LANCOM Release Notes

LCOS FX

10.6 RU4

LANCOM Systems GmbH
Adenauerstrasse 20 / B2
52146 Würselen
Germany

Internet: http://www.lancom-systems.de

04.10.2021, MKoser

Inhaltsübersicht

1. Einleitung **2**
2. Unterstützte Hardware **2**
3. Historie LCOS FX **3**
LCOS FX-Änderungen 10.6 RU4 3
LCOS FX-Änderungen 10.6 RU3 3
LCOS FX-Änderungen 10.6 RU2 6
LCOS FX-Änderungen 10.6 RU1 6
LCOS FX-Änderungen 10.6 Rel 7
LCOS FX-Änderungen 10.5 RU3 9
LCOS FX-Änderungen 10.5 RU2 10
LCOS FX-Änderungen 10.5 RU1 12
LCOS FX-Änderungen 10.5 13
4. Installationsanleitung zum Update auf LCOS FX 10.6 RU4 **17**
5. Weitere Informationen **21**
6. Bekannte Probleme **21**
7. Haftungsausschluss **21**

LANCOM Systems

1. Einleitung

Alle Mitglieder der LANCOM Betriebssystem-Familie – LCOS, LCOS SX, LCOS LX und LCOS FX – sind die vertrauenswürdige Grundlage für das gesamte LANCOM Produktportfolio. Im Rahmen der von den Produkten vorgegebenen Hardware ist die jeweils aktuelle Firmware-Version für alle LANCOM Produkte verfügbar und wird von LANCOM Systems kostenlos zum Download angeboten.

Dieses Dokument beschreibt die Neuerungen der LCOS FX Software Release 10.6 RU4 sowie die Änderungen und Verbesserungen zur Vorversion.

2. Unterstützte Hardware

Version 10.6 RU4 unterstützt die folgenden Hardware Appliances:

- LANCOM R&S®Unified Firewalls UF-50/60/T-60/100/160/200/260/300/360/500/900/910
- R&S®UF-50/100/200/300/500/800/900/1000/1200/2000
- R&S®UF-T10
- R&S®UTM+100/200/300/500/800/1000/2000/2500/5000
- R&S®NP+200/500/800/1000/2000/2500/5000
- R&S®GP-U 50/100/200/300/400/500
- R&S®GP-E 800/900/1000/1100/1200
- R&S®GP-S 1600/1700/1800/1900/2000
- R&S®GP-T 10

Version 10.6 RU4 unterstützt die folgenden virtuellen Appliances:

- LANCOM vFirewall S, M, L, XL
- R&S®UVF-200/300/500/900

Version 10.6 RU4 unterstützt die folgenden Hypervisor:

- Vmware ESX
- Microsoft HyperV
- Oracle Virtualbox
- KVM

3. Historie LCOS FX

LCOS FX-Änderungen 10.6 RU4

Weitere Verbesserungen

- Stabilitätsverbesserungen der LMC-Anbindung

LCOS FX-Änderungen 10.6 RU3

Neue Features

- **Cloud-managed Firewall**[1]

  Mit dem aktuellen Release stehen ganz neue Konfigurationsmöglichkeiten der Cloud-managed Firewalls im Zusammenspiel mit der LANCOM Management Cloud zur Verfügung. Das One-Click-Security-Paket umfasst die übergreifende Steuerung des Application Filters, des Content Filters, der SSL Inspection sowie der Anti-Virus-/Anti-Malware-Funktionen (inkl. Whitelist-Optionen). Eine initial erstellte Konfiguration kann hierbei bequem auf alle Geräte, Standorte und Netzwerke ausgerollt werden.

  LCOS FX 10.6 RU3 erweitertet außerdem die Einsatzmöglichkeiten der Cloud-managed Firewall, sodass die LANCOM R&S®Unified Firewalls nun sowohl als VPN-Gateway als auch als Central Site VPN-Gateway z.B. für die Vernetzung von verschiedenen Standorten genutzt werden können. Das alles mit wenigen Klicks in der LANCOM Management Cloud via Auto-VPN.

- **IDS/IPS- und Anti-Virus-Ausnahmen**

  Spezifische Hosts und Netzwerke lassen sich über Einstellungen im jeweiligen Desktop-Objekt von der Prüfung durch die IDS/IPS- oder Anti-Virus-Engine ausnehmen.

Weitere Verbesserungen

- Bei SSL-VPN-Verbindungen ist es seit LCOS FX 10.6 REL möglich, auf der Server-Seite eine CA auszuwählen, wodurch die Unified Firewall jeden Client akzeptiert, der ein von dieser CA unterzeichnetes Zertifikat besitzt. Somit ist es nicht notwendig, für jeden VPN-Client eine eigene VPN-Verbindung zu konfigurieren. Ab LCOS FX 10.6 RU3 funktioniert dies nun auch bei VPN-SSL im Bridging-Modus.

Korrekturen

- In einigen Fällen konnte es vorkommen, dass ein Login auf der Web-Konfigurationsoberfläche nicht möglich war. Dies konnte im laufenden Betrieb der Fall sein, oder auch nach einer Erst-Installation bzw. Konfiguration der Unified Firewall auftreten.
- Der Zähler für erfolglose Admin-Logins auf der Web-Konfigurationsoberfläche funktionierte nicht.
- Wenn der Kommunikationsport für die Web-Konfigurationsoberfläche ungleich dem Standard-Port 3438 war,

1 Unterstützung dieser Funktionen in der LANCOM Management Cloud folgt in Kürze

konnte eine Konfiguration nach einem Pairing mit der LMC nicht an die Unified Firewall ausgerollt werden.

- Ein Online-Firmware-Upgrade von LCOS FX 10.5 auf 10.6 bei Unified Firewalls, welche in einem High-Availability-Cluster (HA) betrieben wurden, schlug fehl.
- Bei der Konfiguration einer E-Mail-Benachrichtigung war das Passwort für den Zugriff auf das verwendete E-Mail-Postfach im Klartext zu lesen.
- Beim Import eines unter LCOS FX 9.6 erstellten Backups wurde eine für den Zugriff auf das interne Portal veränderte Port-Angabe nicht in die Datei webserver.ini übernommen.

- Desktop-Icons der LMC wurden nach einem Rollout über die LMC und dem Setzen eines Filters, der diese Icons ausblenden sollte, trotzdem angezeigt.
- In seltenen Fällen konnte eine leere dns.ini-Datei im Pfad ‚/opt/gateprotect/etc/' dafür sorgen, dass nach einem Firmware-Upgrade auf LCOS FX 10.6 RU2 der Webclient nicht funktionierte.
- Nach dem Import eines Konfigurations-Backups wurden in der IPSec-Konfiguration vorhandene Subject Alternative Name (SAN)-Identifier nicht mehr angezeigt.
- Wenn sämtlicher Datenverkehr über eine IPSec-Verbindung übertragen (sowohl Client-to-Site als auch Site-to-Site) und darüber eine Webseite aufgerufen wurde, kam es bei einigen Webservern vor, dass diese die Path-MTU-Aushandlung per ICMP ignorierten. Dies führte aufgrund einer zu großen MTU dazu, dass die Webseiten nicht aufgerufen werden konnten.
  Für IPSec-Verbindungen wird jetzt ein TCP-MSS-Clamping durchgeführt, damit die MTU passend gewählt wird.
- Obwohl die Synchronisierung eines HA-Clusters erfolgreich durchgeführt wurde, war der Status des Clusters in der Konfigurationsoberfläche als ‚Nicht synchron' angegeben.
- Eine IPSec-VPN-Verbindung wurde vom Initiator nach einem Verbindungsabbruch nicht automatisch erneut aufgebaut, sondern erst bei einer stattfindenden Datenübertragung.
- In einem im CSV-Format exportierten Management-Bericht (report_data.csv) war die Zeitangabe ‚Statistics Period' nicht enthalten.
- Im Dialog zur Verbindungskonfiguration konnte es vorkommen, dass in der Registerkarte ‚Application-Management' bei einem hinzugefügten Routing-Profil die Schaltfläche zum Entfernen der Regel fehlte.
- Ein Benutzer mit konfiguriertem ‚Wake on LAN' konnte sich im ‚internen Portal' nicht mehr anmelden.

LCOS FX-Änderungen 10.6 RU2

Korrekturen

- Kleinere Verbesserungen für LCOS FX 10.6 RU1

LCOS FX-Änderungen 10.6 RU1

Neue Features

- Unterstützung der LANCOM R&S®Unified Firewall UF-360 mit einen massiven Performance-Schub im Vergleich zum Vorgängermodell UF-300: Verdoppelte Performance, verdoppelte Speicherkapazität, Modul-Erweiterungsslot sowie zwei 10 Gbit/s SFP+-Schnittstellen für ganz neue Einsatzszenarien.
- Umwandlung der VPN-Tunnel-Begrenzung der UF-60 / UF-160 / UF-260 in eine Empfehlung zur Kundenorientierung.

Weitere Verbesserungen

- **CSV-Export des Management-Berichts**
  Der Management-Bericht kann zur einfacheren maschinellen Verarbeitung jetzt ebenfalls im CSV-Format exportiert werden.

Korrekturen

- Im englischen Dialog für den Export von SSL-VPN-Konfigurationen wurden deutsche Texte / Begriffe angezeigt.
- Wenn im Menü ‚Netzwerk / DNS / Netzwerk spez. Einstellungen' ein Eintrag hinzugefügt wurde und der Eintrag nach dem ersten Speichern geändert werden sollte, konnte die Änderung nicht gespeichert werden.
- Nach einer Änderung des Ports für den lokalen Webclient im Menü ‚Firewall / Firewall-Zugriff / Webclient-Einstellungen' war es nicht möglich, sich bei einem erneuten Login mit dem geänderten Port an der Web-Oberfläche anzumelden.
- Wenn ein administrativer Benutzer angelegt wurde, welcher in den Webclient-Rechten (Menü ‚Firewall / Administratoren / Webclient-Rechte') das Monitoring-Recht ‚Lesen / Öffnen' besaß, war es nicht möglich, mit diesem Benutzerkonto die Liste der DHCP-Leases im Menü ‚Monitoring & Statistiken / DHCP-Leases' anzusehen. Der Benutzer erhielt stattdessen den Fehler „403 Forbidden".
- Nach einem Neustart konnte es vorkommen, dass die Verbindung zur LMC nicht mehr aufgebaut werden konnte.
- Wurden in dem Menü ‚Netzwerk / DNS / Netzwerkspezifische Einst.' DNS-Einstellungen für ein bestimmtes Netzwerk vorgenommen, wurden für dieses Netzwerk keine DNS-Anfragen beantwortet.
- Bei Anbindung zweier Filialen an eine Zentrale unter Verwendung von VPN-SSL mit Bridge konnten die beiden Außenstellen nicht über die Zentrale miteinander kommunizieren.

LCOS FX-Änderungen 10.6 Rel

Neue Features

- **Erweiterte Funktionen für Cloud-managed Firewalls** [2]

  LANCOM FX 10.6 stattet die LANCOM R&S®Unified Firewalls mit vielen zusätzlichen Funktionen für den Betrieb mit der LANCOM Management Cloud (LMC) aus und rüstet sie zum vollwertigen Stand-alone-VPN-Gateway für Filialen auf, denn: Ab sofort erfolgt die sichere VPN-Vernetzung von Standorten inklusive Netzvirtualisierung vollautomatisiert. Dank der Unterstützung des DynDNS-Services der LMC werden Firewalls zudem einfach über eine selbstgewählte Subdomain erreicht. Weiterhin können Anwendungen durch die Firewall nun auch im Stand-alone-Betrieb auf Layer-7-Ebene blockiert werden.

- **Zonenverwaltung für DNS**

  Ab sofort unterstützen die LANCOM R&S®Unified Firewalls unterschiedliche DNS-Server für unterschiedliche Zonen. Außerdem kann die DNS-Konfiguration für einzelne Netze separat angepasst werden. Dies erlaubt die separate DNS-Konfiguration für einzelne Netze, sodass beispielsweise der Zugriff auf lokale Zonen ausschließlich vom Mitarbeiternetzwerk und nicht vom Gastnetzwerk erfolgen kann.

Weitere Verbesserungen

- **VPN-SSL CA Auth**

  Für eine VPN-SSL Client-to-Site-Verbindung kann eine CA zur Authentifizierung ausgewählt werden. Alle Clients, deren Zertifikat von dieser CA unterzeichnet wurden, können sich zu dieser Site verbinden.

Korrekturen

- Mit LCOS FX 10.6 wurde eine Sicherheitslücke (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31538) der LANCOM R&S®Unified Firewall behoben. Dies betrifft alle Geräte mit LCOS FX 10.5-Versionen. Die LCOS FX 10.4-Versionen und kleiner sind von der Sicherheitslücke nicht betroffen.
- Wenn bei der Verwendung des internen Benutzerportals eine Benutzeranmeldung durchgeführt wurde, während der Hintergrundprozess x-rulesd startete, führte dies dazu, dass sich der Hintergrundprozess beendete und keine Benutzeranmeldung über das interne Portal mehr möglich war.
- Beim Anlegen einer neuen Client-To-Site-Verbindung mit SSL-VPN war die Schaltfläche zum Exportieren der VPN-Konfiguration ausgegraut und somit nicht nutzbar.
- Wenn eine neue SSL-VPN-Verbindung konfiguriert wurde, war die Datenkompresssion standardmäßig aktiviert und es wurde im Default immer das TCP-Protokoll verwendet. Die Datenkompression ist jetzt im Default deaktiviert und es wird standardmäßig das UDP-Protokoll für den VPN-Tunnel eingesetzt.
- Wenn das Profil einer IPSec-VPN-Client-Verbindung, bei welcher das Passwort Sonderzeichen (z.B. #) enthielt, in eine AVC-Profildatei (*.ini-Datei) exportiert wurde, konnte das exportierte Profil nicht in den LANCOM Advanced VPN Client importiert werden.
- In einem HA-Cluster wurden geänderte Passworte der Administratoren sowie ein geändertes Support-Passwort nicht vom Master-Gerät auf das Slave-Gerät synchronisiert.

2 Unterstützung dieser Funktionen in der LANCOM Management Cloud folgt in Kürze

- Bei Installationen mit sehr vielen Client-to-Site-Verbindungen (SSL-VPN) kann es zu häufigen An- und Abmeldungen der VPN-Clients kommen. Der von den für die An- und Abmeldung der VPN-Clients zuständigen Prozessen reservierte Speicher wurde dabei nicht mehr freigegeben. Dadurch wurde der ‚OOM'-Prozess (Out Of Memory) aufgerufen, welcher für den Betrieb erforderliche Prozesse beendete, sodass die Funktion nicht mehr gegeben war. Dies konnte lediglich durch einen Neustart behoben werden.
- Wenn bei aktiver IDS/IPS ein Backup über die Software ‚Veeam' erstellt wurde, reservierte der IDS/IPS-Dienst immer weiter Speicher und gab diesen nicht mehr frei. Dies führte somit zu einem unvermittelten Neustart.
- War eine DHCP-Konfiguration mit dem gleichen DHCP-Adressbereich nach einem Update auf LCOS FX 10.5.3 doppelt vorhanden (etwa durch eine Migration eines IP-Adressbereiches auf ein anderes Interface ohne die DHCP-Konfiguration zu entfernen), konnte der DHCP-Dienst aufgrund des Adress-Konflikts nicht gestartet werden.
  Fehlerhafte DHCP-Konfigurationen werden jetzt bei einem Firmware-Update ignoriert.
- Ein Wechsel des HTTP-Proxy zwischen den Modi ‚Transparent' und ‚Intransparent' führte dazu, dass der Proxy anschließend solange nicht mehr funktionierte, bis die Regeln neu aktiviert wurden.
- Wenn ein Benutzer zwecks Authentifizierung auf die Login-Seite des ‚Internen Portals' zugriff, aber das SSL-Zertifikat der Login-Seite nicht akzeptierte, führte dies zu einer hohen Prozessor-Auslastung der Unified Firewall.
- Zwecks Überprüfung der Internet-Verbindung wird über einen Heartbeat-Test ein Ping auf eine hinterlegte IP-Adresse durchgeführt. Bisher war standardmäßig der Google DNS-Server 8.8.8.8 hinterlegt. Schlug ein Ping fehl, wechselte die Internet-Verbindung in den Status Offline.
  Es werden jetzt die folgenden DNS-Server für die Heartbeat-Tests verwendet. Dabei werden jeweils drei Ping-Pakete abgesetzt, wovon mindestens eines beantwortet werden muss.
  - 8.8.8.8
  - 9.9.9.9
  - 1.1.1.1

LCOS FX-Änderungen 10.5 RU3

Neue Features

- **Unterstützung der LANCOM R&S®Unified Firewall UF-60**
  Volle UTM-Performance in kleinen Installationen
- **DHCP-Refresh**
  - DHCP Lease Monitoring: Die aktuell vergebenen DHCP Leases lassen sich einsehen.
  - Neue DHCP-Server-Optionen: Routen, PXE- und Proxy-Einstellungen können zum Client gepusht werden.
  - Mischbetrieb DHCP-Server und -Relay möglich: Es kann pro Netzwerkinterface separat konfiguriert werden, ob DHCP-Server oder -Relay aktiv sein soll.
- **mDNS-Relay**
  Zur Geräte-Erkennung innerhalb des Netzwerks kann die Unified Firewall mDNS-Anfragen zwischen lokalen Netzwerken weiterleiten.
- **Route-based IPsec**
  Tunnel mit identischen Policies können eingerichtet und über Routen ausgewählt werden.
- **Lizenzablaufverhalten**
  - Übergangsphase bis 30 Tage nach Lizenzablauf: Die Konfiguration bleibt editierbar, es wird bei jeder Änderung eine Warnung ausgegen.
  - Ab 30 Tage vor Lizenzablauf warnt LCOS FX in der Kopfzeile und beim Einloggen in die Administrationsoberfläche.
  - Konfigurierbares Verhalten der UTM-Features bei Lizenzablauf: Es können Web- und Mailverkehr blockiert oder ohne UTM-Filter erlaubt werden.
  - Bei Lizenzablauf: Es erscheint ein Hinweis auf die abgelaufene Lizenz in der Kopfzeile der Administrationsoberfläche. Nach Ablauf der Übergangsphase ist die Konfiguration weiterhin lesbar, aber nicht mehr editierbar.

Korrekturen

- Bei einer VPN-Client Verbindung, welche den gesamten Datenverkehr durch die Firewall sendete und zudem den Content Filter verwendete, wurde bei blockierten Webseiten keine Sperr-Seite der Firewall angezeigt.
- Wenn in einer Firewall-Konfiguration VLANs auf Ethernet-Schnittstellen gebrückt waren, konnte dies beim Zurückspielen einer Backup-Konfiguration dazu führen, dass der Dienst ‚gpNetworkd' nicht mehr startete. In der Folge war ein Zugriff auf die Firewall nicht mehr möglich.
- Bei Verwendung des Mail-Proxy konnte es vorkommen, dass E-Mails mit bestimmten Zeichen im Betreff (z.B. Herzen oder Sterne) per POP3 bzw. POP3s nicht abgerufen werden konnten.
  Es konnte ebenfalls vorkommen, dass der Mail-Proxy empfangene E-Mails nicht decodieren konnte und diese dann nicht weiterleitete.
- Nach dem Import einer Backup-Konfiguration erschien beim ersten Login ein Fenster, in welchem man dazu aufgefordert wurde, entweder die vorhergehende Sitzung zu beenden oder die Konfiguration im ‚Nur Lesen'-Modus zu öffnen. Diese Meldung wurde entfernt, und es ist der normale Konfigurationszugriff auf die Firewall möglich.

- Wenn eine E-Mail spezielle Unicode-Zeichen enthielt, konnte dies dazu führen, dass der Virus-Scan für diese E-Mail fehlschlug.
- Bei Abfrage der SNMP-IDs des Mail-Proxy für die Zähler ‚Spam' und ‚Virus' wurde immer der Wert ‚0' zurückgegeben.
- Wurden bei aktiviertem Mail-Proxy E-Mails mit Zeichen empfangen, welche nicht im ASCII Zeichensatz enthalten sind und nicht in Unicode konvertiert werden konnten (z.B. kyrillisch oder E-Mails mit Umlauten), konnten diese E-Mails per POP3 bzw. POP3s nicht abgerufen werden. Dies führte dazu, dass auch alle nachfolgenden E-Mails per POP3 nicht abgerufen werden konnten.
- Ein Zertifikats-Request konnte nicht erstellt werden, da ein Klick auf ‚Erzeugen' keine Reaktion zeigte.
- In Szenarien mit speziellen Kombinationen von Desktop-Objekten und Firewall-Regeln kam es nach einer Änderung der Firewall-Regeln zu einer vollständigen Auslastung der CPU durch den für die Firewall zuständigen Dienst (xrulesd). Weiterhin verwendete der Dienst immer mehr Speicher und gab diesen nicht mehr frei. Dies führte nach einiger Zeit zu einem unvermittelten Neustart der Firewall.

LCOS FX-Änderungen 10.5 RU2

Neue Features

- **Unterstützung der LANCOM R&S®Unified Firewalls UF-160 und UF-260**
  Die neue Generation der Desktop LANCOM R&S®Unified Firewalls mit einem deutlichen Performance-Sprung ermöglicht bereits ab der UF-160 den Einsatz aller UTM-Features. Die UF-260 ist als erste Desktop LANCOM R&S®Unified Firewall mit einem dedizierten SFP-Port ausgestattet.
- **Management-Bericht**
  Der neue Management-Bericht ermöglicht eine regelmäßige tabellarische und/oder graphisch aufbereitete Übersicht via PDF oder HTML. Neben der aktuellen Desktopkonfiguration und der Darstellung aller Regeln können auch Sicherheitsstatistiken eingebunden werden (z.B. blockierte Verbindungen/Inhalte, aufgerufene/blockierte Domains / Traffic pro Quelle).
- **Lizenzablaufverhalten**
  - Ab 30 Tage vor Lizenzablauf warnt LCOS FX in der Kopfzeile und beim Einloggen in die Administrationsoberfläche
  - Konfigurierbares Verhalten der UTM-Features bei Lizenzablauf:
    Es können Web- und Mailverkehr blockiert oder ohne UTM-Filter erlaubt werden.
  - Bei Lizenzablauf:
    Es erscheint ein Hinweis auf die abgelaufene Lizenz in der Kopfzeile der Administrationsoberfläche.
    Die Konfiguration ist weiterhin lesbar, aber nicht mehr editierbar.
  - Ab LCOS FX 10.5 RU 3 Übergangsphase bis 30 Tage nach Lizenzablauf:
    Die Konfiguration bleibt editierbar, es wird bei jeder Änderung eine Warnung ausgegeben.

Weitere Verbesserungen

- Umsetzung des LANCOM und R&S® Co-Brandings
- Verbesserte Benutzerführung und Standardeinstellungen im Ersteinrichtungs-Assistenten
- Nach Abschluss des Ersteinrichtungs-Assistenten wird sofort auf Firmware-Updates geprüft.
- Angepasster Info-Bereich im Web-Client mit der Möglichkeit, die Einstellungsdialoge direkt aufzurufen
- Einträge in der HTTP(S) Proxy Whitelist können gruppiert werden und enthalten eine optionale Beschreibung.
- Zertifikatsexport mit .crt Endung für direkten Import unter Windows

Korrekturen

- Im Menü ‚Benutzerauthentifizierung / Nicht zugewiesen' war im minimierten Zustand das Wort ‚Benutzer-authentifizierung' in der Überschrift des Konfigurationsdialoges nur zur Hälfte lesbar.
- Die Content-Filter-Kategorien wurden in der deutschsprachigen Benutzeroberfläche in Englisch dargestellt.
- Der Import von Administrator-Konten für den Zugriff auf den Webclient schlug fehl, wenn die Konten aus einer vorherigen Firmware-Version exportiert wurden.
- Nach einem Firmware-Update von LCOS FX 10.5 auf LCOS FX 10.5 RU1 wies eine vorher mit Einträgen gefüllte Liste im Menü ‚UTM / Reverse-Proxy / Frontends' keine Einträge mehr auf.
- Bei Verwendung des SMTP-Proxy konnte es vorkommen, dass eingehende E-Mails nicht weitergeleitet wurden. Vom Proxy wurde dann die die Fehlermeldung „UnicodeDecodeError: ‚utf-8' codec can't decode byte xxx in position" ausgegeben.
- Wurde der Zugriff per SSH für einen VPN-Tunnel (IPSec) erlaubt, erfolgte eine Freischaltung des Protokolls TFTP für alle Verbindungen (auch WAN-Verbindungen).
- Die Performance wurde auf das Niveau der vorigen Firmware-Versionen angehoben.
- In einem Szenario mit einem VPN SSL Bridging Server konnte nur der erste VPN SSL Bridging Client eine Verbindung zu einer Gegenstelle aufbauen. Verbindungen weiterer VPN SSL Bridging Clients zur gleichen Gegenstelle kamen nicht zustande.
- Bei Verwendung des IMAP-Proxy konnte es vorkommen, dass per IMAP abgerufene E-Mails falsch encodiert zugestellt wurden und in der Folge vorhandene Datei-Anhänge nicht lesbar waren.

LCOS FX-Änderungen 10.5 RU1

Verhalten bei Lizenzablauf

Wie bisher lassen sich nach dem Ablauf der Nutzungslizenz keine Änderungen an der Firewall-Konfiguration vornehmen. Diese ist nun allerdings weiter einsehbar. Ergänzend wurde ein klarer Dialog in das Interface integriert, der eine direkte Verlinkung zur Lizenzverlängerung enthält.

Neue Features

- **VPN-Profil-Portal**
  Das neue externe Benutzerportal bietet eine einfache und sichere Methode, VPN-Profil-Dateien für Mitarbeiter zur Verfügung zu stellen. Von zu Hause oder unterwegs können Mitarbeiter sich mit ihrem gewohnten Active Directory- oder LDAP-Login an der Firewall anmelden und ihre VPN-Profil-Datei herunterladen.
- **Wake-On-LAN**
  Die Firewall kann ab sofort PCs im internen Netzwerk per Wake-On-Lan aufwecken. Dies ist zum Beispiel sinnvoll bei Mitarbeitern im Home Office, die von zu Hause aus per VPN auf dedizierte PCs innerhalb des Firmennetzes zugreifen. Das Versenden der WoL-Pakete findet bei der Anmeldung am internen Benutzerportal statt.
- **LDAP-TLS**
  Verbindungen zwischen der Firewall und einem ActiveDirectory- oder LDAP-Server können jetzt mithilfe des TLS Protokolls gesichert werden.

Korrekturen

- Zwecks Fehlervermeidung gibt es eine Prüfung, ob das entfernte Netzwerk einer IPSec-Verbindung mit dem lokalen Netzwerk kollidiert. Es konnte dabei vorkommen, dass eine Kollision mit der Default-Route (0.0.0.0/0) erkannt und eine entsprechende Fehlermeldung ausgegeben wurde.
- Wurde ein Applikations-Filter-Profil in einem Desktop-Objekt hinterlegt, konnte es vorkommen, dass nicht alle Firewall-Regeln erstellt wurden. Dies führte dazu, dass die Kommunikation nicht oder nur eingeschränkt möglich war.
- Wurden bei aktivierter IDS/IPS große Dateien per SMB übertragen, stieg der Speicher-Verbrauch immer weiter an und wurde nicht wieder freigegeben. Dies konnte zu einem unvermittelten Neustart oder zu einem Einfrieren des Gerätes führen.
- Bei gleichzeitiger Verwendung eines VLAN auf einer Bridge und des HTTP-Proxy war keine Verbindung zum Internet möglich.
- Beim Erstellen einer Desktop-Regel über das Alarmprotokoll konnte es in Einzelfällen vorkommen, dass das falsche Quell-Objekt vorgeschlagen wurde.
- Im Alarmprotokoll gab es keine Möglichkeit, eine IDS/IPS-Regel aus einer Alarmmeldung zu erstellen.
- Die Content-Filter-Regeln für LDAP-Gruppen, bei welchen ein intransparenter Proxy und Client-Authentifizierung verwendet wurden, waren funktionslos.
- Bei einem Neustart der Firewall wurden die Zertifikate zur Kommunikation mit der LMC gelöscht. In der Folge wurde die Firewall nach dem Neustart in der LMC als ‚Offline' angezeigt und konnte nicht mehr von der LMC verwaltet und überwacht werden.

- Ein Code zum Override des Content-Filters, welcher in der englischen Bedienoberfläche erstellt wurde, war funktionslos.
- Es konnten keine Änderungen an den Zeit-Einstellungen bzw. Zeit-Tabellen für Desktop-Regeln abgespeichert werden.
- In der Sysinfo-Ausgabe einer UF-910 wurde auch der Raid-Status angegeben. Hierdurch war die Sysinfo-Ausgabe sehr unübersichtlich.
- Eine 10-stelllige Signatur-ID konnte bei aktiviertem IDS/IPS nicht ignoriert werden, weil das System nur 9-stellige Signatur-IDs erlaubte.
- Es konnte in seltenen Fällen vorkommen, dass der Antivirus-Dienst nicht gestartet werden konnte, weil ein anderer Dienst den Start verhinderte. In der Folge war der Web-Proxy funktionslos.
- In einigen Konfigurationsfeldern fehlten die Platzhalter-Texte mit Vorschlägen zur Eingabe, oder die Texte waren fehlerhaft.
- Wenn die Liste mit konfigurierten IPSec-VPN-Verbindungen expandiert wurde, konnte es vorkommen, dass einige Icons (z.B. das Löschen-Icon) nicht angezeigt wurden.
- Die Konfigurationsoberfläche zeigte WAN-Verbindungen, bei welchen DHCP verwendet wurde, als Offline an, obwohl diese aufgebaut waren.

LCOS FX-Änderungen 10.5

Neue Features

- **IMAP Proxy**

  Ab LCOS FX 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 Endkunden, die ihre E-Mails nicht selbst hosten, die gewohnte E-Mail-Sicherheit mit Anti-Malware und Anti-Spam vollständig nutzen.

- **Application Based Routing**

  Application Based Routing ermöglicht, auf Basis der PACE2 DPI-Engine das Routing erkannter Protokolle und Applikationen zu bestimmen. Dabei gibt es drei Möglichkeiten: Die Selektion einer bestimmten ausgehenden Verbindung in Multi-WAN-Szenarien (z.B. Streaming-Dienste über die langsamere Leitung, VPN über die schnellere), das Ausnehmen bestimmter Applikation vom Proxy (z.B. vertrauenswürdige Cloud-Applikationen) und das Ausnehmen bestimmter Applikationen von IPSec-Tunneln (z.B. für Zweigstellen, die den gesamten Internetverkehr an die Zentrale schicken, aber bestimmte vertrauenswürdige Applikationen davon ausnehmen möchten).

Weitere Verbesserungen

- **Desktop-Suche**

  Der Desktop-Tags-Filter wird erweitert zum Desktop-Filter. Es kann sowohl nach Desktop-Objekten als auch nach Desktop-Verbindungen gesucht werden. Nicht zutreffende Objekte / Verbindungen werden ausgeblendet. Es kann nach einer Vielzahl von Parameter gesucht werden, u.a. Name, IP-Addresse, dazugehörige VPN-Verbindung oder Proxy-Flag.

- **Regeln aus dem Protokoll erstellen**

  Sie können Regeln für abzuweisende Zugriffe direkt aus dem Alarm- und Systemprotokoll erstellen. Falls die Firewall mit dem aktuellen Regelwerk erwünschten Netzwerkverkehr blockiert, können Sie direkt im Protokoll mit wenigen Klicks eine neue Regel für diesen Netzwerkverkehr zum Regelwerk hinzufügen. Sowohl das initiale Erstellen des Regelwerks, als auch die Pflege werden dadurch deutlich erleichtert und beschleunigt.

- **Mehrere angemeldete Administratoren**

  Mehrere Administratoren können zur gleichen Zeit am LANCOM R&S®Unified Firewall Webclient angemeldet sein. Der zuerst angemeldete Administrator verfügt über Schreibrechte, kann also Änderungen an der Konfiguration vornehmen. Weitere Administratoren haben ausschließlich Leserechte. Meldet sich der erste Administrator ab, geht das Schreibrecht an den nächsten über. Dies vereinfacht deutlich die Administration von LANCOM R&S®Unified Firewalls in größeren Administrations-Teams.

- **Wiederherstellungspunkte**

  Mittels der Wiederherstungspunkte ist es müglich, die LANCOM R&S®Unified Firewalls nach einem Upgrade wieder auf die Ursprungsversion zurückzusetzen.

- **Content-Filter-Codes**

  Die Verwaltung des Content-Filters wurde um Codes erweitert, mit denen Benutzer trotz des Filters geblockte Seiten innerhalb bestimmter Zeiten durch die Eingabe des jeweiligen Codes ansehen können. Diese Ausnahme-Codes können von Endnutzern im Endnutzerportal erstellt werden, wenn diese vom Administrator dafür freigeschaltet wurden. So können zum Beispiel Vorgesetzte bei Bedarf für ihren Bereich Ausnahmen für den Content-Filter ermöglichen.

- **VPN-SSL-Bridging**

  Mittels VPN-SSL-Bridging ist es möglich, zwei oder mehrere Netze an unterschiedlichen Standorten sicher und zuverlässig auf Layer-2 zu verbinden, z.B. um Kommunikation über nicht-IP-basierte Protokolle zu ermöglichen.

Korrekturen

- Nach dem Import einer Backup-Konfigurationsdatei und anschließendem Neustart der Firewall konnte es vorkommen, dass die Einstellungen des Application-Filters nicht geladen wurden.
- Nach einem Update auf die Firmware-Version 10.4 RU1 akzeptierte eine GP-NP-200 Firewall ausschließlich die Lizenz für eine Firewall des Typs UF-900.
- Nach dem Import einer Backup-Konfigurationsdatei und anschließendem Neustart der Firewall konnte es vorkommen, dass im Application-Filter die Kategorien-Liste fehlte.
- In Einzelfällen konnte es bei deaktiviertem Application-Filter dazu kommen, dass der Speicherverbrauch des

zuständigen Dienstes (gpAppFilterd) immer weiter anstieg.

- Bei Verwendung der Funktion ‚Single Sign On' wurden keine Firewall-Regeln für Benutzer mit einem Umlaut oder dem Buchstaben „ß" im Namen erstellt.
- Ein Konfigurations-Backup konnte in ein Gerät mit einer älteren Firmware-Version importiert werden. Dies führte im Regelfall zu einer nicht funktionsfähigen Konfiguration.
  Es wird jetzt während des Import-Vorgangs die Version geprüft und der Import abgelehnt, wenn die Firmware-Version des Gerätes älter ist als die des Konfigurations-Backups.
- Wurde ein VPN-Profil für den Advanced VPN Client erstellt und exportiert, konnte mit diesem keine VPN-Verbindung aufgebaut werden, da beim Export vor den ‚Local Identifier' die Zeichenkette „email:" eingefügt wurde.

4. Installationsanleitung zum Update auf LCOS FX 10.6 RU4

Hinweis 1:

Falls Sie noch keine funktionierende 10.2.0 Firewall-Installation besitzen, richten Sie zunächst eine einfache 10.2.0 Firewall-Installation mit Internetverbindung ein (siehe Beileger „Erste Schritte zur Inbetriebnahme“). Eine Internetverbindung ist notwendig, um alle weiteren Updates zu erhalten.

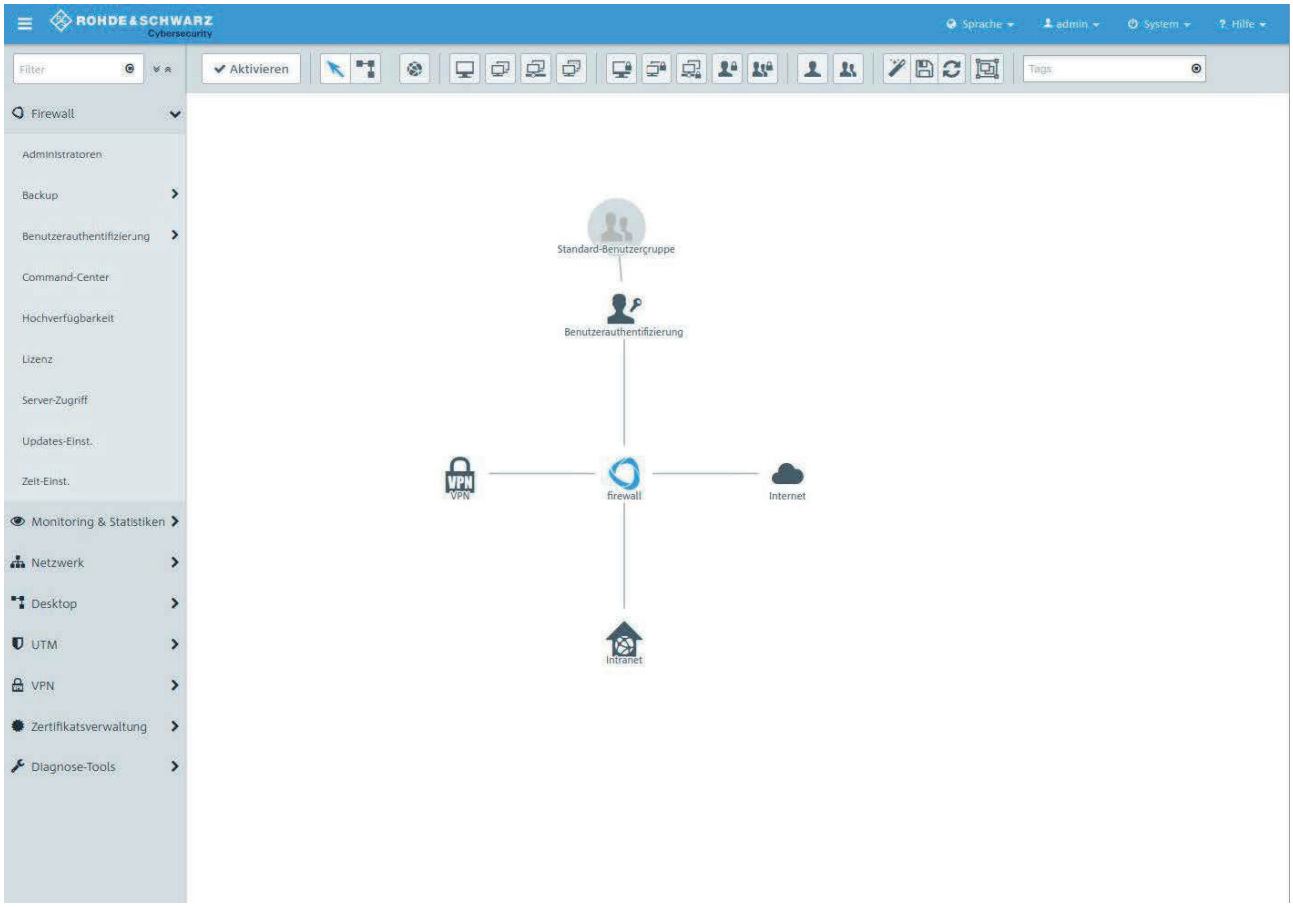
Über den Auto-Updater in der Weboberfläche Ihrer LANCOM R&S®Unified Firewall ist jeweils die nächsthöhere Minor Update-Version zur schrittweisen Aktualisierung verfügbar.

Führen Sie dazu die nachfolgend in diesem Dokument beschriebenen Schritte durch, um Ihr Gerät auf die neueste LCOS FX-Version zu aktualisieren.

Hinweis 2:

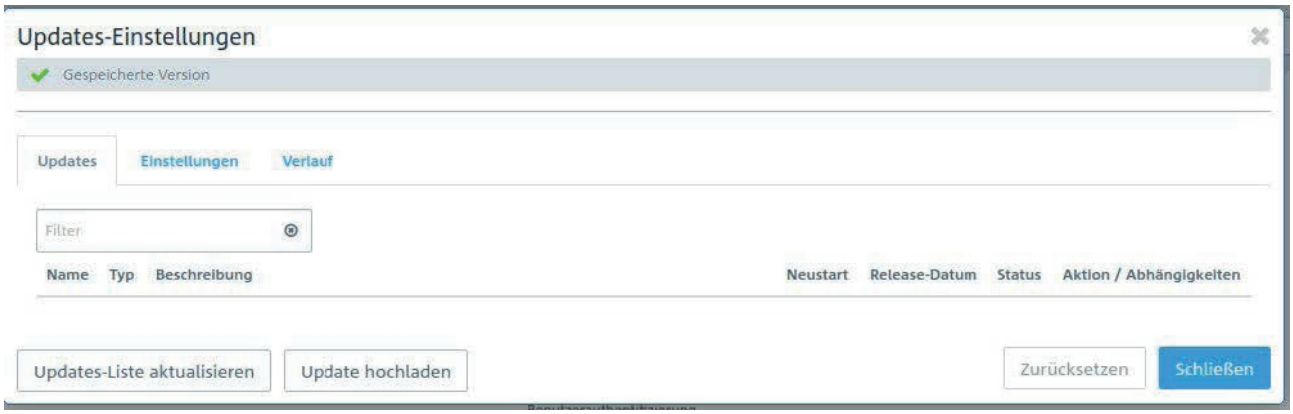
Um Arbeitsabläufe nicht zu behindern, führen Sie das Update zunächst in einer Testumgebung aus und nicht in einem realen Setting.

Wählen Sie in der Navigationsleiste auf der linken Seite unter dem ersten Punkt „Firewall“ den Eintrag „Updates Einst.“.

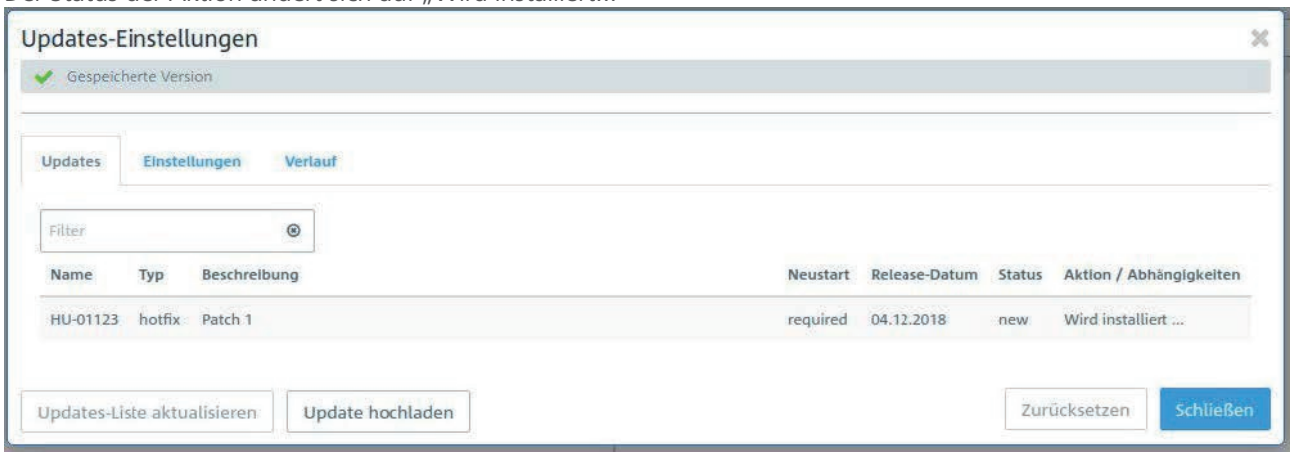


LANCOM Systems

Im sich öffnenden Fenster „Updates-Einstellungen“ klicken Sie im Reiter „Updates“ auf die Schaltfläche „Updates-Liste aktualisieren“.

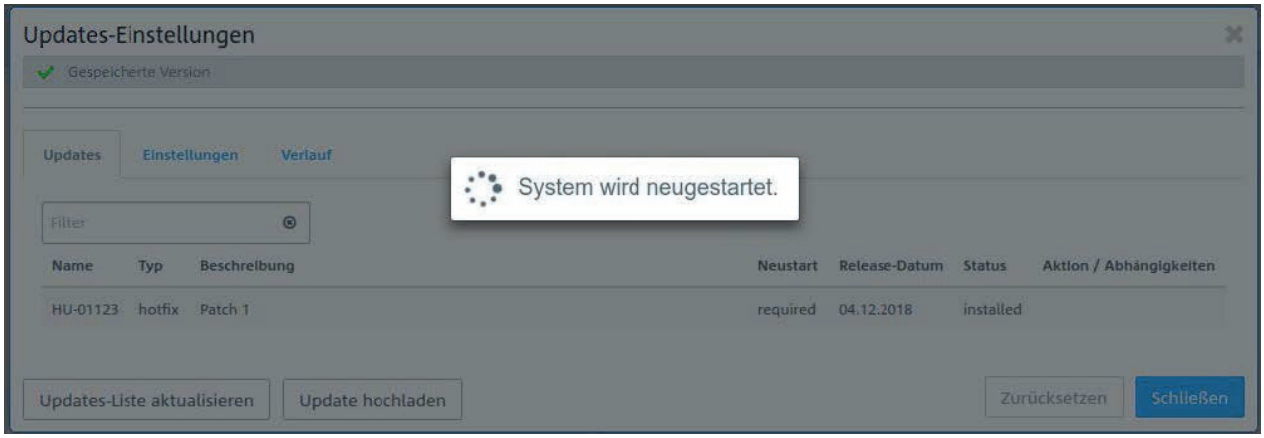


Wählen Sie die zu installierende Firmware-Datei aus der Liste und klicken Sie auf “Installieren”.
Der Status der Aktion ändert sich auf „Wird installiert...“

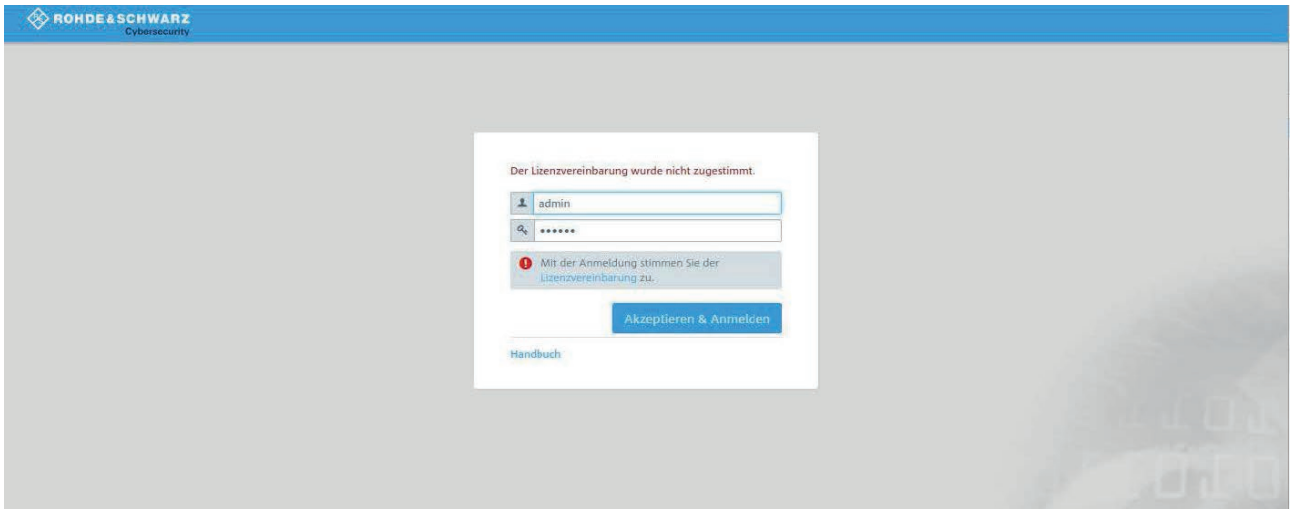


Nach Abschluss der Installation erscheint ein Popup-Dialogfenster, in welchem Sie aufgefordert werden, die Firewall neu zu starten. Bestätigen Sie mit „Neustarten“.

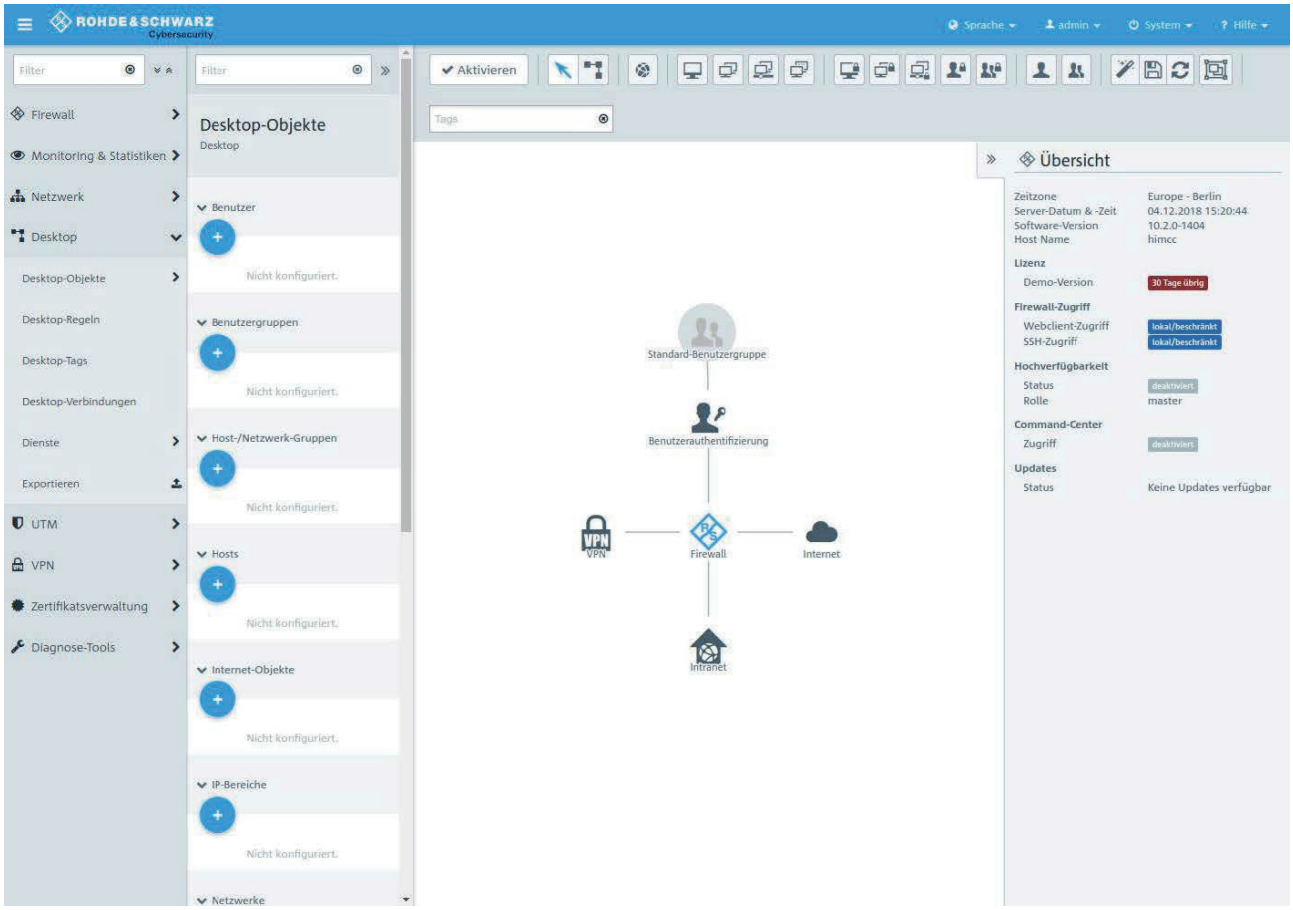
Das System wird neugestartet.



Nach dem Neustart der Firewall erscheint das Login-Fenster. Bei der Eingabe Ihrer Anmeldedaten werden Sie gleichzeitig aufgefordert, der Lizenzvereinbarung zuzustimmen.



Nach dem Anmeldevorgang wird die Oberfläche Ihrer LANCOM R&S®Unified Firewall geöffnet. Auf der rechten Seite sehen Sie die Info-Bar. Hier sehen Sie u.a. Informationen zur aktuellen Software-Version.



LANCOM Systems

5. Weitere Informationen

- Backups der Versionen 9.6, 9.8 und 10.X werden unterstützt.
- Geräte mit weniger als 4 Gbyte RAM können nicht alle UTM-Features zur gleichen Zeit ausführen.

6. Bekannte Probleme

- Systemprotokolle und Auditprotokolle werden im High-Availability-Modus nicht synchronisiert.
- Einige Monitoring-Informationen sind noch nicht verfügbar:
  - Anmeldestatus der Benutzer
  - Last der Netzwerkschnittstellen

7. Haftungsausschluss

Die LANCOM Systems GmbH übernimmt keine Gewähr und Haftung für nicht von der LANCOM Systems GmbH entwickelte, hergestellte oder unter dem Namen der LANCOM Systems GmbH vertriebene Software, insbesondere nicht für Shareware und sonstige Fremdsoftware.