Netzwerk
Lancom R&S Unified Firewall

Hersteller: Gateprotect, Rohde & Schwarz Cybersecurity, Lancom Systems

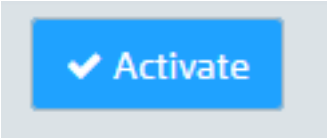
OEM-Partner:
• Antivirus: Avira / DE -> US
• Antispam, Contentfilter, URL-Filter: Bitdefender / Ro

Gerätetypen: UF-60 (5 User) ... UF-760 (200 User), auch als Virtual Appliances

Lizenzmodel:

- Basic Lizenz:
  - Aktivierung der Firewall-Funktionen inclusive Updates
  - Netzwerksegmentierung, Userverwaltung, VPN-Funktion
- Full Lizenz:
  - Aktivierung der UTM- & Firewall-Funktionen,
  - Sandboxing, Machine Learning, AV/Malware Protection, Spamfilter, DPI, IDS/IPS, SSL Insp., inkl. Updates
  - Filter- und Scanfunktion, Contentfilter incl. BPjM Jugendschutz
- Gerät läuft im 30 Tage Testmodus mit allen Funktionen ausser Konfig-Speichern. Ohne Lizenz kann keine Konfiguration gespeichert werden, aber importiert. Nach Werksreset beginnt der Testzeitraum neu.
  Lizenz aktivieren: https://lancom.de/uf-lizenz

Grundsätzliches:
* Alle (je nach Modell: 4...256) Ports lassen sich beliebig als LANs oder WANs konfigurieren.
* Jede Aktion rechts in der Web-Oberfläche muß mit "Activate" aktiviert werden.



- Button blau ist nicht aktiviert.
* Regeln des Netzwerks werden auf untergeordnete Hosts oder Bereiche vererbt, dort können aber abweichende Regeln festgelegt werden.
* Passwort+Support-PW ändern: Firewall->Administrator-> Benutzer wählen "Kennwort-Änderung erforderlich nach nächster Anmeldung"
* RESET Button macht nur Neustart. Werks-Reset siehe unten.

Grundkonfiguration:
* Konfiguration per Default über ETH1, IP= https://192.168.1.254:3438
* Zugang: admin / admin, Passwort festlegen
* 1.LAN an ETH1 konfigurieren: Network / Connections / ETH1 benennen, IP festlegen (Mask im selben Feld!)

Netzwerk

* Internetzugang einrichten. Network / Connections / ETH0 benennen, IP (+Mask) festlegen
- WAN: Default Gateway aktivieren, IP eingeben
- Network / DNS: ggf. DNS-Server hinterlegen
- Firewall / Time Settings: NTP-Einstellungen vornehmen
* Test: unter Diagnostic / Traceroute sollte jetzt eine Internetverbindung funktionieren
* Firewall / Update: Updates installieren
* Firewall / License: Lizenz eintragen
Tip:
* alle Einträge lassen sich bequem über die Suche finden
* Desktopregeln als PDF exportieren (Managementbericht/Export)
* Ansicht kann gefiltert werden über Tag, IP, Port oder Interface
* es können mehrere Nutzer mit granularen Rechten angelegt werden

Firewall in das Netzwerk einbinden:
1. Reihenschaltung Modem/Router -> Firewall
Das Verfahren ist logisch und naheliegend.
Im Idealfall nimmt man aber ein Modem und vermeidet die Router-Kaskade.
https://support.lancom-systems.com/knowledge/pages/viewpage.action?pageId=34925378
2. Einschleifen in den Router (Lancom nennt das Layer-3 Schleife)
Klingt erst mal überflüssig kompliziert, hat aber auch Vorteile.
- das Standardgateway ändert sich nicht. Bekanntlich macht Windows alle Netze dicht, wenn sich dieses Gerät ändert
- die Firewall kann bei Konfigurationsproblemen von extern umgangen oder deaktiviert werden
- bestehende VPN-Verbindungen zum Router lassen sich zumindest übergangsweise bei Umgehung der Firewall weiter nutzen
- die Pakete gehen zweimal durch den Router, das ist deutlich langsamer
https://support.lancom-systems.com/knowledge/pages/viewpage.action?pageId=32982461
3. Transparenter Bridge Mode
- das Standardgateway ändert sich nicht
- Firewall arbeitet nicht als Router oder DNS-Gateway
- das Verfahren wird nicht mehr kommuniziert und dürfte nur mit wenigen Funktionen der Firewall arbeiten
https://support.lancom-systems.com/knowledge/pages/viewpage.action?pageId=56165091
https://www.lancom-systems.de/download/produkte/lc_firewall_jump_start/MA_Firewall-Jump-Start_DE.pdf (ab S. 16)

DNS
Viele Funktionen der Firewall arbeiten auf DNS-Basis. Zu langsames DNS führt häufig zu Funktionsfehlern.
- DNS-Informationen der Firewall von einem potenten DNS-Server holen, nicht vom vorgeschalteten Router
- direkten DNS-Verkehr über die Firewall blocken (manche Dienste haben fest

verdrahtete DNS-Einträge und irgnorieren sonst die Firewall)
- DNS-Cache deaktivieren

Firewall-Konfiguration:
* für interne Zugriffe auf die Firewall ist keine Regel erforderlich (DNS, NTP, HTTP/S...)
* Objekte im Schaubild rechts anlegen:
- Create Internet Objekt erstellt WAN-Objekt. Activate.
- Create Network, Host-Group und/oder Host erstellt die LAN-Objekte, Activate.
* 1. Verbindung konfigurieren:
- gewünschtes LAN-Objekt (Bsp.: Network) anklicken, Connection-Tool anklicken, WAN-Objekt anklicken
- es wird eine neue Verbindung (LAN-Objekt -> Internet-Objekt) konfiguriert
  (Aktions-Pfeil: LAN-Objekt zu WAN, NAT genauso)
- rechts erscheint die Liste der Regeln. Regel "Ping" mit "+" hinzu fügen.
Nun kann man per PING aus dem LAN das Internet erreichen.
* 2. Verbindung konfigurieren:
- gewünschtes LAN-Objekt (Bsp.: Host-Group) anklicken, Connection-Tool anklicken, WAN-Objekt anklicken
- es wird eine neue Verbindung (LAN-Hostgroup-Objekt -> Internet-Objekt) konfiguriert
- rechts erscheint die Liste der Regeln. Regel "HTTP" und "HTTPS" mit "+" hinzu fügen.
Nun kann man per Browser aus der Hostgroup im LAN das Internet erreichen.

• Host für einzelne Geräte/IP
• IP-Bereich für Bereiche (Drucker, Notebooks, IoT...)
• Host-/Netzwerk-Gruppe erlaubt mehrere IP/Geräte in einem Objekt

• DROP-Regeln gehen vor ALLOW-Regeln und lassen sich auch in Vererbung nicht überschreiben
• Regeln vererben sich über Netzwerk -> IP-Range -> Host
• Priorität: Host größer als IP-Range größer als Netzwerk

Dienste
Neben den vordefinierten Diensten können eigene Dienste auch mit mehreren Ports und Protokollen angelegt werden.
Mit Dienst-Gruppen können mehrere Dienste zusammengefasst werden.

NAT (Network Adress Translation)
- wird in jeder Desktop-Verbindungsregel einzeln gesteuert
- ist bei Regeln zum WAN per Default aktiviert
- Achtung bei Regeln zu einzelnen Servern im WAN (DNS o.ä.): NAT setzen, Regel meist nicht bidirektional lassen!

Portforwarding wird im Protokoll der Desktop-Verbindung (Hostobjekt zu WAN) konfiguriert.
Bsp: Dienst HTTP, Verbindungsrichtung drehen (von außen nach innen), NAT aus, DMZ/Port-Weiterleitung aktivieren

(c) 2024 Uwe Kernchen <news@uwe-kernchen.de> | 2024-04-26 14:24
URL: https://uwe-kernchen.de/phpmyfaq/index.php?action=faq&cat=4&id=295&artlang=de
(C) https://uwe-kernchen.de

Netzwerk

Quellport ist das Dienstobjekt, abweichender Zielport kann definiert werden.
Portforwardings können auch für Dienstgruppen eingerichtet werden.

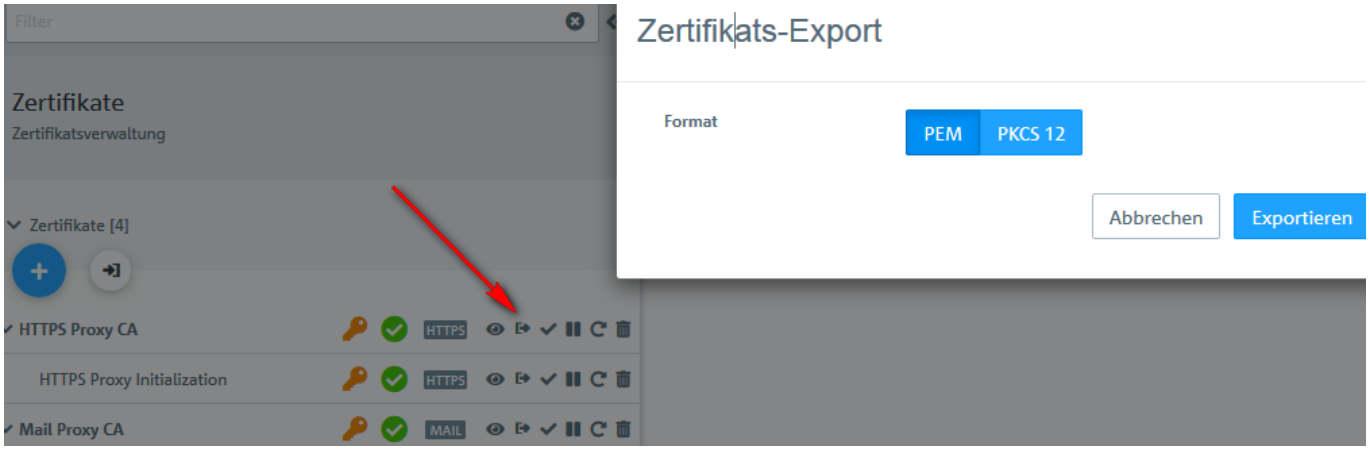
Proxy-Konfiguration:
Der Proxy ist ein klassischer Man-in-the-middle und bricht gültige Zertifikatsketten auf.
Er ist für viele Funktionen unerläßlich, aber er ist eine Dauerbaustelle für Admins und ständiges Ärgernis der Anwender.
• Antivirus funktioniert nur mit aktivem Proxy (HTTP/S, FTP, EMail)
• URL-/ Contentfilter funktioniert nur mit aktivem Proxy (HTTP/S)
• Webstatistik geht nur mit Proxy
• Spamfilter, Blacklist/Whitelist funktioniert nur mit aktivem Proxy (EMail)
• Applicationfilter, IDS und IPS funktionieren auch ohne Proxy.

Hinweis:
* Der Proxy muss global und pro Verbindung aktiviert werden.
* Keine Firewall-Regel darf TCP Port 443 enthalten, sonst wird der HTTPS-Proxy ausgehebelt.

Proxy-Whitelist Syntax: "domain.com" -> nur Domain ohne Subdomains, ".domain.com" -> Domain incl Subdomains

Der moderne "HTTP Strict Transport Security (HSTS)" Modus von Google, Wikipedia u.a. erlaubt keine HTTPS-Proxys.
Weitere Proxy-Ausnahmen:
- Seiten mit Ende-Ende-Zertifikat (Grundbuch, KSA, Onlinebanking, MS WSUS, Windows Aktivierung, Firmwareupdates (VMWare, Lancom)...)
- Signal Desktop Client (.signal.org und .whispersystems.org)
- Microsoft Server- oder Office- Aktivierung

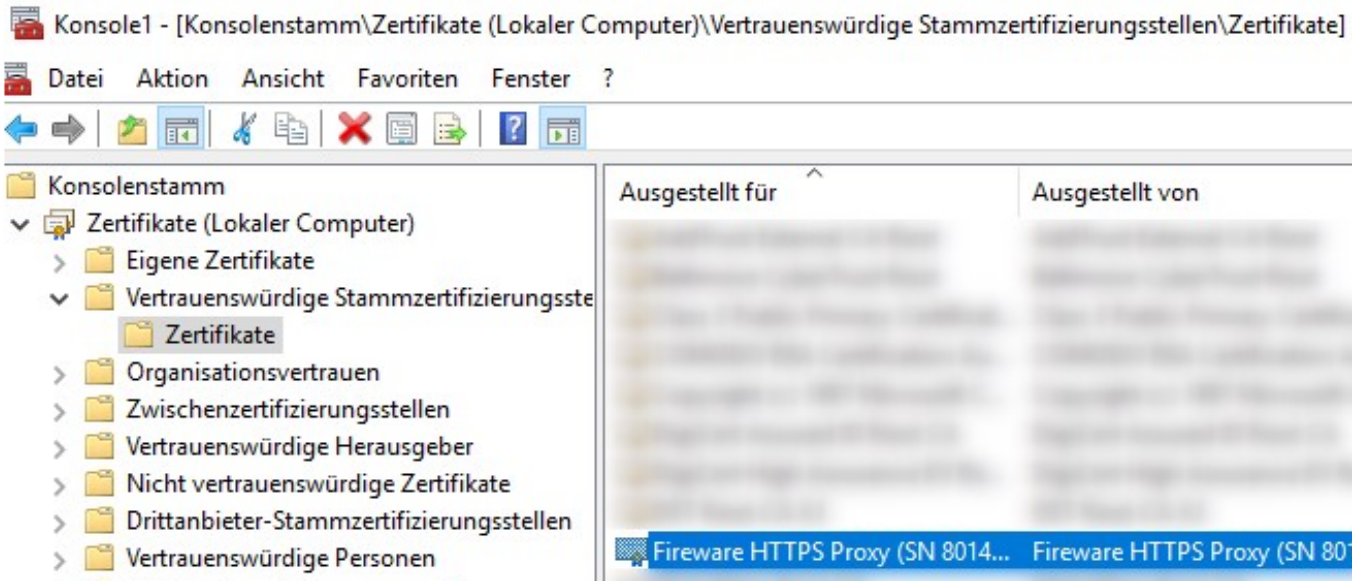
Zertifikate
• Firewall enthält ein eigenes SSL-Zertifikat, wird aber als "Man-in-the-Middle" von allen Browsern als "unsicher" eingestuft (Zertifikat stammt nicht von der Webseite). Das eigene Zertifikat der Firewall muß also auf alle Clients ausgerollt und im Browser als vertrauenswürdig hinterlegt werden (Eport PEM, in CRT umbenennen).
• Let`s Encrypt Zertifikate für Reverse Proxy und externes Portal (-> FX 10.10).



Einbinden des LCOS Root CA und LCOS Proxy-Zertifikates manuell oder per GPO:

Netzwerk

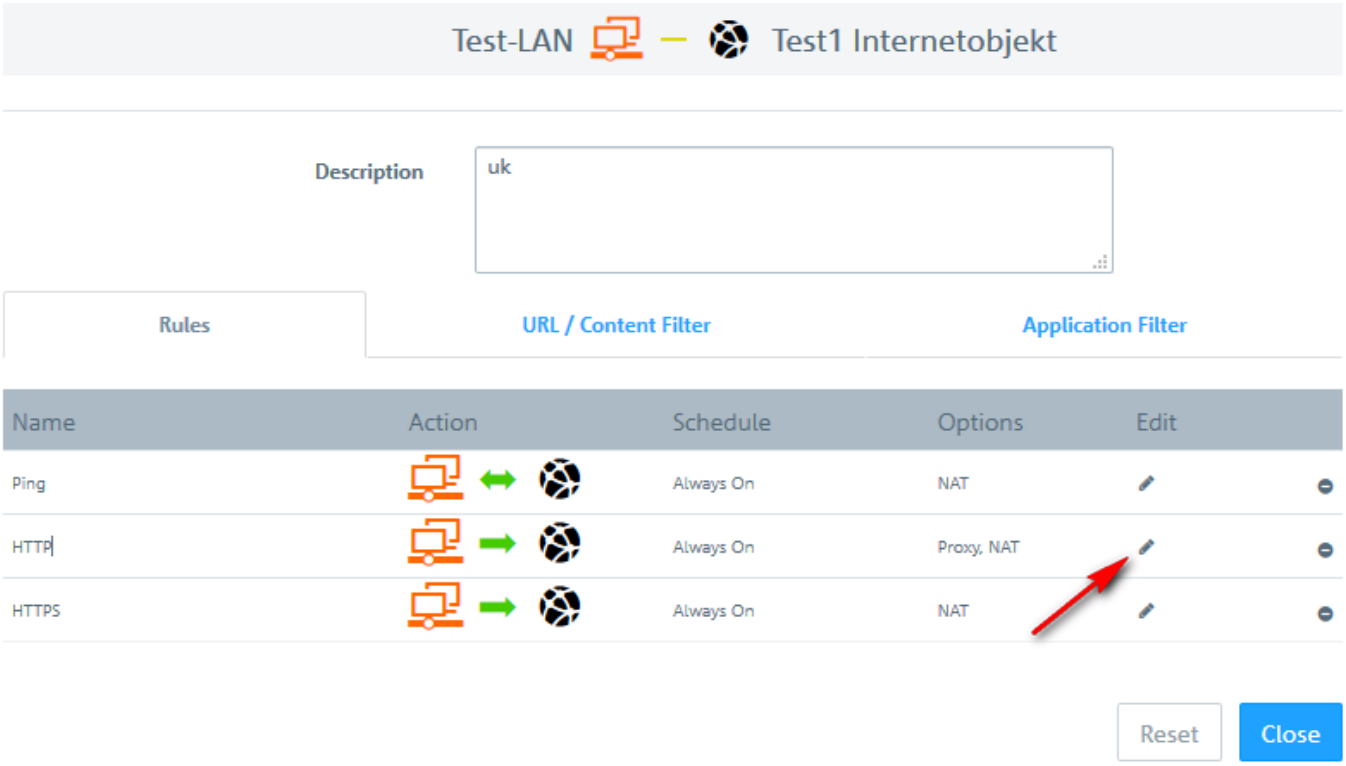
• LCOS Root CA als vertrauenswürdige Stamm-CA
• LCOS HTTPS Proxy als vertrauenswürdiger Herausgeber
Computerkonfiguration \ Richtlinien \ Windows-Einstellungen \ Sicherheitseinstellungen \ Richtlinien öffentlicher Schlüssel \ Vertrauenswürdige Stammzertifizierungsstellen



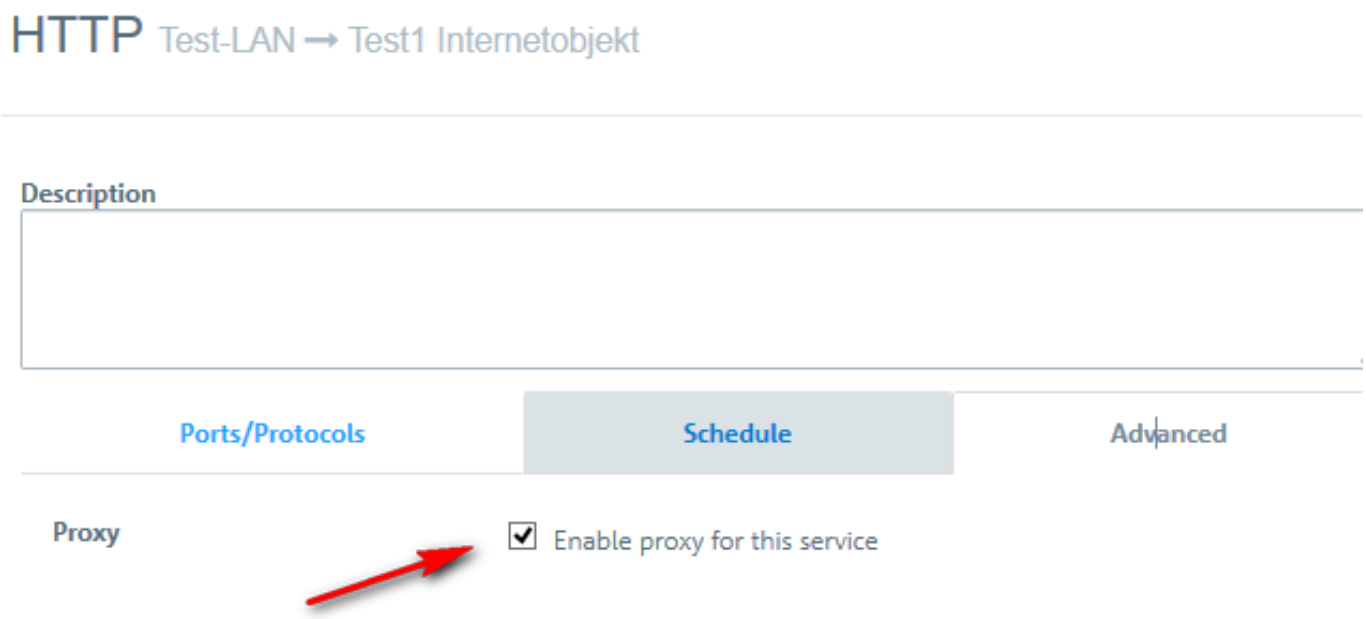
Einbinden manuell in Firefox: als Zertifizierungsstelle importieren.
Firewall-Zertifikate werden beim Reset gelöscht -> sichern!

Zertifikat für HTTPS-Webzugriff erstellen: https://support.lancom-systems.com/knowledge/pages/viewpage.action?pageId=32983640

* Desktop-Connection wählen (Bsp.: Hostgroup-Objekt -> Internet-Objekt), HTTP-Regel editieren.



Unter Advanced: Proxy aktivieren.



* Import Zertifikate in Mobilgeräte ist problematisch.
ggf. IP-Bereich als Objekt definieren, HTTPS ohne Proxy

* E-Mail Proxy: POP3/SMTP- und IMAP-Proxy
* HTTP-, HTTPS-Proxy

URL-/Contentfilter
Um URL- und Contentfilter für HTTP- und HTTPS-Verbindungen zu verwenden, wird der HTTP-Proxy benötigt.
URL/Contentfilter wird für jede Firewall-Verbindung konfiguriert.
Um URL- und Contentfilter für DNS-Anfragen zu verwenden, muss der Web-Filter-Modus auf „DNS“ oder „Proxy und DNS“ gesetzt werden.
Falls Ausnahmen/Override erlaubt sein soll, in "Einstellungen" zentral erlauben.
- vordefinierte Kategorien
- eigene URL-Blacklist
- Blacklists für Dateiendungen (\.exe$)
- eigene URL-Whitelist
Konfiguration des BPjM-Moduls im Content Filter: URL/Contentfilter-Regel in Verbindung aktivieren, WEB-Filter-Modus= DNS
->
https://support.lancom-systems.com/knowledge/pages/viewpage.action?pageId=128418084

UTM / Applikation Firewall:
Per Default: aus.
Vorteil: funktioniert ohne Proxy.
Nachteil: Der Application-Filter liefert keine definierte Block-Seite wie der Content-Filter, sondern der geblockte Aufruf schlägt fehl.
Dienst aktivieren, Filter-Profil erstellen, in Desktop-Verbindung Profil als Whitelist oder Blacklist definieren.

Netzwerk

Die R&S Application Firewall wird u.a. auch von Barracuda genutzt und ist sehr leistungsstark.
Sie kann auch verschlüsselten Traffic über Layer-7 Mustererkennung verarbeiten und erkennt die Anwendung (Aliexpress, AmazonShopping, Apple Maps, Bitcoin, eBay, Facebook, Office365, GoToMeeting, Dropbox, OneDrive, Games, Modebus, Mail, Messenger, News, Peer-to-peer, RemoteControl, Tunnel, Streaming u.v.a.m.).
Unabhängig vom Application-Filter muß der entsprechende Port frei gegeben sein (Verbindungsregel), wenn die Applikation erlaubt sein soll.

Tip:
* Intrusion Detection (IDS) aktivieren, Intrusion Prevention (IPS) aber erst nach Hinzufügen der Ausnahmen! (IDS-Protokoll)
* Fehler, gesperrte Aufrufe usw. im Systemlog. Type=Error, Message=IP eingrenzen

Reverse Proxy
Will man über nur eine externe IP-Adresse verschiedene interne Ziele bei gleichem Port erreichen, nutzt man Reverse Proxy.
Der Reverse Proxy löst verschiedene Domain Namen auf einer IP-Adresse auf und routet sie an verschiedene interne Server.

- mehrere Domainnamen (mail.domain.de und web.domain.de) verweisen auf die selbe externe IP-Adresse
- im Router ist eine Portfreigabe von Port 443 und/oder 80 auf den Server eingerichtet auf dem der Reverse Proxy läuft
- der Reverse Proxy wertet die angefragte Domain aus und leitet dann beispielsweise entweder zum Exchange oder Webserver weiter

VPN Verbindung:
Die R&S Firewall erlaubt beliebig viele (!) IPSec VPN-Verbindungen IKE v1 und IKE v2.
Außerdem unterstützt die Firewall VPN Open-SSL / OpenVPN.
Die Einrichtung des Advanced VPN-Client von Lancom (NCP) per IPSec wird in der Lancom KB beschrieben.
Anleitung für OpenVPN:
• https://blog.hartinger.net/openvpn-einrichten-bei-einer-lancom-unified-firewall/
• https://support.lancom-systems.com/knowledge/pages/viewpage.action?pageId=42108821

- IPSec-Einstellungen: IPSec aktivieren
- virt. IP-Pools: Default IP-Pool konfigurieren (DNS) oder eigenen Pool anlegen
- Verbindung anlegen, Vorlage wählen, Tunnel und Authentifizierung konf.
- VPN-Verbinung: Konfig. exportieren
- Desktop-Objekt: VPN-Host erstellen
- Desktop-Verbindung(en) VPN-Host zu LAN-oder-Host definieren, Dienste frei geben

Netzwerksegmentierung/VLAN

Netzwerk

Die Firewall kann intern nicht arbeiten, wenn alle Geräte im gleichen Netzwerk sind.
Routing über Netzsegmente ist erforderlich.
Da die physischen Ports beschränkt sind, heißt die Lösung VLAN.

- Netzwerk / VLAN interfaces anlegen
- Netzwerk / Verbindungen / Netzwerkverbindungen anlegen (Name, VLAN-Interface wählen, IP festlegen)
- Desktop-Objekt: Netzwerk erstellen, Name festlegen, VLAN-Interface und Netzwerk-IP auswählen

Routing
Die Firewall arbeitet auch als Router.
Unter Netzwerk / Routing können individuelle Routen (beispielsweise zu Transfer-Netzen hinter anderen Routern) angelegt werden.
Routen zwischen Netzwerkobjekten werden automatisch erstellt und sind verborgen (Nicht konfigurierbare Tabellen anzeigen).
Unabhängig vom Routing muß zu dem Netz auch eine Firewallregel angelegt werden.
Weitere interne Netze: ggf. RDP, DNS, SMB.. frei geben!

"Routing" zu anderen Routern im gleichen Netz (bei Lancom-Routern mit ICMP-Redirect) ist mir bei den UF nicht gelungen.
Lösung: Anderen VPN-Router in getrenntes Transfer-Netz hinter die UF.

Monitoring
Die Firewall kann max. 8 GB Monitordaten auf die interne HD speichern. Nach 6GB werden die ältesten Daten automatisch überschrieben.
Die letzten 500 Ereignisse werden angezeigt, für mehr Ereignisse: filtern.
• Alarmprotokoll: Traffic, geblockte Verbindungen
Im Alarmprotokoll können für jedes Ereignis individuell Regeln erstellt werden, wenn das Protokoll als Rohdaten gespeichert wird.

Backup / Daten
Im GUI-Backup ist nur der Config-Pfad enthalten, es fehlen die Zertifikate.
Das Backup erfolgt als passwortgeschützte ZIP-Datei, die sich wieder entpacken läßt.

SSH-Backup:

```
ssh gpadmin@Firewall-Internal-IP
sudo bash
cd /tmp
zip -r backup.zip /opt/gateprotect/etc
```

Datenpfade:
/opt/gateprotect/etc - Configuration
/opt/gateprotect/keys - Zertifikate
/opt/gateprotect/license - Lizenz

(c) 2024 Uwe Kernchen <news@uwe-kernchen.de> | 2024-04-26 14:24
URL: https://uwe-kernchen.de/phpmyfaq/index.php?action=faq&cat=4&id=295&artlang=de
(C) https://uwe-kernchen.de

Netzwerk

Dateien:
gprules.ini -> Firewal Rules
gpnetworkd.json -< Netzwerkkonfiguration, Interfaces, Routen ...

Fehlersuche
• Monitoring & Statistiken > Einstellungen: bsp: "Blockierter eingehender Verkehr" -> Rohdaten speichern
• Fehler provozieren
• Alarmprotokoll: Einträge "Connection Blocked" suchen
• Zahnrad rechts: neue Regel aus Eintrag erstellen

Werksreset:
Werksreset löscht auch die Lizenz aus dem Gerät! Lizenz vorher sichern!

- einfach über GUI (wenn Ports erreichbar und Passwort bekannt)
- wenn nichts mehr geht: USB-Stick -> automatische Installation (LCOS FX-ISO + UF-USB-Stick-Creator)
  Firewall geht danach aus. USB-Stick abziehen(!) und neu starten.

Versionshistorie**:**

• Release-Update FX 10.13 RU2 (05.12.2023)

- When using an IPSec connection and port forwarding at the same time, packets sent via the IPSec connection for the ports used in port forwarding were sent to the port forwarding destination instead of the actual destination. This led to restricted communication via the VPN connection.
- If the mail proxy was activated in the configuration of the Unified Firewall after an update to LCOS FX 10.13 Rel or 10.13 RU1, a mail server (e. g. Microsoft Exchange) could no longer receive e-mails. If the inbound proxy (SMTP-IN) was deactivated, e-mail reception worked again.
- An update to the Squid proxy has fixed a vulnerability in the web proxy that allowed attackers to smuggle data through the proxy using request/response packets in HTTPS 1.1 or ICAP.

• Relase-Update FX 10.13 RU1 (01.11.2023 - zurück gezogen / 10.11.2023):

- Erweiterung des WEB-GUI der Firewall: Desktop-Verbindungen zeigen auch geerbte Berechtigungen

• Release-Update **FX 10.12 RU3** (09/2023):

- Schlüssel zum Betrieb der Avira Antivirus Engine wurden aktualisiert (keine Funktion ab 10/2023 ohne dieses Update!)
- Sicherheitslücke im Border Gateway Protokoll (BGP) behoben (CVE-2023-38802)
- diverse Fehlerkorrekturen in RU2

• Release-Update **FX 10.12 RU1** (07/2023):

(c) 2024 Uwe Kernchen <news@uwe-kernchen.de> | 2024-04-26 14:24
URL: https://uwe-kernchen.de/phpmyfaq/index.php?action=faq&cat=4&id=295&artlang=de
(C) https://uwe-kernchen.de

- Wireguard VPN
- Hardware-Monitoring (CPU, RAM, Festplatte) mit Zuordnung des Ressourcenverbrauches zu Features und Prozessen
- automat. E-Mail-Versand von Security Reportings
- DNS-basierte Firewall-Regeln (Regeln mit Host-Namen statt IP-Adressen)

- Release-Update **FX 10.11** (02/2023):

  - Wechsel des OEM-Partners für Antispam, Contentfilter und URL-Filter von Cyren/US (in Insolvenz) in Bitdefender/Ro

- Release-Update **FX 10.10** (01/2023):

  - Zertifikatsverwaltung > Let's Encrypt: können im Reverse Proxy Frontend bei aktiviertem SSL-Modus und im externen Portal der Benutzerauthentifizierung verwendet werden

- Release-Update **FX 10.9** (08/2022):

  - URL- / Content-Filter auf Basis von DNS ohne SSL-Inspection
    DNS-Abfragen, die über den DNS-Server der LANCOM R&S®Unified Firewall laufen, werden klassifiziert und gemäß ihrer Kategorien oder konfigurierter Black und Whitelists gefiltert. In den Desktop-Verbindungen wurde unter dem Tab "URL-/ Content-Filter" ein neues Auswahlfeld für den Web-Filter-Modus hinzugefügt. Es werden die gleichen Profile genutzt wie beim URL-/ Content-Filter über den HTTP-/ HTTPS-Proxy.
    - gefiltert wird auf der Domain, nicht auf der URL
    - es wird keine Blockpage angezeigt und ist nicht möglich, den Override-Modus zu nutzen
    - gefiltert wird nur, wenn die DNS Anfrage durch die Firewall geht
  - BGP: unter Netzwerk > Routing: neuer Menü-Eintrag BGP
    Monitoring & Statistiken > BGP-Status

- Release-Update **FX 10.5** (06/2020):

  - IMAP-Proxy
  - Content-Filter für ausgewählte Seite kann temporär deaktiviert werden
  - individuelles Routing für mittels PACE2 DPI Engine erkannte Protokolle und Applikationen (über VPN, andere Internetanschlüsse, am Proxy vorbei..)

Quellen:

- Lancom Firewall FAQ: https://support.lancom-systems.com/knowledge/pages/viewpage.action?pageId=34925347
- Firewall Downloads (ISO, USB-Installer, MIBs): https://my.lancom-systems.de/mylancom/lizenzportal/downloads/
- Authentifizierung per Single Sign On an der Firewall: https://support.lancom-

Netzwerk

systems.com/knowledge/pages/viewpage.action?pageId=54952158

Eindeutige ID: #1294
Verfasser: Uwe Kernchen
Letzte Änderung: 2023-12-12 08:38

(c) 2024 Uwe Kernchen <news@uwe-kernchen.de> | 2024-04-26 14:24
URL: https://uwe-kernchen.de/phpmyfaq/index.php?action=faq&cat=4&id=295&artlang=de
(C) https://uwe-kernchen.de