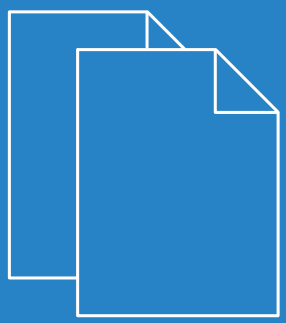
SICHER. **VERNETZT.**

LCOS FX 10.5

Addendum



01/2021

LANCOM Systems

Inhalt

Copyright

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Würselen

Deutschland

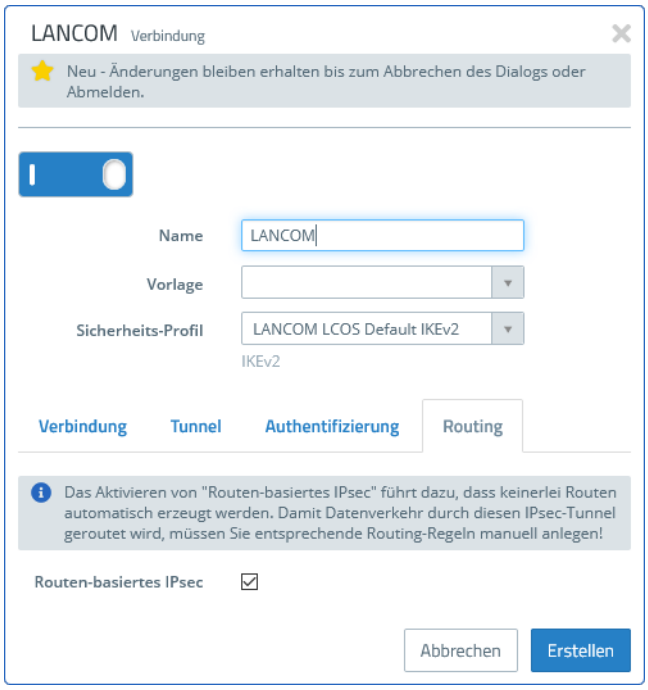
www.lancom-systems.de

1 Addendum zur LCOS FX-Version 10.5

Dieses Dokument beschreibt die Änderungen und Ergänzungen in der LCOS FX-Version 10.5 gegenüber der vorherigen Version.

2 Routen-basiertes IPSec

Ab LCOS FX-Version 10.5 RU3 kann für IPSec-Verbindungen unterhalb von **VPN** > **IPsec** > **Verbindungen** auf dem neuen Reiter **Routing** die Funktion „Routen-basiertes IPsec" aktiviert bzw. deaktiviert werden.



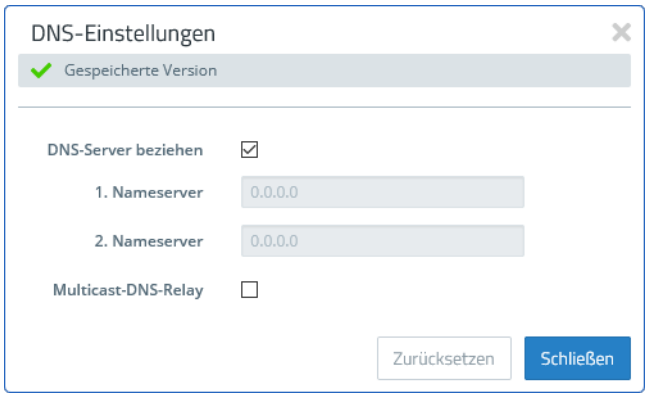
Im Tab **Routing** können Sie diese Einstellung vornehmen:

Tabelle 1: 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.

3 Multicast-DNS-Relay

Ab LCOS FX-Version 10.5 RU3 kann die LANCOM R&S®Unified Firewall als Multicast-DNS-Relay verwendet werden. Dazu wurde in den DNS-Einstellungen unter **Netzwerk** > **DNS-Einstellungen** die Möglichkeit hinzugefügt, das Multicast-DNS-Relay zu aktivieren.

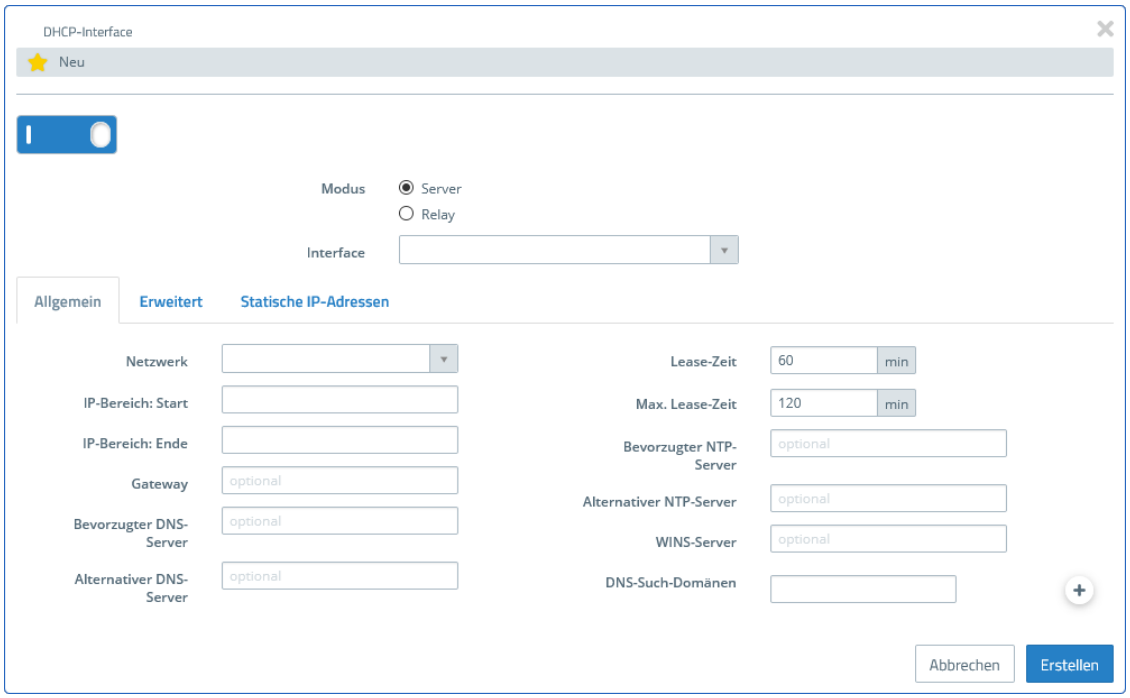


Eingabefeld	Beschreibung
Multicast-DNS-Relay	Aktivieren Sie hier das Multicast-DNS-Relay. Multicast-DNS (mDNS) ist eine Alternative zum herkömmlichen DNS, um Hostnamen in (kleinen) Netzwerken aufzulösen. Dabei wird statt bei einem Server die Namensauflösung anzufragen, eine Anfrage per Multicast an alle 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.

4 DHCP-Interfaces

Ab LCOS FX-Version 10.5 RU3 wurden die DHCP-Einstellungen, die es in den vorangegangen Versionen erlaubten, in einem Dialog das DHCP für alle Interfaces zu konfigurieren, ersetzt und um weitere Einstellungsmöglichkeiten erweitert.

Es existieren keine globalen Einstellungen mehr, wie z.B. der DHCP-Modus (Server, Relay). Stattdessen kann pro Interface bestimmt werden, welche Einstellungen gültig sind. Mit Klick auf den Menüpunkt **Netzwerk** > **DHCP-Interfaces** öffnet sich nicht mehr ein Dialog, sondern die DHCP-Interfaces-Liste, in der Sie neue Interfaces hinzufügen oder bestehende bearbeiten können.



4.1 Einstellungen für 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.
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*. ⓘ 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.

Eingabefeld	Beschreibung
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*. Wenn Sie einen Eintrag bearbeiten, erscheint auf der rechten Seite des Eintrags ein Haken. Klicken Sie auf den Haken, um Ihre Änderungen zu übernehmen.
Aus dem ARP-Cache hinzufügen	Wählen Sie aus der Drop-down-Liste die Adressen aus, die Sie aus dem ARP-Cache hinzufügen möchten.

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.

5 Infobereich

Der Infobereich befindet sich auf der rechten Seite des Desktops.

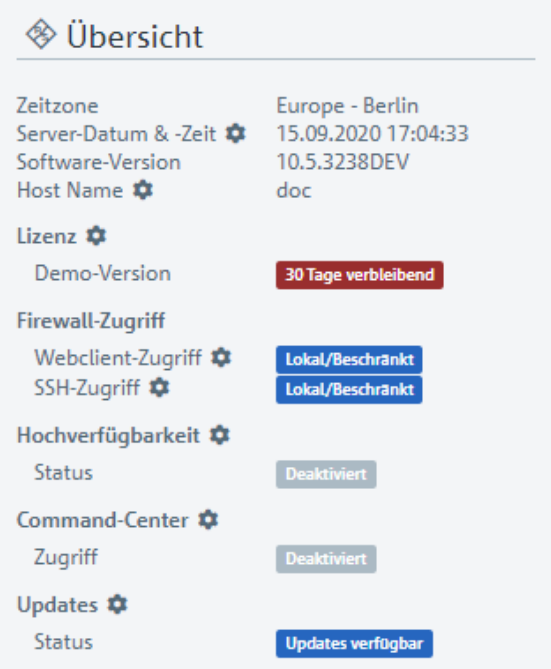


Abbildung 1: Infobereich des LANCOM R&S®Unified Firewall-Webclients

Ab LCOS FX-Version 10.5 RU2 können Sie Einträge mit ⚙ anklicken, um einen dazu passenden Einstellungsdialog zu öffnen.

6 Management-Bericht

Ab LCOS FX-Version 10.5 RU2 wird die Funktion **Desktop** > **Exportieren** durch die im folgenden beschriebene Funktion ersetzt und erweitert.

Navigieren Sie zu **Firewall** > **Management-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 und HTML wählen, indem Sie die entsprechende Optionsschaltfläche auswählen.

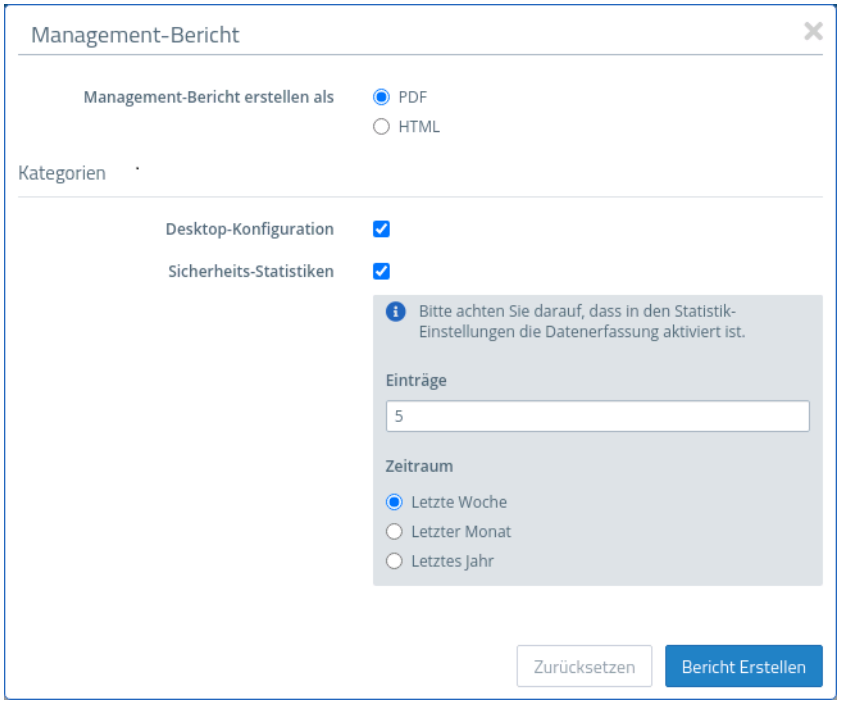


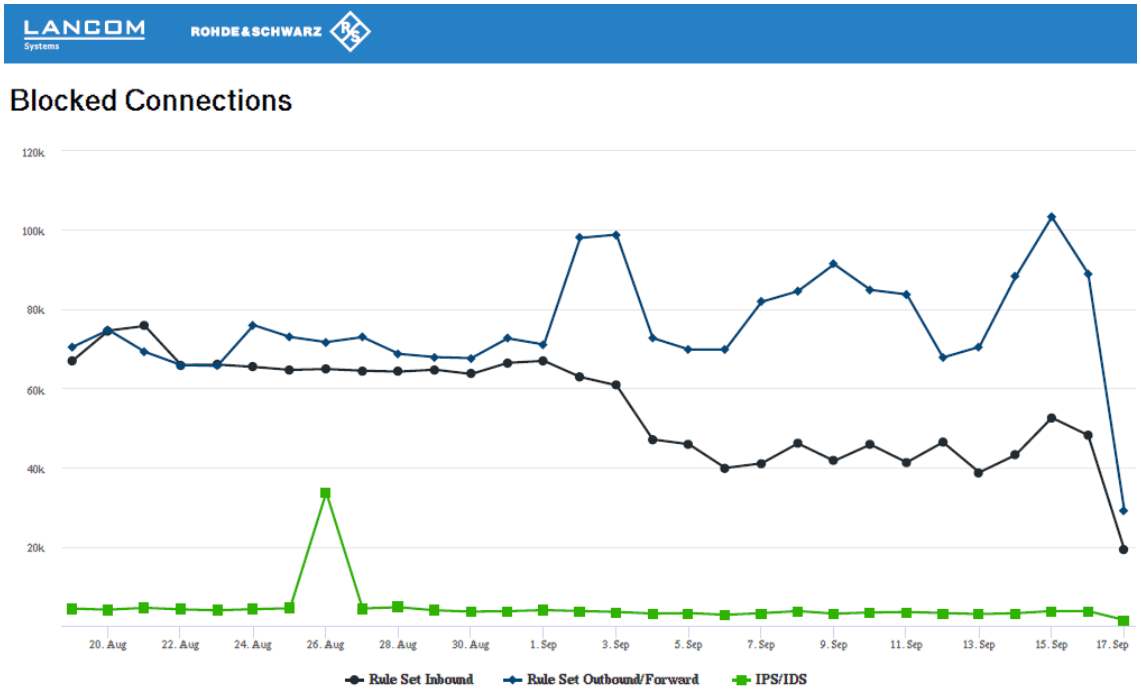
Abbildung 2: Management-Bericht – Einstellungen für den Bericht

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

Eingabefeld	Beschreibung
Desktop-Konfiguration	Die Exportdatei enthält ein Abbild des aktuellen Desktops und 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:

Eingabefeld	Beschreibung
	› 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) › 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.

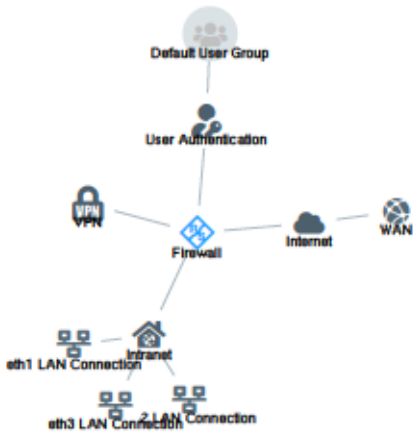


Date	Rule Set Inbound	Rule Set Outbound/Forward	IPS/IDS
17. Sep	19272	29097	1559
16. Sep	48169	88978	3784
15. Sep	52570	103212	3815
14. Sep	43177	88127	3261
13. Sep	38790	70447	3052

Abbildung 3: Beispiel aus einem Management-Bericht

LANCOM Systems ROHDE&SCHWARZ

Desktop Configuration



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 4: Beispiel aus einem Management-Bericht

7 HTTP(S)-Proxy Whitelists

Mit der LCOS FX-Version 10.5 RU2 wurden die Whitelists beim HTTP(S)-Proxy von der bisherigen flachen Liste mit Domains in eine auf Domaingruppen basierenden URL-Listen geändert. Somit können einzelne Gruppen von Domains schnell verboten bzw. erlaubt werden.

Die Domaingruppen können Sie unter **UTM** > **Proxy** > **HTTP-Proxy-Einstellungen** bearbeiten.

Eingabefeld	Beschreibung
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. ⓘ 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.

8 Wiederherstellungspunkte

Mit der LCOS FX-Version 10.4 RU3 wurden die LANCOM R&S®Unified Firewalls für die Wiederherstellungs-Funktionalität vorbereitet. Dadurch wird direkt vor einem Upgrade auf die LCOS FX-Version 10.5 erstmals ein Wiederherstellungspunkt der aktuellen Version (10.4 RU3) erzeugt.

Die Wiederherstellungspunkte können über das System-Menü angezeigt und bei Bedarf ausgeführt werden.

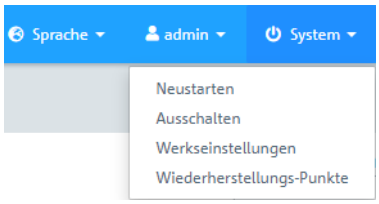


Abbildung 5: System-Menü mit Wiederherstellungspunkten

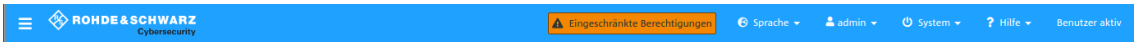
Die Wiederherstellung ist auch bei aktivierter Hochverfügbarkeit möglich, hat aber die Einschränkung, dass lediglich die Hauptfirewall wiederhergestellt wird. Die Ersatzfirewall ist nicht mehr verwendbar und muss neu aufgesetzt werden.

9 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. 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.

10 Desktop-Suche

Ab LCOS FX-Version 10.5 wurde der Desktop-Tags-Filter erweitert zum Desktop-Filter. In dem Eingabefeld wird nun **Filter** statt des vorherigen **Tags** angezeigt.

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 Filterkriterien 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.

11 IMAP-Proxy

Ab LCOS FX-Version 10.5 steht die komplette E-Mail Sicherheit auch für das IMAP Protokoll zur Verfügung. Unterstützt werden sowohl IMAP mit StartTLS als auch IMAPS. Damit können insbesondere auch kleinere Endkunde, die ihre E-Mails nicht selbst hosten, die gewohnte E-Mail Sicherheit mit Antimalware und Antispam vollständig nutzen.

12 Contentfilter-Codes

Die Verwaltung des Contentfilters wurde um Codes erweitert, mit denen Benutzer geblockte Seiten innerhalb bestimmter Zeiten durch Eingabe des jeweiligen Codes trotz des Filters ansehen können. Für diese Änderung wurden Einstellungen für URL- / Contentfilter angepasst. Unter **UTM** > **URL-/Contentfilter** > **Settings** kann nun der Ausnahme-Modus eingestellt werden und die neue Option **Ausnahme nur mit Code erlauben** verwendet werden.

Eingabefeld	Beschreibung
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. 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. Dies können entweder aus Sicht Ihrer LANCOM R&S®Unified Firewall lokale Benutzer, LDAP-Benutzer oder auch LDAP-Gruppen sein.

In der Übersicht der URL- / Contentfilter unter **UTM** > **URL-/Contentfilter** > **URL-/Contentfilter** können Sie dann die jeweiligen Profile bearbeiten. Hierbei hat die Option **Überschreiben durch Benutzer** abhängig von obiger Einstellung eine geänderte Bedeutung.

Eingabefeld	Beschreibung
Überschreiben durch Benutzer	Setzen Sie dieses Häkchen, um ein Contentfilterprofil als überschreibbar zu markieren. Abhängig von Ihren Einstellungen wird ggf. alternativ ein Code benötigt. Näheres zur Verwaltung der Codes finden Sie unter *URL- / Contentfilter-Codes managen* auf Seite 20. Diese Option ist nur für Profile verfügbar, die keine Standardprofile sind.

12.1 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 hierzu den Abschnitt „Benutzerauthentifizierung" im Benutzerhandbuch.

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.

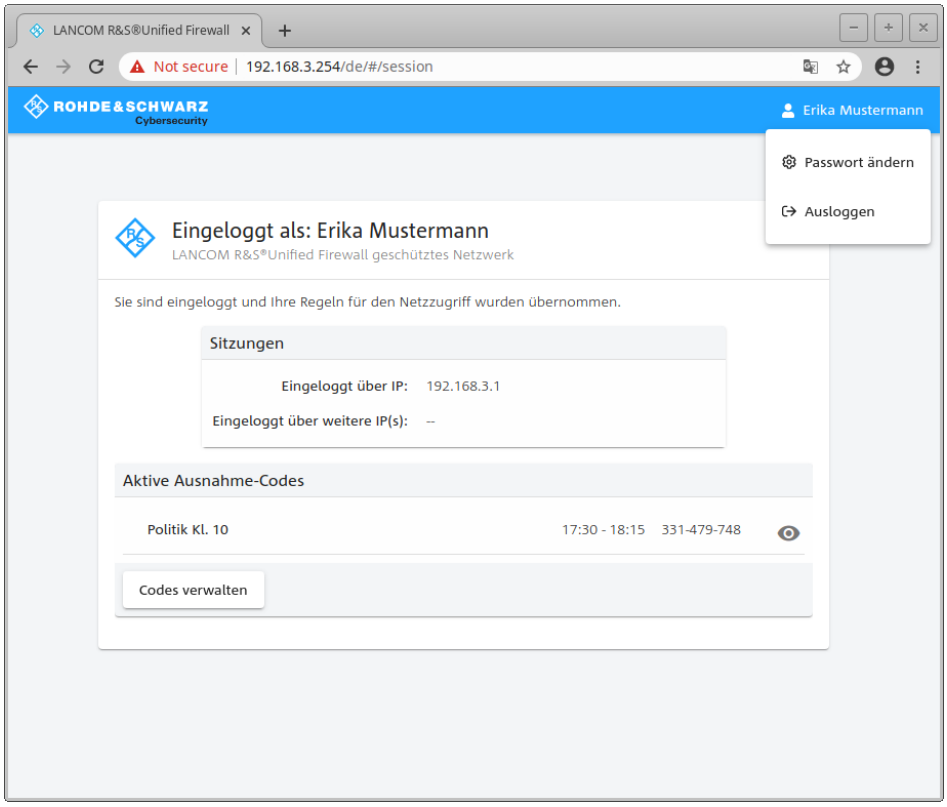


Abbildung 6: Ausnahme-Code: Einstieg in die Verwaltung

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.

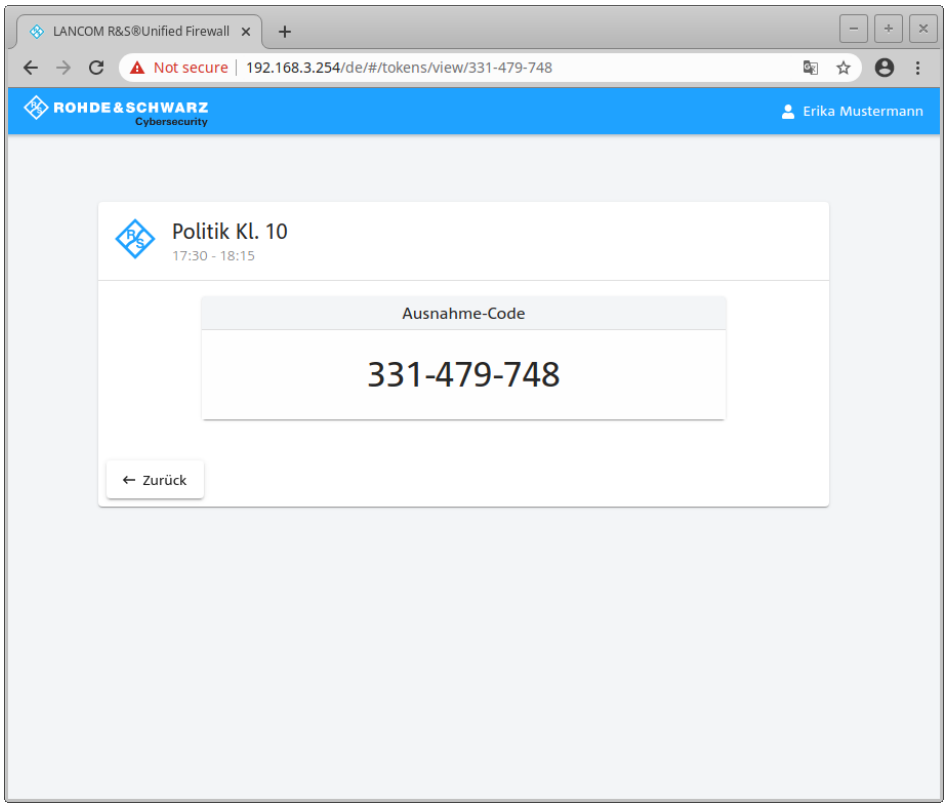


Abbildung 7: Ausnahme-Code: Präsentationsmodus

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.

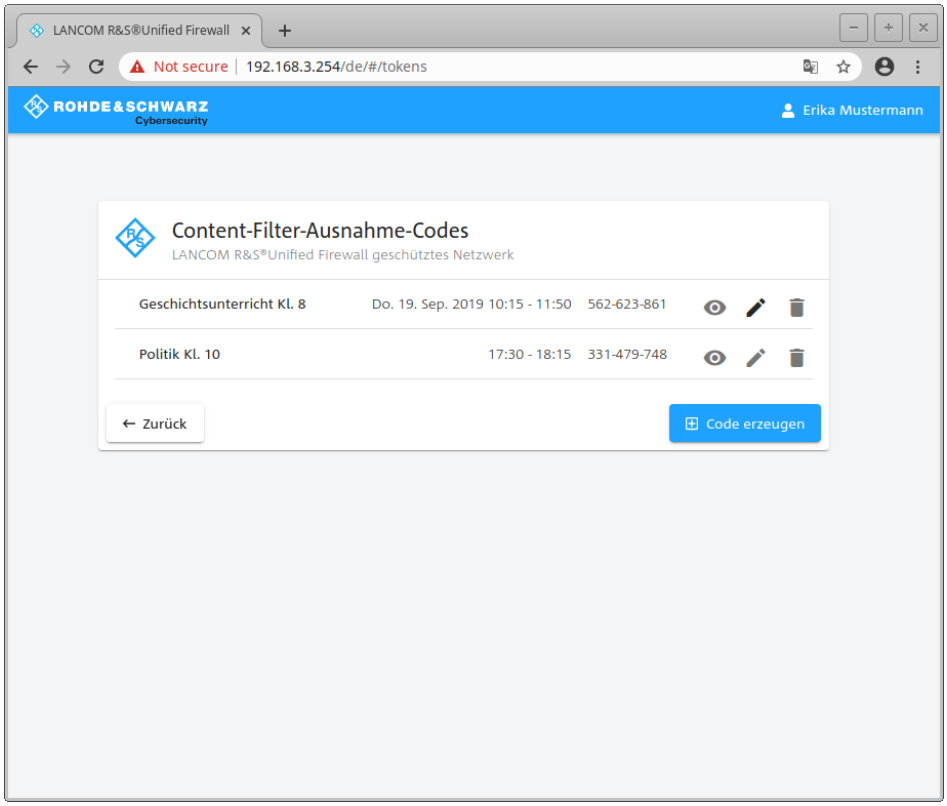


Abbildung 8: Ausnahme-Code: Managementmodus

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.

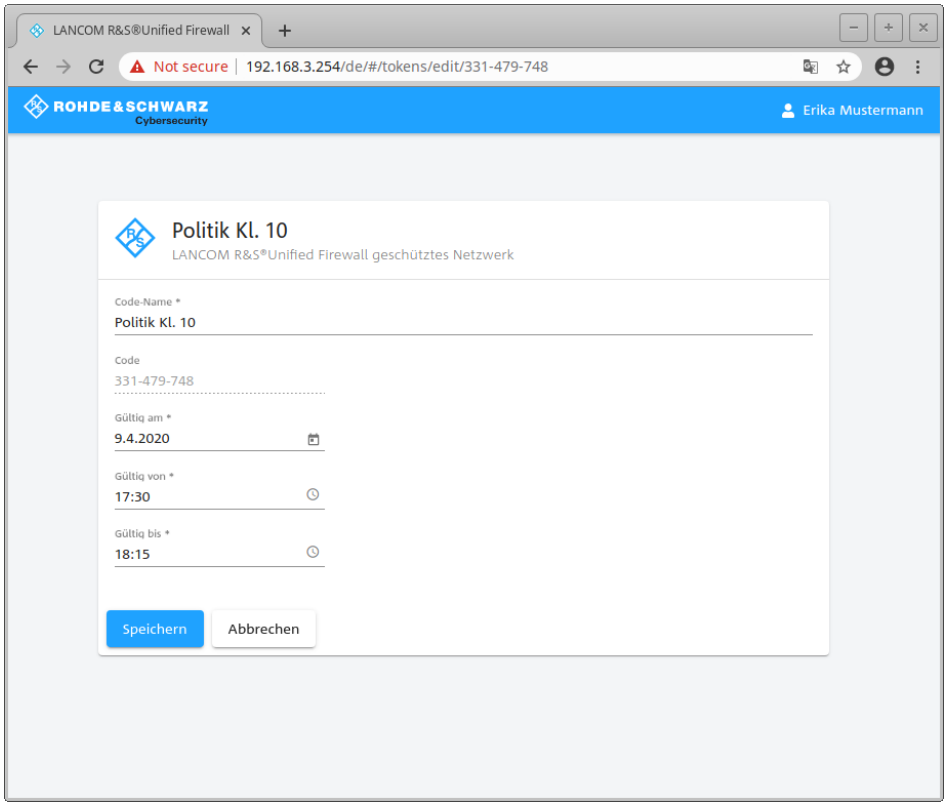


Abbildung 9: Ausnahme-Code: Code erzeugen

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.

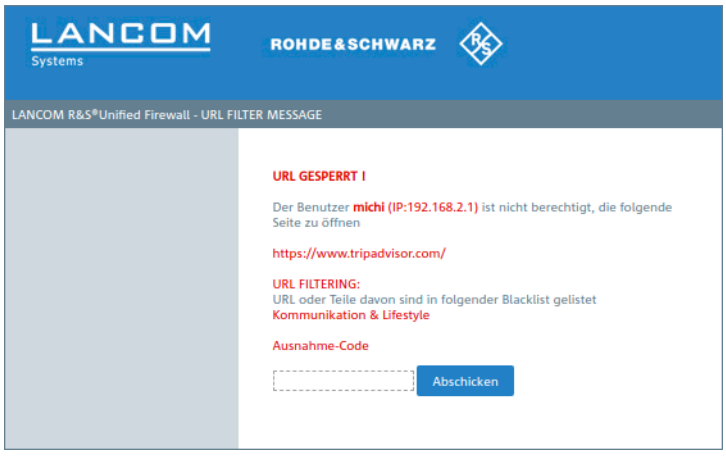


Abbildung 10: Ausnahme-Code: Meldung über gesperrte Seite

13 Application Based Routing

Ab LCOS FX-Version 10.5 steht Ihnen für Verbindungen das Application Based Routing zur Verfügung. Der Bereich Application-Filter wurde dazu in Application-Management umbenannt und um Routing-Profile erweitert.

Wie bei den Application-Filter-Profilen werden die Routing-Profile in den Desktop-Verbindungen verwendet. Der Verbindungs-Dialog wurde um den Tab „Application Based Routing" erweitert, in dem die konfigurierten Routing-Profile über die Liste zur Rechten hinzugefügt werden können.

Für die Routing-Profile existiert im Gegensatz zu den Filter-Profilen keine Modus-Einstellung.

13.1 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.

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.
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.
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.

14 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.

15 VPN-SSL-Bridging

Ab LCOS FX-Version 10.5 ist es möglich, bei VPN-SSL den Bridging-Modus zu verwenden. Dazu wurde der VPN-SSL-Einstellungsdialog unter **VPN** > **VPN-SSL** > **VPN-SSL-Einstellungen** um einen Bridging-Tab erweitert.

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.
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.
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: Entfernen Sie dieses Häkchen, um LZO (Lempel-Ziv-Oberhumer, ein Algorithmus für verlustfreie Datenkompression) zu deaktivieren. Dieses Kontrollkästchen ist standardmäßig aktiviert.

Unter **VPN** > **VPN-SSL** > **VPN-SSL-Verbindungen** können Sie eine VPN-SSL-Verbindung hinzufügen, oder eine vorhandene Verbindung bearbeiten. In den Einstellungen unter **VPN-SSL-Verbindungen** sind die folgenden Elemente für Bridging hinzugekommen:

Eingabefeld	Beschreibung
Verbindungstyp	Wählen Sie den Typ der Verbindung und die Funktion der LANCOM R&S®Unified Firewall aus, indem Sie die entsprechende Optionsschaltfläche auswählen. Ab LCOS FX-Version 10.5 können Sie zusätzlich aus den folgenden Typen auswählen: › **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 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 Bridge-Server-Verbindungen können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Bridge	Wählen Sie eine Bridge aus den vorkonfigurierten Bridges aus.

Bei Bridge-Client-Verbindungen können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Bridge	Wählen Sie eine Bridge aus den vorkonfigurierten Bridges aus.
Remote-Adressen	Geben Sie die IP-Adresse ein, unter der das entfernte Verbindungsende erreichbar ist. Klicken Sie auf **Hinzufügen**, um eine IP-Adresse 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. 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.

16 Benutzerauthentifizierung

Ab LCOS FX-Version 10.5 RU1 wurde der Benutzerauthentifizierung ein extern erreichbares Portal hinzugefügt, in dem VPN-Profile für den LANCOM Advanced VPN Client zur Verfügung gestellt werden können. Zu diesem Zweck wurde die Benutzerauthentifizierung im Menü eine Ebene höher angesiedelt und die bisherigen Einstellungen in die Bereiche **Benutzerauthentifizierung** > **LDAP/AD** sowie **Benutzerauthentifizierung** > **Internes Portal** verlegt. Neben dem neuen Bereich **Benutzerauthentifizierung** > **Externes Portal** gibt es darüber hinaus die neu hinzugekommene Möglichkeit, Geräte eines Benutzers bei einer Anmeldung mittels Wake-on-LAN-Paket zu starten.

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.

16.1 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.

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. Sowohl Microsoft Active Directory als auch openLDAP verwenden das Protokoll Kerberos für die Verifizierung aller Login-Daten, die von Benutzerauthentifizierungs-Clients bereitgestellt werden.

Active Directory-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.

16.2 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.

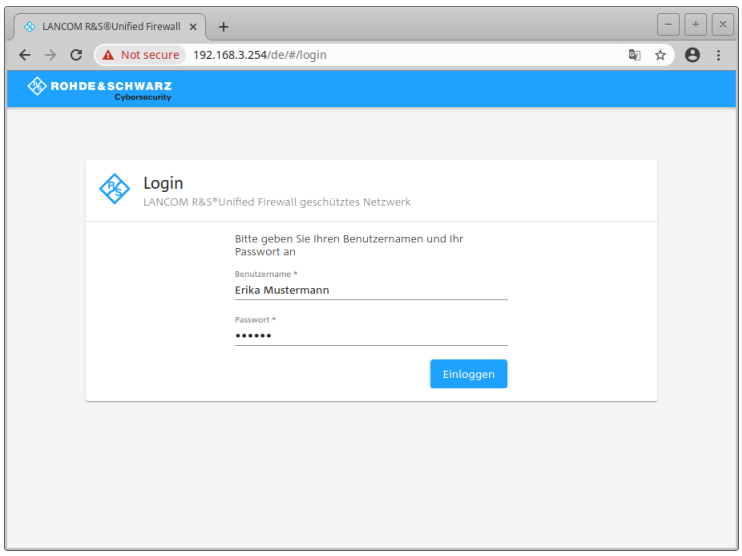


Abbildung 11: Benutzerauthentifizierung über einen Webbrowser

4. 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.

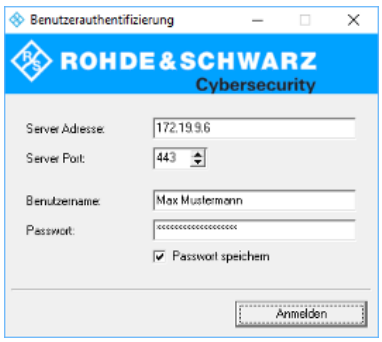


Abbildung 12: LANCOM R&S®Unified Firewall Benutzerauthentifizierungs-Client

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.

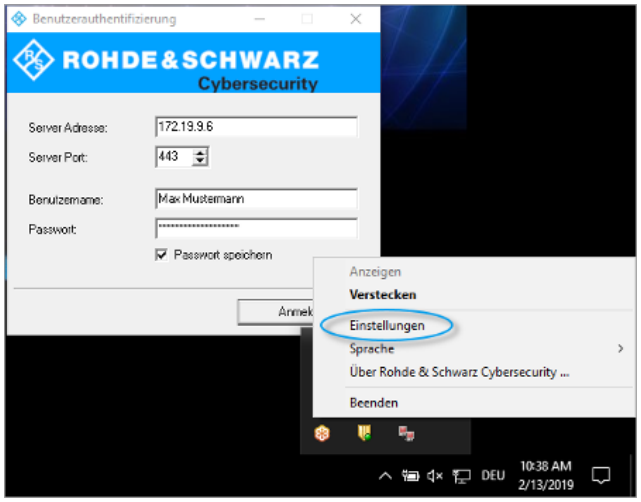


Abbildung 13: LANCOM R&S®Unified Firewall Benutzerauthentifizierungs-Client-Einstellungen

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 41.

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.

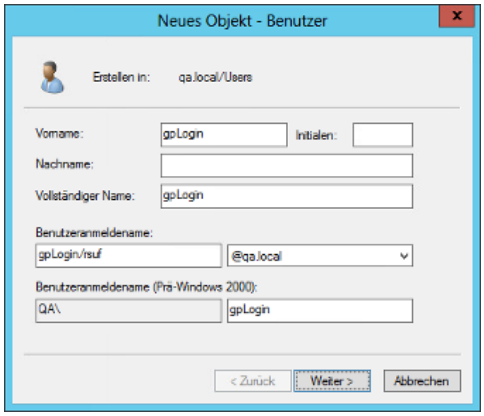


Abbildung 14: Benutzer anlegen

   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 15: 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 41).
- 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`.

16.3 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

Eingabefeld	Beschreibung
	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 35.
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.

Eingabefeld	Beschreibung
Group-Query	Optional: Geben Sie den Filter an, der verwendet werden soll, um die Liste der Gruppen abzurufen.
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. Weitere Informationen finden Sie unter *Einloggen* auf Seite 32.

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 32.

16.4 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.

16.4.1 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.
Verbindung	Wählen Sie eine Verbindung aus. Sie können sowohl eine Netzwerkverbindung als auch eine PPP-Verbindung auswählen.
Port	Konfigurieren Sie den extern erreichbaren Listen-Port für das externe Portal.
SSL-Zertifikat	Wählen Sie ein Zertifikat mit einem privaten Schlüssel aus.

16.4.2 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.

16.5 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.

16.5.1 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. Indem Sie dieses Kontrollkästchen aktivieren, bringen Sie ihre Netzwerksicherheit in Gefahr. Weitere Informationen finden Sie unter *Benutzerauthentifizierung* auf Seite 31.
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.

16.5.2 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.

16.6 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.

16.7 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 37 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.

16.8 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 37 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.

16.9 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.

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.

16.10 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.

16.11 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**.

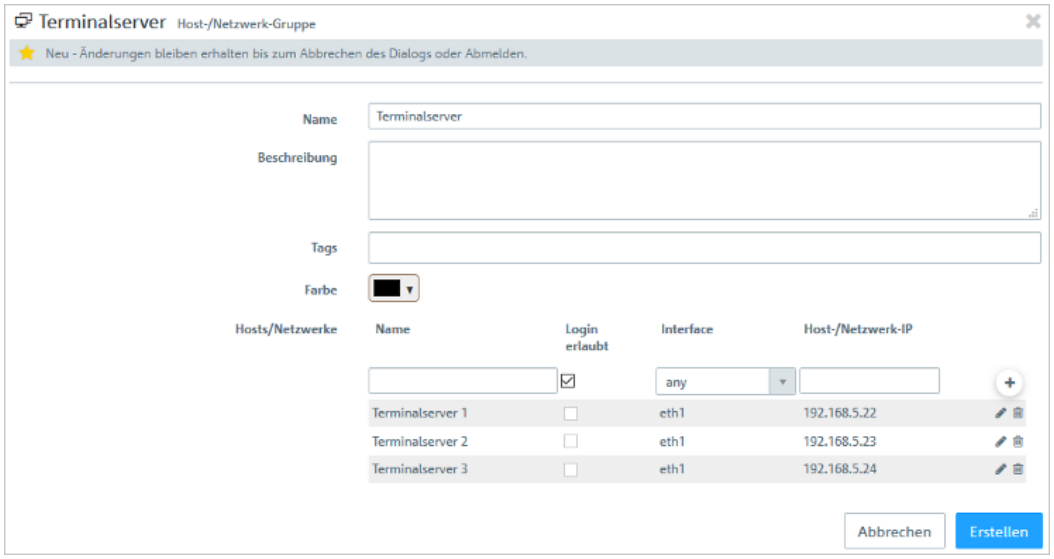


Abbildung 16: Objekteinstellungen – Terminalserver

Falls Ihre Benutzer eine Authentifizierung im Terminalserver benötigen, können Sie Remotedesktop-IP-Virtualisierung im Terminalserver aktivieren. Hierdurch wird allen Benutzern während einer Sitzung eine eigene IP-Adresse zugewiesen.