwort	Wenn eine CA ausgewählt ist, ist dieses Feld obligatorisch, es sei denn, es handelt sich um eine der in *Tabelle 25: Bereits angelegte Zertifikate* auf Seite 206 aufgeführten LCOS FX CAs. Geben Sie ein Passwort für den privaten Schlüssel der signierenden Zertifizierungsstelle ein. Das Passwort ist notwendig, da die Signatur des öffentlichen Schlüssels für das neue Zertifikat mit dem privaten Schlüssel der signierenden Zertifizierungsstelle erfolgt.
Zeige CA-Passwort	Optional: Setzen Sie den Haken im Kontrollkästchen, um das Passwort zur Überprüfung anzuzeigen.
Certificate Authority	Diese Option bestimmt, ob das zu erstellende Zertifikat als Zertifizierungsstelle auch andere Zertifikate signieren kann oder nicht. **Vorsicht**: Die Standard-Gültigkeitsdauern für Zertifikate (1 Jahr) und Certificate Authorities (5 Jahre) unterscheiden sich. Bei Änderung dieser Eigenschaft wird die Gültigkeitsdauer angepasst.
Pfad-Länge	Nur bei Auswahl von **Certificate Authority** vorhanden. Hier bestimmen Sie, wie viele Sub-CA-Ebenen mit dieser CA erzeugt werden können. Bei einem Wert von 0 können keine Sub-CAs mit dieser CA signiert werden, d. h. nur noch „normale“ Zertifikate können mit dieser CA signiert werden. Wenn das Feld leer bleibt, gibt es keine Begrenzung.
Schlüsselverwendung	Hier können Sie nach einem Klick in das Feld vordefinierte Eigenschaftswerte aus einer Liste hinzufügen wie z. B. Datenverschlüsselung.
Verschlüsselungs-Algorithmus	Wählen Sie aus der Liste der Algorithmen den von Ihnen gewünschten aus. › RSA (Standard-Einstellung) › NIST Curves › ED448 › ED25519 Bei Auswahl der Option „NIST Curves“ muss in dem Feld **Kurve** die Art der NIST-Kurve gewählt werden. Die neuen Algorithmen „NIST Curves“, „ed448“ und „ed25519“ werden allerdings von einigen Diensten nur zum Teil oder noch gar nicht unterstützt, z.B. im Reverse Proxy.
Kurve	Falls Sie unter **Verschlüsselungs-Algorithmus** die Option „NIST Curves“ ausgewählt haben, dann können Sie hier die Art der NIST-Kurve auswählen. › NIST P-224 (SECP224R1) › NIST P-256 (SECP256R1) › NIST P-384 (SECP384R1) › NIST P-521 (SECP521R1)

Eingabefeld	Beschreibung
	› SECP256K1
Schlüssel-Größe	Falls Sie unter **Verschlüsselungs-Algorithmus** die Option „RSA" ausgewählt haben, dann können Sie hier die Schlüsselgröße auswählen. Beachten Sie, dass Schlüsselgrößen unter 2048 von einigen Diensten auf der Firewall wie z. B. Mail- und HTTPS-Proxy, nicht mehr akzeptiert werden.
Hash-Algorithmus	Wählen Sie einen der vorgegebenen Hash-Algorithmen aus. › sha1 › sha224 › sha256 › sha384 (Standard-Einstellung) › sha512
Erweiterte Schlüsselverwendung	Hier können Sie nach einem Klick in das Feld weitere vordefinierte Eigenschaftswerte aus einer Liste hinzufügen wie z. B. Zeitstempel.
Subjekt	Optional: Wählen Sie eine beliebige Anzahl an Subjekten wie z. B. **Land (C)**, **Bundesland (ST)**, **Organisation (O)**, oder **Abteilung (OU)** aus der Drop-down-Liste aus und geben Sie den dazu gewünschten Inhalt in das Eingabefeld rechts daneben ein. Klicken Sie rechts auf ⊕, um einen Eintrag zur Liste hinzuzufügen. Sie können einzelne Einträge in den Listen bearbeiten oder löschen, indem Sie auf die entsprechende Schaltfläche neben einem Eintrag klicken. Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28. Wenn Sie ein **Subjekt** bearbeiten, erscheint auf der rechten Seite des Eintrags ein Haken. Sie müssen Ihre Änderung zunächst mit diesem Haken bestätigen, bevor Sie die Einstellungen für das Zertifikat speichern können.
Subject Alternative Name (SAN)	Optional: Geben Sie eine beliebige Anzahl benutzerdefinierter alternativer Namen für bestimmte Nutzungszwecke ein und wählen Sie die entsprechenden Typen aus der Drop-down-Liste aus. Die folgenden Typen stehen zur Verfügung: `E-Mail`, `DNS`, `DirName`, `URI`, `IP` und `RegID`. Klicken Sie rechts auf ⊕, um einen Subject Alternative Name (SAN) zur Liste hinzuzufügen. Sie können einzelne Einträge in den Listen bearbeiten oder löschen, indem Sie auf die entsprechende Schaltfläche neben einem Eintrag klicken. Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28. Wenn Sie einen **Subject Alternative Name (SAN)** bearbeiten, erscheint auf der rechten Seite des Eintrags ein Haken. Sie müssen Ihre Änderung zunächst mit diesem Haken bestätigen, bevor Sie die Einstellungen für das Zertifikat speichern können.

Mit den Schaltflächen rechts unten im Bearbeitungsfeld können Sie ein neues Zertifikat erstellen und zu der Liste der verfügbaren Zertifikate hinzufügen oder die Erstellung eines neuen Zertifikats abbrechen (**Abbrechen**).

Zertifikat importieren oder Certificate Signing Request signieren

Mit der Schaltfläche oberhalb der Liste können Sie ein Zertifikat aus einer Datei importieren bzw. einen Certificate Signing Request signieren.

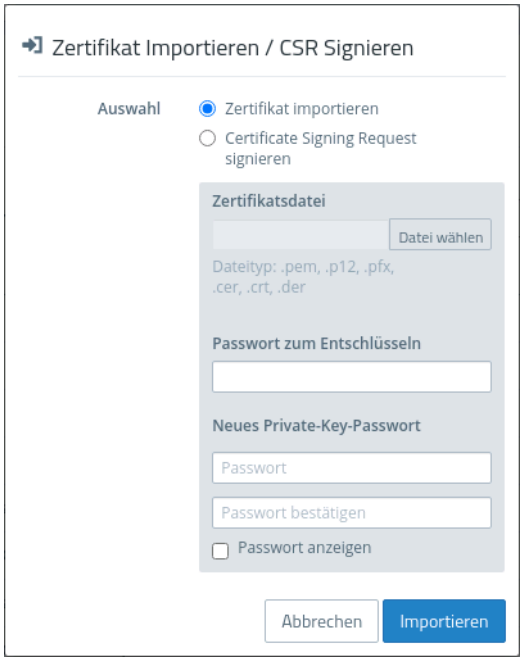


Abbildung 39: Zertifikat importieren / Certificate Signing Request signieren

Über die Auswahl im oberen Bereich entscheiden Sie, ob Sie ein Zertifikat importieren oder einen Certificate Signing Request signieren wollen.

Für den Import können Zertifikatsdateien mit verschiedenen Datei-Endungen ausgewählt werden (*.pem, *.p12, *.pfx, *.cer, *.crt, *.der). Je nachdem, ob in der Datei ein privater Schlüssel vorhanden ist, muss ein Passwort zum Entschlüsseln und ein Passwort zum Wiederverschlüsseln des privaten Schlüssels eingegeben werden. Optional können Sie sich das Passwort anzeigen lassen.

Im Falle einer Zertifikatssignierungsanforderung wählen Sie die zugehörige Datei aus. In Frage kommen die folgenden Dateitypen: *.pem, *.crt, *.cer, *.der. Es muss eine signierende CA ausgewählt und das dazugehörige Passwort eingegeben werden. Zudem muss der Gültigkeitszeitraum gewählt werden. Sobald das Zertifikat erfolgreich signiert wurde, wird das signierte Zertifikat als PEM zum Download angeboten.

Mit den Schaltflächen rechts unten im Bearbeitungsfeld können Sie die ausgewählte Zertifikatsdatei importieren und zu der Liste der verfügbaren Zertifikate hinzufügen bzw. den Certificate Signing Request signieren oder den Dialog abbrechen (**Abbrechen**).

Zertifikat erneuern

Mit der Schaltfläche bei einem Zertifikat in der Liste wird ein neues Zertifikat mit einem neuen Gültigkeitszeitraum erstellt.

Im Falle eines einfachen Zertifikats wählen Sie unter **Gültigkeit** den neuen Zeitraum und geben das **CA-Passwort** des zugehörigen CA-Zertifikats ein. Bei nicht selbstsignierten Zertifikaten kann bei der Erneuerung eine komplett andere CA gewählt werden. Es ist nicht beschränkt auf die gegenwärtige CA. Bei nicht selbstsignierten Zertifikaten müssen zwei Passwörter eingegeben werden; das CA-Passwort und das Private-Key-Passwort des zu erneuernden Zertifikats.

Bei einer Certificate Authority (CA) können Sie zusätzlich den Common Name ändern und den von dieser CA signierten Zertifikaten einen neuen Gültigkeitszeitraum zuweisen.

Abgeleitete Sub-CAs und Zertifikate müssen manuell erneuert werden.

Die zu erneuernden Zertifikate werden nicht mehr automatisch revoziert. Optional können Sie das Revozieren im Anschluss an die Erneuerung durchführen.

Mit den Schaltflächen rechts unten im Bearbeitungsfeld können Sie den Gültigkeitszeitraum des ausgewählten Zertifikats bzw. der CA und ggf. den von dieser signierten Zertifikaten erneuern oder den Dialog abbrechen (**Abbrechen**).

Zertifikat revozieren

Mit der Schaltfläche ⃠ bei einem Zertifikat in der Liste können Sie dieses revozieren. Dazu müssen Sie einen Grund auswählen und das Passwort des privaten Schlüssels der übergeordneten CA des Zertifikats eingeben.

Zertifikate können nicht revoziert werden, wenn

- das Zertifikat bereits revoziert wurde,
- das Zertifikat keine CA hat (First-Level-CA) oder
- die CA des Zertifikats keinen privaten Schlüssel hat.

Mit den Schaltflächen rechts unten im Bearbeitungsfeld können Sie die Revozierung des ausgewählten Zertifikats durchführen oder den Dialog abbrechen (**Abbrechen**).

Zertifikatsdetails ansehen

Mit der Schaltfläche 👁 bei einem Zertifikat in der Liste können Sie sich die Zertifikatsdetails ansehen.

Mit den Schaltflächen rechts unten im Bearbeitungsfeld können Sie den öffentlichen Schlüssel und den Fingerabdruck des Zertifikats in die Zwischenablage kopieren oder den Dialog schließen (**Schließen**).

Zertifikat oder privaten Schlüssel löschen

Mit der Schaltfläche 🗑 bei einem Zertifikat in der Liste können Sie das Zertifikat oder nur den zugehörigen privaten Schlüssel löschen. Das gelöschte Zertifikat wird im Gegensatz zum Revozieren auch aus dem Zertifikatsbaum entfernt. Es wird kein Passwort zum Löschen benötigt.

Mit den Schaltflächen rechts unten im Bearbeitungsfeld können Sie das Zertifikat bzw. alternativ nur den privaten Schlüssel löschen oder den Dialog abbrechen (**Abbrechen**).

Zertifikat exportieren

Mit der Schaltfläche ⮆ bei einem Zertifikat in der Liste können Sie dieses in einem der Formate PEM, PKCS oder DER exportieren

PEM

Beim Export im PEM-Format wird in der Regel nur der öffentliche Teil des Zertifikats exportiert. Optional können zusätzlich auch alle zugehörigen CAs der PEM-Datei hinzugefügt werden. Zusätzlich kann, wenn vorhanden, der private Schlüssel mit exportiert werden. Dafür müssen sowohl das aktuell gültige Passwort für den privaten Schlüssel zum Entschlüsseln und ein neues Passwort zum Verschlüsseln des exportierten privaten Schlüssels eingegeben werden. Wenn das Zertifikat keinen privaten Schlüssel hat, wird diese Option nicht angeboten.

PKCS

Das PKCS-Format kann beim Export nur gewählt werden, wenn das Zertifikat einen privaten Schlüssel besitzt. Dazu wird wie beim PEM-Export mit Schlüssel das aktuell gültige Passwort und ein neues Passwort zum Verschlüsseln zwingend benötigt. Im Gegensatz zu PEM wird das Passwort zum Verschlüseln des gesamten Containers verwendet und nicht für den privaten Schlüssel.

DER

Beim Export im DER-Format, wird das Zertifikat im PEM-Format exportiert, wobei die PEM Base64-kodiert wird. Optional kann auch hier der private Schlüssel unter Eingabe der Passwörter exportiert werden. Da das DER-Format nur ein Zertifikat unterstützt, wird in diesem Fall das Zertifikat und der private Schlüssel separat gespeichert und in einer ZIP-Datei zusammengefasst. Der private Schlüssel wird im pkcs8-Format gespeichert.

Mit den Schaltflächen rechts unten im Bearbeitungsfeld können Sie das Zertifikat exportieren oder den Dialog abbrechen (**Abbrechen**).

3.4.8.1.2 Private-Key-Passwort

Sie müssen immer, wenn ein Zertifikat mit einem privaten Schlüssel benötigt wird, dieses Passwort zur Entschlüsselung des Schlüssels eingeben, wenn

- die jeweiligen Einstellungen aktiviert werden oder
- das verwendete Zertifikat geändert wird.

Dieses Verhalten betrifft folgende Dialoge bzw. Einstellungen:

- Command-Center-Einstellungen
- Webclient-Einstellungen
- Application-Management-Einstellungen
- HTTP-Proxy-Einstellungen
- Mail-Proxy-Einstellungen
- Reverse-Proxy-Frontend-Einstellungen
- Einstellungen des externen Portals
- VPN-Profile
- Einstellungen des internen Portals
- IPsec-Verbindungen mit Zert. oder CA-Authentifizierung
- VPN-SSL-Einstellungen

Abweichend hiervon muss kein Private-Key-Passwort eingegeben werden, wenn es sich um eine der in *Tabelle 25: Bereits angelegte Zertifikate* auf Seite 206 aufgeführten LCOS FX CAs handelt.

3.4.8.2 Vorlagen

Zur vereinfachten Erstellung neuer Zertifikate können Sie Vorlagen nutzen, um die Eingabefelder für einige optionale Felder, z. B. den **Distinguished Name** und die **Subject Alternative Names** automatisch auszufüllen.

3.4.8.2.1 Übersicht Vorlagen

Navigieren Sie zu **Zertifikatsverwaltung** > **Vorlagen**, um die Liste der derzeit im System angelegten Vorlagen in der Objektleiste anzuzeigen. Zwei Vorlagen für Zertifikate und Certificate Authorities sind nach Installation bereits eingerichtet.

In der erweiterten Ansicht zeigen die Tabellenspalten den Namen und die Einstellungen der Vorlage. Mit den Schaltflächen in der letzten Spalte können Sie die Einstellungen für eine vorhandene Vorlage einsehen und anpassen, eine neue Vorlage ausgehend von einer vorhandenen anlegen, oder eine Vorlage aus dem System löschen.

Die beiden Standardvorlagen können nicht gelöscht werden.

Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28.

3.4.8.2.2 Einstellungen für Vorlagen

Im Bearbeitungsfenster **Vorlagen** können Sie zusätzliche Optionen für Zertifikate vorgeben, die bei der Zertifikatserstellung dann automatisch übernommen werden können. Die folgenden Elemente können vorgegeben werden:

Eingabefeld	Beschreibung
Name	Geben Sie einen Namen für die Vorlage an. Über diesen Namen können Sie die Vorlage bei der Zertifikatserstellung auswählen.
Certificate Authority	Diese Option bestimmt, ob das zu erstellende Zertifikat als Zertifizierungsstelle auch andere Zertifikate signieren kann oder nicht. **Vorsicht**: Die Standard-Gültigkeitsdauer für Zertifikate (1 Jahr) und Certificate Authorities (5 Jahre) unterscheiden sich. Bei Änderung dieser Eigenschaft wird die Gültigkeitsdauer angepasst.
Pfad-Länge	Nur bei Auswahl von **Certificate Authority** vorhanden. Hier bestimmen Sie, wie viele Sub-CA-Ebenen mit dieser CA erzeugt werden können. Bei einem Wert von 0 können keine Sub-CAs mit dieser CA signiert werden, d. h. nur noch „normale" Zertifikate können mit dieser CA signiert werden. Wenn das Feld leer bleibt, gibt es keine Begrenzung.
Schlüsselverwendung	Hier können Sie nach einem Klick in das Feld vordefinierte Eigenschaftswerte aus einer Liste hinzufügen wie z. B. Datenverschlüsselung.
Verschlüsselungs-Algorithmus	Wählen Sie aus der Liste der Algrithmen den von Ihnen gewünschten aus. Bei Auswahl der Option „NIST Curves" muss in dem Feld **Kurve** die Art der NIST-Kurve gewählt werden.
Kurve	Falls Sie unter **Verschlüsselungs-Algorithmus** die Option „NIST Curves" ausgewählt haben, dann können Sie hier die Art der NIST-Kurve auswählen.
Schlüssel-Größe	Falls Sie unter **Verschlüsselungs-Algorithmus** die Option „RSA" ausgewählt haben, dann können Sie hier die Schlüsselgröße auswählen.
Hash-Algorithmus	Wählen Sie einen der vorgegebenen Hash-Algorithmen aus.
Erweiterte Schlüsselverwendung	Hier können Sie nach einem Klick in das Feld weitere vordefinierte Eigenschaftswerte aus einer Liste hinzufügen wie z. B. Zeitstempel.
Subjekt	Optional: Wählen Sie eine beliebige Anzahl an Subjekten wie z. B. **Land (C)**, **Bundesland (ST)**, **Organisation (O)**, oder **Abteilung (OU)** aus der Drop-down-Liste aus und geben Sie den dazu gewünschten Inhalt in das Eingabefeld rechts daneben ein. Klicken Sie rechts auf ⊕, um einen Eintrag zur Liste hinzuzufügen. Sie können einzelne Einträge in den Listen bearbeiten oder löschen, indem Sie auf die entsprechende Schaltfläche neben einem Eintrag klicken. Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28. Wenn Sie ein **Subjekt** bearbeiten, erscheint auf der rechten Seite des Eintrags ein Haken. Sie müssen Ihre Änderung zunächst mit diesem Haken bestätigen, bevor Sie die Einstellungen für das Zertifikat speichern können.
Subject Alternative Name (SAN)	Optional: Geben Sie eine beliebige Anzahl benutzerdefinierter alternativer Namen für bestimmte Nutzungszwecke ein und wählen Sie die entsprechenden Typen aus der Drop-down-Liste aus. Die folgenden Typen stehen zur Verfügung: `E-Mail`, `DNS`, `DirName`, `URI`, `IP` und `RegID`. Klicken Sie rechts auf ⊕, um einen Subject Alternative Name (SAN) zur Liste hinzuzufügen. Sie können einzelne Einträge in den Listen bearbeiten oder löschen, indem Sie auf die entsprechende Schaltfläche neben einem Eintrag klicken. Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28. Wenn Sie einen **Subject Alternative Name (SAN)** bearbeiten, erscheint auf der rechten Seite des Eintrags ein Haken. Sie müssen Ihre Änderung zunächst mit diesem Haken bestätigen, bevor Sie die Einstellungen für das Zertifikat speichern können.

Die Schaltflächen rechts unten im Bearbeitungsfeld hängen davon ab, ob Sie eine neue Vorlage hinzufügen oder eine bestehende bearbeiten. Klicken Sie für eine neu konfigurierte Vorlage auf **Erstellen**, um sie zur Liste der verfügbaren Vorlagen hinzuzufügen, oder auf **Abbrechen**, um Ihre Änderungen zu verwerfen. Zum Bearbeiten einer vorhandenen

Vorlagen klicken Sie auf **Speichern**, um die neu konfigurierte Vorlage zu speichern, oder auf **Zurücksetzen**, um Ihre Änderungen zu verwerfen.

3.4.8.3 Let's Encrypt

Mit den Einstellungen unter **Let's Encrypt** können Sie Let's Encrypt-Zertifikate verwendet werden. Dazu werden neben einem Let's Encrypt Account nur wenige Einstellungen auf der Firewall benötigt.

3.4.8.3.1 Einstellungen für Let's Encrypt

Im Bearbeitungsfenster **Zertifikatsverwaltung** > **Let's Encrypt** können Sie Einstellungen für Let's Encrypt-Zertifikate vornehmen. Die folgenden Elemente können vorgegeben werden:

Eingabefeld	Beschreibung
E-Mail-Adresse	Geben Sie die E-Mail-Adresse ein, mit welcher der Let's Encrypt-Account registriert wird.
Server-Adresse	Geben Sie optional eine URL für den Let's Encrypt-Server an. Falls das Zertifikat des Servers nicht global vertrauenswürdig ist, dann muss die dazugehörige Certificate Authority im Zertifikatsmanagement importiert und hier dann ausgewählt werden.
Certificate Authority	Geben Sie bei einer geänderten URL für den Let's Encrypt-Server hier die Certificate Authority an, falls diese nicht global vertrauenswürdig ist.

Wenn Sie Änderungen vorgenommen haben, können Sie diese mit den Schaltflächen unten rechts im Bearbeitungsfenster speichern (**Speichern**) oder verwerfen (**Zurücksetzen**). Andernfalls können Sie das Fenster schließen (**Schließen**).

Die mittels Let's Encrypt erstellten Zertifikate werden unter **Zertifikatsverwaltung** > **Zertifikate** unter **Let's Encrypt-Zertifikate** angezeigt. Diese Zertifikate können nur „Erneuert", „Angesehen" und „Exportiert" werden. „Revozieren", „Löschen" und auch das „Erneuern", sobald das Ende des Gültigkeitszeitraums erreicht wird, werden automatisch durchgeführt.

3.4.8.4 Proxy-CAs

Mit den Einstellungen unter **Proxy CA** können Sie Ihre CA-Zertifikate verwalten. Dazu werden diese in vertrauenswürdige und nicht vertrauenswürdige Listen eingeordnet.

3.4.8.4.1 Vertrauenswürdige Proxy-CAs

Navigieren Sie zu **Zertifikatsverwaltung** > **Proxy-CAs** > **Vertrauenswürdige CAs**, um die Liste der derzeit im System angelegten benutzerdefinierten und System-Zertifizierungsstellen, denen der SSL-Proxy für externe Verbindungen vertraut, in der Objektleiste anzuzeigen.

In der erweiterten Ansicht wird in der ersten Tabellenspalte der **Common Name** des CA-Zertifikats angezeigt. Mit den Schaltflächen in der letzten Spalte können Sie die Einstellungen für ein vorhandenes CA-Zertifikat einsehen oder ein CA-Zertifikat als nicht vertrauenswürdig kennzeichnen. Dadurch wird es in die Liste unter **Zertifikatsverwaltung** > **Proxy-CAs** > **Nicht vertrauenswürdige CAs** verschoben. Benutzerdefinierte CA-Zertifikate können Sie auch löschen.

Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28.

Um eine benutzerdefinierte CA an Ihre LANCOM R&S®Unified Firewall zu senden, klicken Sie auf die ➔ (Import)-Schaltfläche in der Kopfzeile der Objektleiste, wählen Sie die gewünschte PEM-/CRT-Datei aus, öffnen Sie sie und klicken Sie auf **Importieren**. Das importierte benutzerdefinierte Zertifikat wird zur Liste verfügbarer vertrauenswürdiger Proxy-CAs hinzugefügt. Über die Option **Nur benutzerdefinierte CAs anzeigen** können Sie die angezeigte Liste auf die von Ihnen hinzugefügten Certificate Authorities reduzieren.

3.4.8.4.2 Nicht vertrauenswürdige Proxy-CAs

Navigieren Sie zu **Zertifikatsverwaltung** > **Proxy-CAs** > **Nicht vertrauenswürdige CAs**, um die Liste der derzeit im System angelegten benutzerdefinierten und System-Zertifizierungsstellen, denen der SSL-Proxy für externe Verbindungen **nicht** vertraut, in der Objektleiste anzuzeigen.

In der erweiterten Ansicht wird in der ersten Tabellenspalte der **Common Name** des CA-Zertifikats angezeigt. Mit den Schaltflächen in der letzten Spalte können Sie die Einstellungen für ein vorhandenes CA-Zertifikat einsehen oder ein CA-Zertifikat als vertrauenswürdig kennzeichnen. Dadurch wird es in die Liste unter **Zertifikatsverwaltung** > **Proxy-CAs** > **Vertrauenswürdige CAs** verschoben. Benutzerdefinierte CA-Zertifikate können Sie auch löschen.

Weitere Informationen finden Sie unter *Symbole und Schaltflächen* auf Seite 28.

Über die Option **Nur benutzerdefinierte CAs anzeigen** können Sie die angezeigte Liste auf die von Ihnen hinzugefügten Certificate Authorities reduzieren.

3.4.9 Diagnose-Tools

Navigieren Sie zum Menü **Diagnose-Tools**, um Diagnose-Tools zu nutzen, falls Probleme in der Kommunikation zwischen der LANCOM R&S®Unified Firewall und anderen Geräten auftreten.

Nutzen Sie die Diagnose-Tools, um zu prüfen, ob Ihre LANCOM R&S®Unified Firewall mit einem Computer oder einem anderen Gerät mit einer bestimmten Netzwerkadresse kommunizieren kann (`Ping`), oder um den Weg einer Mitteilung durch das Netzwerk zu verfolgen (`Traceroute`).

Um eine diagnostische Analyse zwischen verschiedenen Zonen zu ermöglichen, muss eine Firewall-Regel mit dem ICMP-Protokoll oder der ICMP-Ping-Anwendung in der entsprechenden Richtung aktiv sein.

In den folgenden Abschnitten finden Sie detailliertere Informationen zu Netzwerk-Tools.

3.4.9.1 Ping

Navigieren Sie zu **Diagnose-Tools** > **Ping**, um über den Befehl `ping` zu prüfen, ob Ihre LANCOM R&S®Unified Firewall mit einem Computer oder einem anderen Gerät mit einer bestimmten Netzwerkadresse kommunizieren kann.

Ping ist ein Diagnose-Tool, das dauerhaft ein Ping-Signal an ein Ziel sendet, um zu prüfen, ob dieses Ziel Daten empfangen kann. Mit dem Ping-Befehl können Sie Kommunikationsprobleme beheben, indem Sie die Konnektivität zwischen Ihrer LANCOM R&S®Unified Firewall und dem Remote-Gerät prüfen.

Im Bearbeitungsfenster **Ping** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Ziel	Geben Sie eine gültige Netzwerkadresse ein, die Sie mithilfe eines Ping-Befehls prüfen möchten.
Anzahl Anfragen	Geben Sie die Anzahl der ICMP-Echo-Request-Pakete an, die an das Ziel gesendet werden sollen. Hierfür können Sie eine ganze Zahl von `1` bis `10` aus der Drop-down-Liste auswählen. Voreingestellt sind `4` Anfragen.

Klicken Sie auf **Starten**, um den Ping zu starten. Im Bereich **Ausgabe** wird der Ausgang des `Ping`– Befehls angezeigt. Wenn das andere Gerät auf den Ping antwortet, kann Ihre LANCOM R&S®Unified Firewall das Gerät erreichen.

Mit der Schaltfläche **Schließen** unten in dem Fenster können Sie das Fenster schließen und zur kompletten Übersicht Ihres gesamten konfigurierten Netzwerks zurückkehren.

3.4.9.2 Traceroute

Navigieren Sie zu **Diagnose-Tools** > **Traceroute**, um den Befehl `traceroute` zu nutzen, um den Weg einer Mitteilung durch das Netzwerk zu verfolgen.

Von Ihrer LANCOM R&S®Unified Firewall gesendete Pakete können auf dem Weg zu ihrem endgültigen Ziel mehrere andere Geräte durchlaufen. Dies kann das genaue Orten eines Verbindungsproblems erschweren. Mithilfe des `traceroute`-Befehls können Sie die Route verfolgen, die Pakete von Ihrer LANCOM R&S®Unified Firewall bis zu einem bestimmten Host einschlagen.

Mit den **Traceroute**-Einstellungen können Sie die folgenden **Parameter** konfigurieren:

Eingabefeld	Beschreibung
Ziel	Geben Sie die IP-Adresse des endgültigen Ziel ein.
Max. Anzahl Hops	Geben Sie die maximale Anzahl von Knoten (Router oder andere Geräte) an, die auf dem Weg zum Ziel durchlaufen werden. Die Anzahl ist standardmäßig auf `30` gesetzt, Sie können jedoch eine beliebige ganze Zahl von `1` bis `255` eintragen. Falls das Ziel vor dieser Grenze nicht erreicht wird, werden die Testpakete verworfen.

Klicken Sie auf **Starten**, um Tracerouting zu starten. Die Liste der auf dem Weg durchlaufenen Gateways wird im Bereich **Ausgabe** angezeigt.

Mit der Schaltfläche **Schließen** unten in dem Fenster können Sie das Fenster schließen und zur kompletten Übersicht Ihres gesamten konfigurierten Netzwerks zurückkehren.