

LCOS FX 11.1

Addendum

06/2025



LANCOM
SYSTEMS

Inhalt

1 Addendum zur LCOS FX-Version 11.1.....	4
2 REST-API-Dokumentation.....	5
3 TFTP.....	7
4 Ping-Einstellungen.....	8
5 IPv6.....	9
6 Traffic Shaping.....	11
7 Host- und Netzwerk-Objekt-Referenzen in Hostgruppen-Objekten.....	12
8 Quell-Ports bei benutzerdefinierten Diensten.....	13
9 Protokolle.....	14
9.1 Benutzerdefinierte Protokolle.....	14
10 Reverse Proxy.....	16
11 TCP-Load-Balancer.....	18
12 Externes Portal.....	20
13 SAML / Single Sign-On.....	22
13.1 SAML / Single Sign-On (Internes Portal).....	22
13.2 SAML / Single Sign-On (Externes Portal).....	27
14 Let's Encrypt-Server.....	30
15 Änderungen bei Antivirus.....	31
16 Fortgeschrittene Einstellungen.....	32

Copyright

© 2025 LANCOM Systems GmbH, Würselen (Germany). Alle Rechte vorbehalten.

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.

Weitergabe und Vervielfältigung der zu diesem Produkt gehörenden Dokumentation und Software und die Verwendung ihres Inhaltes sind nur mit schriftlicher Erlaubnis von LANCOM Systems gestattet. Änderungen, die dem technischen Fortschritt dienen, bleiben vorbehalten.

Windows® und Microsoft® sind eingetragene Marken von Microsoft, Corp.

LANCOM, LANCOM Systems, LCOS, LANcommunity, LANCOM Service LANcare, LANCOM Active Radio Control und AirLancer sind eingetragene Marken. Alle anderen verwendeten Namen und Bezeichnungen können Marken oder eingetragene Marken ihrer jeweiligen Eigentümer sein. Dieses Dokument enthält zukunftsbezogene Aussagen zu Produkten und Produkteigenschaften. LANCOM Systems behält sich vor, diese jederzeit ohne Angaben von Gründen zu ändern. Keine Gewähr für technische Ungenauigkeiten und / oder Auslassungen.

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 (ey@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

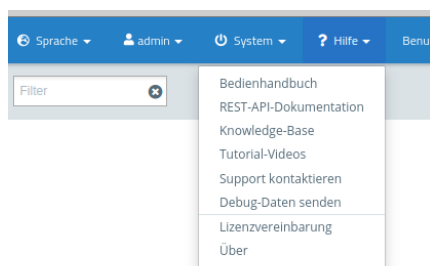
www.lancom-systems.de

1 Addendum zur LCOS FX-Version 11.1

Dieses Dokument beschreibt die Änderungen und Ergänzungen in der LCOS FX-Version 11.1 gegenüber der vorherigen Version.

2 REST-API-Dokumentation

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

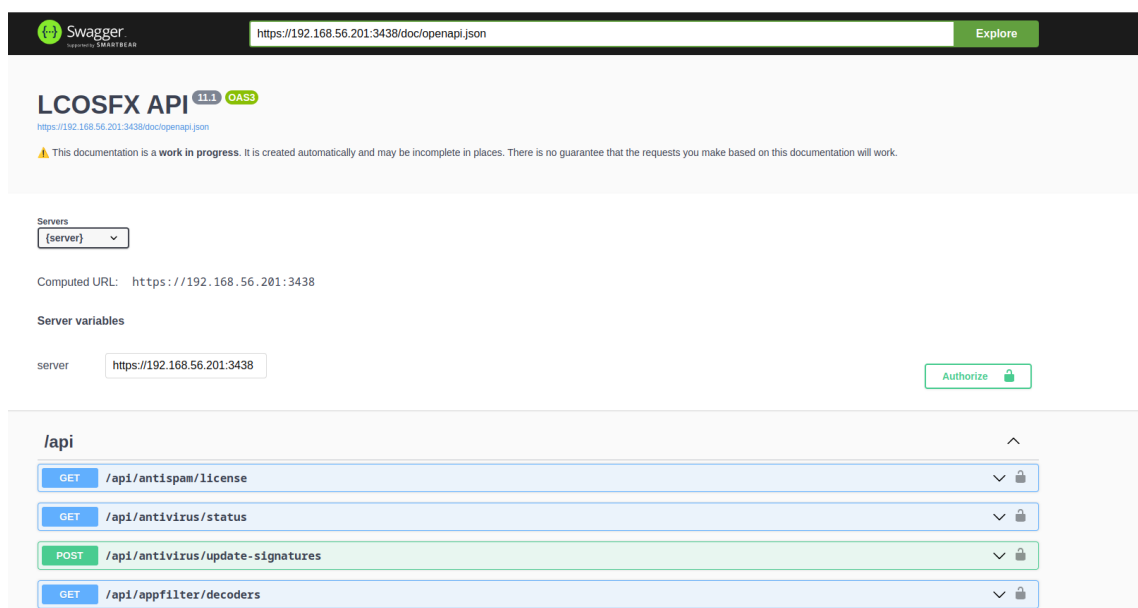


Die Dokumentation wird in einem separaten Tab geöffnet mit der derzeit verwendeten Adresse für den Web-Client-Zugriff als Server.



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 erfolgreichen 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.

server Authorize

/api

Docker

Authentication

POST /auth/login Admin login

On first login, `newAdminPassword` and `newConsolePassword` are required.

Parameters Try it out

No parameters

Request body required application/json

Example Value | Schema

```
{
  "username": "string",
  "password": "string",
  "eulaAccepted": true,
  "newAdminPassword": "string",
  "newConsolePassword": "string"
}
```

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

Swagger Explore

LCOSFX API 11.1 OAS3

<https://192.168.56.201:3438/doc/openapi.json>

⚠ This documentation is a **work in progress**. It is created automatically and may be incomplete in places. There is no guarantee that the requests you make based on this documentation will work.

Servers {server}

Computed URL: `https://192.168.56.201:3438`

Server variables

server Authorize

Available authorizations x

TokenAuth (apiKey)

Name: X-Gateprotect-Auth-Token

In: header

Value:

Authorize Close

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

3 TFTP

Ab LCOS FX 11.1 wurde eine neue Option hinzugefügt, mit welcher der Zugriff auf die Firewall per TFTP erlaubt oder verboten werden kann.

The screenshot shows the 'Allgemeine Einstellungen' (General Settings) window. At the top, there is a status bar with a green checkmark and the text 'Gespeicherte Version'. Below this, the 'Hostname' field is set to 'master' and the 'Domain' field is set to 'branch'. There are three main sections with checkboxes: 'Nutzungs-Statistiken senden' (unchecked), 'Diagnoseberichte senden' (checked), and 'TFTP' (checked). The TFTP checkbox is labeled 'TFTP-Server für den sysinfo-Zugriff aktivieren (Nur LAN)'. At the bottom right, there are two buttons: 'Zurücksetzen' (Reset) and 'Schließen' (Close).

Abbildung 1: Firewall > Allgemeine Einstellungen

Eingabefeld	Beschreibung
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.

4 Ping-Einstellungen

Ab LCOS FX 11.1 wird unter **Firewall > Firewall-Zugriff > Ping-Einstellungen** zwischen IPv4- und IPv6-Ping unterschieden.

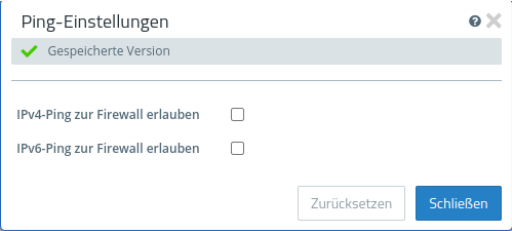






Abbildung 2: Firewall > Firewall-Zugriff > Ping-Einstellungen

Eingabefeld	Beschreibung
IPv4-Ping zur Firewall erlauben IPv6-Ping zur Firewall erlauben	<p>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.</p> <ul style="list-style-type: none">> „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. <div><div>!</div><p>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.</p></div>

5 IPv6

Ab LCOS FX 11.1 gibt es eine (eingeschränkte) Unterstützung von IPv6. IPsec-Verbindungen können nun auf Basis von IPv6 erstellt werden. Dazu wurden unter **Netzwerk > Verbindungen > Netzwerk-Verbindungen** zwei neue Verbindungstypen in den hinzugefügt: **Static IPv6** und **DHCPv6**.

Abbildung 3: Netzwerk > Verbindungen > Netzwerk-Verbindungen

Eingabefeld	Beschreibung
Typ	<p>Wählen Sie den Verbindungstyp aus der Drop-down-Liste aus. Diese Option ist standardmäßig auf <code>Static</code> gesetzt, Sie können die Einstellungen jedoch bei Bedarf auf einen der anderen Werte setzen:</p> <ul style="list-style-type: none"> > Static IPv4 – In diesem Modus wird eine statische IPv4-Adresse für die Verbindung festgelegt. > DHCPv4 – In diesem Modus werden IPv4-Adressen dynamisch zugewiesen. > Static IPv6 – In diesem Modus wird eine statische IPv6-Adresse für die Verbindung festgelegt. <p> Diese Verbindungen können nur in IPsec-Verbindungen verwendet werden.</p> <ul style="list-style-type: none"> > DHCPv6 – In diesem Modus werden IPv6-Adressen dynamisch zugewiesen. <p> Diese Verbindungen können nur in IPsec-Verbindungen verwendet werden.</p> <p> Sobald Sie auf Erstellen klicken, um die Netzwerkverbindung herzustellen, kann der Verbindungstyp nicht mehr geändert werden.</p> <p> Die Elemente im Tab Netzwerk hängen vom gewählten Verbindungstyp ab.</p>

i Mit Auswahl einer der beiden Optionen **Static IPv6** oder **DHCPv6**, können in verschiedenen Feldern nur noch IPv6-Werte verwendet werden:

- > **IP-Adressen**
- > **Standard-Gateway**
- > **Heartbeats**

IPsec-Verbindung

In einer IPsec-Verbindung kann die IPv6-Verbindung wie zuvor für IPv4 gewählt oder weggelassen werden.

Abbildung 4: VPN > IPsec > Verbindungen

i Ist keine Verbindung ausgewählt, können unter **Listening-IP-Adressen** und **Remote Gateways** sowohl IPv4- als auch IPv6-Adressen gewählt werden. Anderfalls müssen diese dem Verbindungstypen entsprechen.

i Unter dem Tab **Tunnel** können nur IPv4-Werte, keine IPv6-Werte, verwendet werden.

WireGuard

Die Verbindungen zwischen zwei Peers können nun IPv6 verwenden. Interne IPs sind weiterhin auf IPv4 beschränkt.

Externes Portal

Das Externe Portal kann nun auch über IPv6 erreicht werden.

Reverse Proxy

Reverse-Proxy-Frontends können nun auch über IPv6 erreicht werden und mit IPv6 Reverse-Proxy-Backends kommunizieren.

DNS

Es können IPv6 Adressen als DNS-Server-Adressen angegeben werden.

6 Traffic Shaping

Ab LCOS FX 11.1 können in den **Eingehende Regeln** und **Ausgehende Regeln** von Shaping-Konfigurationen nicht mehr nur Traffic-Gruppen ausgewählt werden, sondern auch Interfaces, auf welches die Regel angewendet werden soll. Dazu wurden unter **Netzwerk > Traffic Shaping > Shaping-Konfigurationen** die entsprechenden Auswahlfelder erweitert.

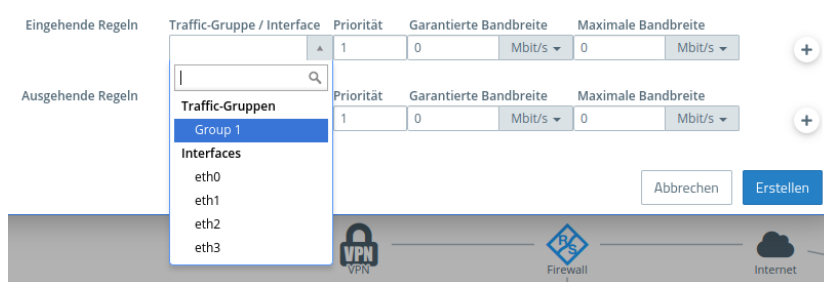


Abbildung 5: Netzwerk > Traffic Shaping > Shaping-Konfigurationen

Eingabefeld	Beschreibung
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.

7 Host- und Netzwerk-Objekt-Referenzen in Hostgruppen-Objekten

Ab LCOS FX 11.1 ist nun möglich in Hostgruppen-Objekten (**Desktop > Desktop-Objekte > Host-/Netzwerk-Gruppen**) bereits erstellte Host- oder Netzwerk-Objekte auszuwählen.

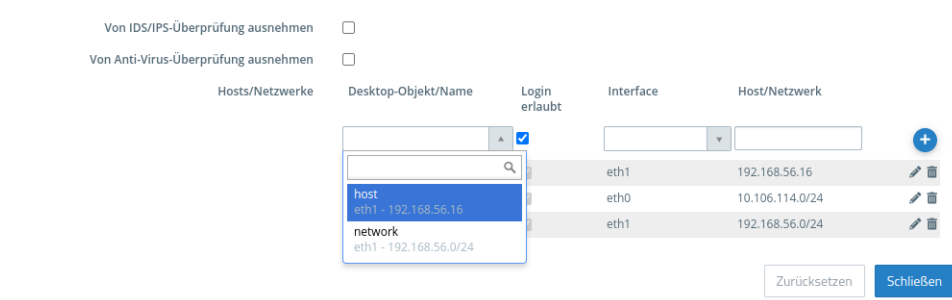



Abbildung 6: Desktop > Desktop-Objekte > Host-/Netzwerk-Gruppen

Bei **Hosts / Netzwerke** wählen Sie nun alternativ 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 Liste hinzugefügt wurde. Im Infobereich werden referenzierte Objekte mit einem  markiert, sie sind somit auch von dort direkt zu bearbeiten.

8 Quell-Ports bei benutzerdefinierten Diensten

Ab LCOS FX 11.1 wird unter **Desktop > Dienste > Benutzerdef. Dienste** die Möglichkeit angeboten, die Quell-Ports zu beschränken. Dazu wurde der Anzeige-Dialog erweitert, um die Quell-Port-Einstellungen anzuzeigen

Abbildung 7: Desktop > Dienste > Benutzerdef. Dienste

Im Bearbeitungsfenster **Benutzerdefinierte Dienste** wurden die Eingabemöglichkeiten erweitert, um ggf. den Quell-Port anzugeben.

Abbildung 8: Bearbeitungsfenster Benutzerdefinierte Dienste

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.

9 Protokolle

Ab LCOS FX 11.1 sind die bisher verfügbaren Protokolle (ICMP, TCP, UDP, GRE, ESP, AH) um drei weitere Protokolle erweitert worden (IGMP, OSPF und VRRP) und ähnlich den Diensten unter **Vordefinierte Protokolle** zusammengefasst worden.

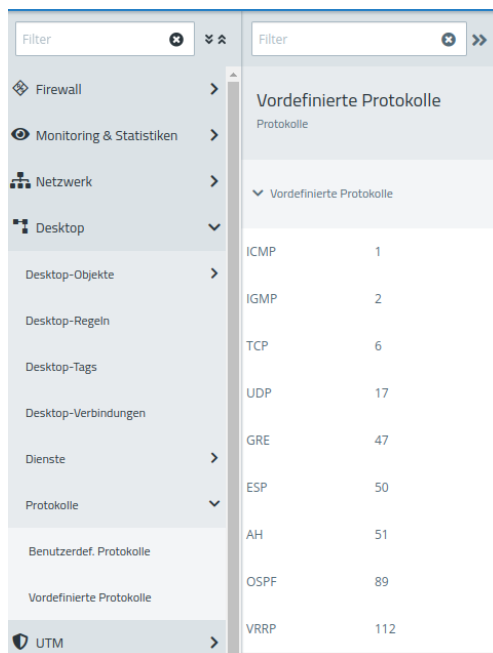


Abbildung 9: Desktop > Protokolle > Vordefinierte Protokolle

Unter **Benutzerdefinierte Protokolle** können weitere Protokolle bzw. Protokollnummern hinzugefügt werden.

9.1 Benutzerdefinierte Protokolle

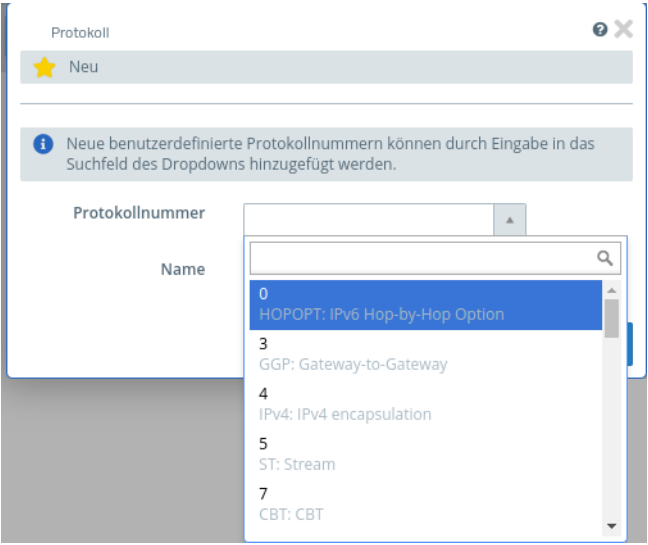
Wenn Sie einen Port oder ein Protokoll benötigen, das nicht von einem der vordefinierten Protokolle abgedeckt ist, können Sie ein benutzerdefiniertes Protokoll erstellen, das bei einem Dienst verwendet werden kann.

Navigieren Sie zu **Desktop > Protokolle > Benutzerdefinierte Protokolle**, um die Liste der im System angelegten benutzerdefinierten Protokolle in der Objektliste anzuzeigen.

Hier können Sie ein neues benutzerdefiniertes Protokoll hinzufügen oder ein vorhandenes benutzerdefiniertes Protokoll bearbeiten.

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

Eingabefeld	Beschreibung
Protokollnummer	<p>Eine Protokollnummer von 0 bis 255 kann gewählt werden. Die vorgeschlagenen Werte entsprechen denen der IANA.</p> <p>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</p>

Eingabefeld	Beschreibung
	<p>werden als benutzerdefiniertes Protokoll gekennzeichnet und der Name wird nicht automatisch vorausgefüllt.</p>  <p>Abbildung 10: Desktop > Protokolle > Benutzerdefinierte Protokolle</p>
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.

10 Reverse Proxy

Websockets

Ab LCOS FX 11.1 wurde eine **Websocket**-Option zu den Einstellungen der einzelnen Proxy-Pfade eines Reverse-Proxy-Frontends hinzugefügt. Die Option Websocket muss aktiviert sein, damit ein vom Backend bereitgestellter Websocket korrekt über Proxy verwendet werden kann. Für TLS-Websockets müssen sowohl im Frontend als auch im Backend die Option SSL aktiviert sein.

The screenshot shows the 'Reverse-Proxy-Frontend' configuration window with the 'Allgemein' tab selected. At the top, a status bar indicates 'Neu - Änderungen bleiben erhalten bis zum Abbrechen des Dialogs oder Abmelden.' Below this is a toggle switch for the frontend. The configuration fields include: 'Domäne oder IP-Adresse' (text input), 'Verbindung' (dropdown menu), 'Port' (text input with '8080'), 'SSL' (checked checkbox), 'Let's Encrypt verwenden' (unchecked checkbox), 'Zertifikat' (dropdown menu), 'Private-Key-Passwort' (text input), 'HTTP auf HTTPS umleiten' (unchecked checkbox), 'Host-Header bewahren' (unchecked checkbox), 'Proxy-Pfade' (table with 'Backend' and 'URL' columns, showing 'Backend' and '/test'), 'Websocket' (checked checkbox), and 'Blockierte Pfade' (text input). At the bottom are 'Abbrechen' and 'Erstellen' buttons.

Abbildung 11: UTM > Reverse-Proxy > Frontends > Allgemein

Host-Header bewahren

Zudem kann eine neue Option **Host-Header bewahren** gesetzt werden, um den „Host“-HTTP-Header beim Reverse Proxy eingehender HTTP-Anfragen beizubehalten. Je nach Anwendungsszenario kann das An- oder Abschalten dieser Option Probleme in der Kommunikation mit dem Ziel-Server beheben.

Zugangsbeschränkungen für Reverse-Proxy-Frontends

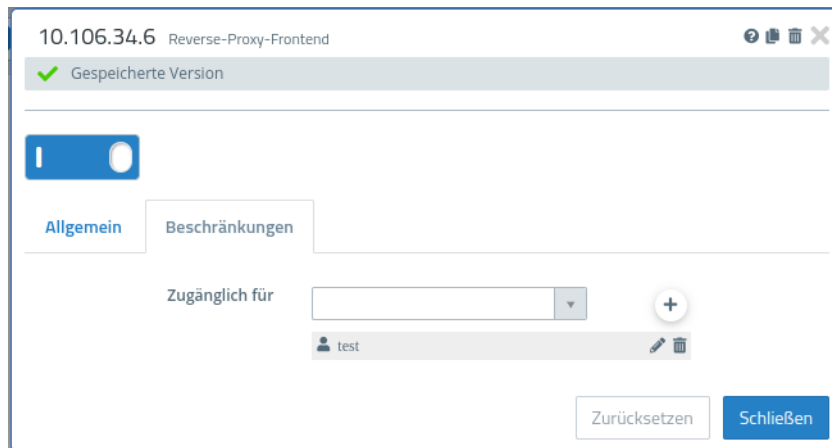


Abbildung 12: UTM > Reverse-Proxy > Frontends > Beschränkungen

Tabelle 1: Beschränkungen

Eingabefeld	Beschreibung
Zugänglich für	<p>Einzelne Reverse-Proxy-Frontends können hier mit Zugangsbeschränkungen versehen werden.</p> <p>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.</p> <p>Sind keine Beschränkungen eingerichtet, kann das Reverse Proxy Frontend ohne vorherige Authentifizierung verwendet werden.</p>

Wireguard

Bei den auswählbaren Verbindungen kann nun auch eine vorher definierte Wireguard-Verbindungen ausgewählt werden.

11 TCP-Load-Balancer

Ab LCOS FX 11.1 RU1 wurde der Reverse Proxy um einen TCP-Load-Balancer erweitert.

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:

0.0.0.0:0 TCP-Load-Balancer

Neu

Modus

roundrobin

Nähere Angaben zu den Modi finden Sie unter <https://docs.haproxy.org/1.8/configuration.html#4.2-balance>.

Adresse

optional

Port

Überprüfungsintervall

3

Sek.

Anzahl fehlgeschlagener Überprüfungen

3

bis der Server als nicht verfügbar angesehen wird.

Anzahl erfolgreicher Überprüfungen

2

bis der Server als verfügbar angesehen wird.

Server

Adresse

Port

Gewicht

1

Abbrechen

Erstellen

Abbildung 13: UTM > Reverse-Proxy > TCP-Load-Balancer

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 fehlgeschlagener Überprüfungen ein Server als nicht verfügbar angesehen wird.

Eingabefeld	Beschreibung
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.

12 Externes Portal

Für die Reverse-Proxy-Authentifizierung werden Cookies verwendet. Damit dieser Cookie unter den korrekten Bedingungen vom Browser an den Server gesendet werden, kann es nötig sein, das `domain`-Attribut des Cookies entsprechend zu setzen. Hierzu wurden die Einstellungen unter **Benutzerauthentifizierung > Externes Portal > Einstellungen** um das Feld **Cookie-Domain für Reverse-Proxy-Authentifizierung** ergänzt.

Externes Portal

Gespeicherte Version

Domäne oder IP-Adresse

Cookie-Domain f.
Reverse-Proxy-Auth.

Verbindung

Port

8080

Let's Encrypt verwenden

☐

SSL-Zertifikat

Private-Key-Passwort

HTTPS-Proxy-CA zum
Download anbieten

☐

Das Zertifikat "LCOS FX Default HTTPS
Proxy CA" kann auf der Login-Seite des
externen Portals heruntergeladen
werden, wenn der HTTPS-Proxy
aktiviert ist.

Hilfe-Link

☒ Standard-Hilfe-Link

☐ Benutzerdefinierter Hilfe-Link

https://support.lancom-
systems.com/knowledge/pages/view
page.action?pageId=32983645


Ändern Sie diesen Link, um
benutzerdefinierte Informationen
anzuzeigen, wie die Proxy-CA installiert
werden kann.

Zurücksetzen

Schließen

Abbildung 14: Benutzerauthentifizierung > Externes Portal > Einstellungen

Eingabefeld	Beschreibung
Cookie-Domain für Reverse-Proxy-Authentifizierung	<p>Für die Reverse-Proxy-Authentifizierung werden Cookies verwendet. Damit diese Cookies unter den korrekten Bedingungen vom Browser an den Server gesendet werden, kann es nötig sein, das <code>domain</code> Attribut des Cookies entsprechend zu setzen.</p> <p>Ist dieses Feld leer, dann wird die Cookie-Domain nicht explizit gesetzt und entspricht der Domain- oder IP-Angabe des externen Portals.</p> <p>Wurde der Wert vom Benutzer nicht angepasst, wird ein sinnvoller Standard-Wert verwendet:</p> <ul style="list-style-type: none">> Keine Cookie-Domain bei Angabe einer IP-Adresse.

Eingabefeld	Beschreibung
	<ul style="list-style-type: none"> ➤ 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. <p>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.</p> <hr/> <p> Wichtiger Sicherheitshinweis: Das Setzen einer Cookie-Domain veranlasst den Browser, diesen Cookie bei Anfragen an die angegebene Domain an den Zielsever 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.</p>

Wireguard

Bei den auswählbaren Verbindungen kann nun auch eine vorher definierte Wireguard-Verbindungen ausgewählt werden.

13 SAML / Single Sign-On

Internes und Externes Portal unterstützen nun Single Sign-On an ausgewählten Identity Providern (IdP) mittels SAML. Unterstützt werden Microsoft Azure und Keycloak. Die Einstellungen hierfür erfolgen unabhängig voneinander für das externe Portal und das interne Portal.

13.1 SAML / Single Sign-On (Internes Portal)

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.

The screenshot shows a web interface titled "SAML Internes Portal". At the top, there is a status bar indicating "Bearbeitete Version - Änderungen bleiben erhalten bis zum Zurücksetzen oder Abmelden." Below this, there are two radio buttons, with the second one selected. The main section is titled "IdP-Synchronisation". It contains several input fields: "IdP-Typ" (set to "Azure"), "Basis-URL", "IdP-Zertifikat (PEM)" (with an "Import" button), "Tenant-ID", "Client-ID", and "Client-Geheimnis". Below these is a "Grant-Typ" dropdown set to "Client-Zugangsdaten". The "Synchronisations-Intervall" is set to "15" minutes. The "Letzte Synchronisation" status is "n. v.". There is a "Jetzt synchronisieren" button with a note "Dies kann einige Minuten dauern." Below the "IdP-Synchronisation" section is the "IdP-SAML-Einstellungen" section, which contains an information message: "Es liegt noch keine IdP-Konfiguration vor. Klicken Sie auf den Button, um eine IdP-Konfiguration zu importieren." and an "IdP-Metadaten importieren" button. At the bottom of the interface, there are four buttons: "IdP-Metadaten importieren", "SP-Einstellungen exportieren", "Zurücksetzen", and "Speichern".

SAML Internes Portal

Bearbeitete Version - Änderungen bleiben erhalten bis zum Zurücksetzen oder Abmelden.

IdP-Synchronisation

IdP-Typ: Azure

Basis-URL:

IdP-Zertifikat (PEM):
 Import

Tenant-ID:

Client-ID:

Client-Geheimnis:

Grant-Typ: Client-Zugangsdaten

Synchronisations-Intervall: 15 Minuten

Letzte Synchronisation: n. v.
 Jetzt synchronisieren
 Dies kann einige Minuten dauern.

IdP-SAML-Einstellungen

Es liegt noch keine IdP-Konfiguration vor. Klicken Sie auf den Button, um eine IdP-Konfiguration zu importieren.

IdP-Metadaten importieren

IdP-Metadaten importieren SP-Einstellungen exportieren Zurücksetzen Speichern

Abbildung 15: IdP-Synchronisation (Microsoft Azure)

The screenshot shows a web interface titled "SAML Internes Portal". At the top, there is a status bar indicating "Bearbeitete Version - Änderungen bleiben erhalten bis zum Zurücksetzen oder Abmelden." Below this, there are two radio buttons for activation. The main section is titled "IdP-Synchronisation" and contains several input fields: "IdP-Typ" (set to Keycloak), "Basis-URL", "IdP-Zertifikat (PEM)" with an "Import" button, "Client-ID", "Grant-Typ" (set to Passwort), "Master-Realm", "Realm", "Benutzername", and "Passwort". There is also a "Synchronisations-Intervall" set to 15 Minuten and a "Letzte Synchronisation" field showing "n. v.". A "Jetzt synchronisieren" button is present with a note "Dies kann einige Minuten dauern." Below this is the "IdP-SAML-Einstellungen" section, which is currently empty. At the bottom, there are four buttons: "IdP-Metadaten importieren", "SP-Einstellungen exportieren", "Zurücksetzen", and "Speichern".

Abbildung 16: IdP-Synchronisation (Keycloak)

Eingabefeld	Beschreibung
I/O	Ein Schiebeschalter gibt an, ob die SAML-Anbindung derzeit aktiv (I) oder inaktiv (O) 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 Zertifikate hilfreich. Es kann in Textform eingegeben werden oder aus einer Datei importiert werden.
IdP-Typ Azure	
Tenant-ID	Azure Tenant ID.

Eingabefeld	Beschreibung
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.
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.

Abbildung 17: SP-SAML-Einstellungen

Eingabefeld	Beschreibung
Identität	Ein frei wählbarer Identifikator für den Service Provider. Z. B. der Firewall Name.
Beschreibung	Eine optionale Beschreibung.
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.

Eingabefeld	Beschreibung
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.

13.2 SAML / Single Sign-On (Externes Portal)

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/O	Ein Schiebeschalter gibt an, ob die SAML-Anbindung derzeit aktiv (I) oder inaktiv (O) 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 Zertifikate hilfreich. Es kann in Textform eingegeben werden oder aus einer Datei importiert werden.
IdP-Typ Azure	


Eingabefeld	Beschreibung
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.
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 Beschreibung.
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.

Eingabefeld	Beschreibung
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.

14 Let's Encrypt-Server

Ab LCOS FX 11.1 gibt es bei den Einstellungen zum Let's Encrypt-Server weitere Optionen, um eine eigene Adresse für diesen zu konfigurieren.

Let's Encrypt-Einstellungen

Gespeicherte Version

E-Mail-Adresse

Server-Adresse

https://acme-v02.api.letsencrypt.org/directory

Certificate Authority

Das Ändern der Server-Adresse wird nur Experten geraten, da dieses Sicherheitsrisiken birgt.
Wird ein Let's Encrypt-Zertifikat innerhalb einer Zeitspanne zu oft erneuert, wird das Erneuern für eine gewissen Zeitraum gesperrt. Einzelheiten zu den Let's Encrypt-Einschränkungen finden Sie unter <https://letsencrypt.org/de/docs/rate-limits/>.

Zurücksetzen

Schließen

Abbildung 18: Zertifikatsverwaltung > Let's Encrypt

Eingabefeld	Beschreibung
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.

15 Änderungen bei Antivirus

Ab LCOS FX 11.1 ist die Option **Heuristische Analyse** im Zuge der Umstellung auf die Antivirus-Engine von Bitdefender weggefallen. Die Heuristische Analyse ist von nun an immer aktiv.

Außerdem ist die Option **Archivdateien scannen** nun getrennt für **Mail** bzw. **HTTP(s) und FTP** einstellbar.

Scanner	Whitelist	Updates
Cloud-Scan aktivieren	<input type="checkbox"/>	
	Mail	HTTP(s) und FTP
Aktiv	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Max. zu scannende Datei-Größe	32 MB	256 MB
Dateien bei Überschreiten der max. Datei-Größe blockieren	<input type="checkbox"/>	<input type="checkbox"/>
Fehlerhaft gescannte Dateien blockieren	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Archivdateien scannen	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Abbildung 19: UTM > Antivirus-Einstellungen > Scanner

16 Fortgeschrittene Einstellungen

Ab LCOS FX 11.1 RU3 wurde ein Dialog für „Fortgeschrittene Einstellungen“ der Firewall hinzugefügt.
Navigieren Sie zu **Firewall > Fortgeschrittene Einstellungen**, um ein Bearbeitungsfenster zu öffnen, in dem Sie die Einstellungen für VoIP-Helper anzeigen und anpassen können.

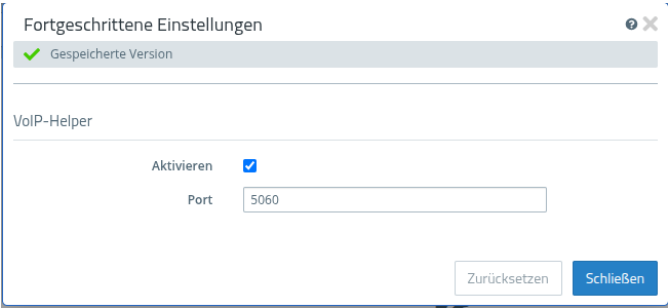



Abbildung 20: Firewall > Fortgeschrittene Einstellungen

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

Eingabefeld	Beschreibung
VoIP-Helper	
Aktivieren	Aktivieren Sie hier die Option, die VoIP-Helper-Kernel-Module zu laden.. <div> Eine Warnung wird angezeigt, falls für die Aktivierung bzw. Deaktivierung dieser Option ein Neustart der Firewall benötigt wird.</div>
Port	Geben Sie den Port an, auf dem der SIP-Server erreicht werden kann. Default: 5060.

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.