LANCOM Release Notes

LCOS FX

10.5 RU2

LANCOM Systems GmbH
Adenauerstrasse 20 / B2
52146 Würselen
Germany

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

01.10.2020, CBuersch

Inhaltsübersicht

LANCOM Systems

1. Einleitung

LCOS FX ist das Betriebssystem für alle LANCOM R&S®Unified Firewalls. Im Rahmen der von den Produkten vorgegebenen Hardware ist die jeweils aktuelle LCOS FX-Version für alle LANCOM R&S®Unified Firewalls verfügbar und wird kostenlos zum Download angeboten.

Dieses Dokument beschreibt die Neuerungen der LCOS FX Software Release 10.5 RU2 sowie die Änderungen und Verbesserungen zur Vorversion.

2. Unterstützte Hardware

Version 10.5 RU2 unterstützt die folgenden Hardware Appliances:

- LANCOM R&S®Unified Firewalls UF-50/100/160/200/260/300/500/900/910
- 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 10.5 RU2 unterstützt die folgenden virtuellen Appliances:

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

Version 10.5 RU2 unterstützt die folgenden Hypervisor:

- Vmware ESX
- Microsoft HyperV
- Oracle Virtualbox
- KVM

3. Historie LCOS FX

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 freige-

schaltet 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.

LCOS FX-Änderungen 10.4 RU3

Verbesserungen

- Vorbereitung der Möglichkeit zur Wiederherstellung der alten Version nach einem Firmware-Update. Einrichtung unter ‚Firewall / Update Einstellungen / Automatische Wiederherstellung'. Dieses Feature wird erst aktiv für das zukünftige Update von LCOS FX 10.4 auf LCOS FX 10.5.

Korrekturen

- Nach einer Firmware-Aktualisierung auf LCOS FX 10.4 RU1 wurden folgende Bezeichnungen und Texte mit der jeweiligen UUID (Universally Unique Identifier) des Parameters ersetzt:
  - die Namen von einigen Diensten, auch innerhalb einer Dienste-Gruppe
  - die Beschreibung von Firewall-Regeln
- Desktop-Objekte, welche von der LMC angelegt wurden, ließen sich nicht kopieren.
- Es konnte vorkommen, dass die Unified Firewall einen Benutzer als ‚angemeldet' führte, obwohl dieser bereits von der Firewall abgemeldet war. In der Folge wurden die benutzerspezifischen Regeln für IP-Adressen geschrieben.
- Wenn in einer Konfigurations-Sicherung eine VPN-Verbindung mit abgelaufenem Zertifikat enthalten war, konnten beim Import vom IPSec-Dienst alle nachfolgenden VPN-Tunnel nicht geladen werden.
  Dies konnte dazu führen, dass bei einer VPN-Verbindung mit abgelaufenem Zertifikat nicht alle VPN-Tunnel geladen werden konnten.
- Nach Ablauf eines VPN-Zertifikats konnte die zugehörige VPN-Verbindung nicht deaktiviert werden.
- Wurde eine Konfigurationssicherung importiert, konnte es dazu kommen, dass VPN-Verbindungen nicht deaktiviert und der Name der Verbindung nicht editiert werden konnten.

LCOS FX-Änderungen 10.4 RU2

Verbesserungen

- Die IPSec EAP-Konfigurationsmöglichkeiten wurden erweitert, um EAP bei Verbindungen mit LANCOM Advanced VPN Client, Windows 10 und iOS zu ermöglichen.
- Unterstützung der LANCOM R&S®Unified Firewall UF-910

Korrekturen

- Nach einer Aktualisierung der Firmware auf LCOS FX 10.4.1 wurden VPN-Hosts auf dem Desktop ohne Icon-Grafik angezeigt.
- In einer IPSec VPN-Verbindung führte ein PSK mit maximal 63 Zeichen dazu, dass die VPN-Verbindung nicht aufgebaut werden konnte.
- Wenn in einer IPSec VPN-Verbindung im Feld ‚Listening-IP-Adressen' eine lokale IP-Adresse eingetragen war und eine Netzwerkverbindung mit mehreren lokalen IP-Adressen verwendet wurde, nutzte die Unified Firewall alle dort angegebenen lokalen IP-Adressen als Listening-Adressen. Die Listening-IP-Adressen werden jetzt priorisiert behandelt.
- Das DPD-Verhalten wurde mit „Trap policies" umgesetzt, was dazu führte, dass VPN-Tunnel nur erneut aufgebaut wurden, wenn Daten durch die Tunnel gesendet werden sollten. Dieses Verhalten verursachte jedoch in einigen VPN-Szenarien Funktionsstörungen. Das DPD-Verhalten wird nun mit einer „Restart policy" umgesetzt. Stellt die Unified Firewall per DPD fest, dass die Gegenseite nicht mehr reagiert, versucht diese den VPN-Tunnel erneut aufzubauen.
- Wenn an einer Netzwerk-Schnittstelle Konfigurationsänderungen durchgeführt wurden, welche dazu führen konnten, dass kein WebClient-Zugriff auf die Unified Firewall mehr möglich war, erschien kein Warn-Hinweis.
- Wurde im Menü „VPN/IPSec/Verbindungen" eine neue VPN-Verbindung erstellt, eine Vorlage ausgewählt und anschließend über die Escape-Taste das Menü verlassen, war das Menü bei erneutem Aufruf über die Menüleiste in der Kopfzeile leer.
- Im Menü „Netzwerk/Verbindungen/Netzwerk-Verbindungen" konnte das Gateway fälschlicherweise in CIDR-Schreibweise (Classless Inter Domain Routing) angegeben werden. Die Konfiguration ließ sich aber nicht zurückschreiben.
- Nach Ablauf der Lizenz für die Unified Firewall verlor die Firewall die Verbindung zur LANCOM Management Cloud, sodass über die Detail-Konfiguration in der LMC kein Zugriff auf das Webinterface mehr möglich war und somit keine neue Lizenz eingespielt werden konnte.
- Im Menü „Monitoring & Statistiken/Statistiken" konnte in den Statistiken für blockierte Inhalte und blockierte Verbindungen nicht gescrollt werden, sodass nicht alle Daten einsehbar waren.
- Wurde auf dem Desktop ein Netzwerk-Objekt mit einem Netzbereich angelegt, welcher der Unified Firewall nicht bekannt war, gab diese eine Warnmeldung aus, dass das angelegte Netzwerk über die verwendete Schnittstelle gegebenenfalls nicht erreichbar sein könnte.
  Die Warnmeldung wird jetzt nicht mehr angezeigt.
- Obwohl LDAP-Gruppen in der Unified Firewall hinterlegt waren, konnten in einer Benutzergruppe auf dem Desktop lediglich einzelne Benutzer ausgewählt werden, nicht aber die vorhandenen Benutzergruppen.

LCOS FX-Änderungen 10.4 RU1

Verbesserungen

- Das Verhalten des Webclients beim Verbindungsverlust zur Firewall wurde verbessert.
- Nach dem Auto-Logout aus dem Webclient wird der zuletzt bearbeitete Dialog wieder geöffnet.

Korrekturen

- Es wurde das Problem behoben, dass nach Einspielen eines Backups in manchen Fällen der Ersteinrichtungswizard gestartet wurde.
- Ein Problem mit Serpent und Twofish Ciphers und IPSec wurde behoben.
- Die Anzahl der IPSec Retransmission-Versuche wurde verringert.
- Ein Problem mit Kollisionswarnungen bei IPSec-Verbindungen wurde behoben.
- Es wurde das Problem behoben, dass Anfragen auf Port 3439 beantwortet wurden.
- Ein Fehler bei der Konvertierung von VPN-Netzwerk-Desktop-Objekten wurde behoben.
- Fehlerbehebung bei der Nutzung von Network Discovery Tools
- Die Anzahl der Log-Nachrichten aus der Anti-Malware Engine wurde verringert.

LCOS FX-Änderungen 10.4

Neue Features

Ersteinrichtungswizard

In unter 5 Minuten die Firewall einrichten, inklusive Internetzugang, lokaler Netze und UTM-Features.

In 4 einfachen Schritten konfiguriert der Wizard:

- Hostname der Firewall
- Internetzugang
- Lokale Netzwerke
  - IP-Addressen
  - DHCP-Server
  - Regeln für Internetzugang
- UTM-Features (Anti-Malware, IDS/IPS, URL- und Content-Filter)

Integration in die LANCOM Management Cloud

- **SD-SECURITY**
  - Ermöglicht standortübergreifendes Application Managment
  - Einmal pro Netzwerk Applikationszugriffe konfigurieren und einfach auf alle Standorte ausrollen.
- **Monitoring**
  - Gerätestatus (Hardwareauslastung, Schnittstellendurchsatz, ..)
  - Sicherheitsstatus (blockierte Verbindungen, blockierte Inhalte wie Malware)
- **Webclient-Tunnel**
  - Einfacher Zugriff auf die komplette Managementoberfläche der Firewall

- **Cloud-ready**
  - Ab LCOS FX 10.4 sind alle neu ausgelieferten Unified Firewalls Cloud-ready.
  - Einfach anschließen und sofort komplett über die LMC managen

Neue IPSec-Implementierung

- Komfortable Bedienung durch wiederverwendbare Sicherheitsprofile für IKE und ESP
- Vorgefertigte Profile für gängige Clients (Windows 10, iOS, Android, LANCOM Advanced VPN Client) und Server (LCOS FX 10.4, LCOS ab 10.30)
- Export der Konfiguration für den LANCOM Advanced VPN Client
- Konfiguration mehrerer Netze in einer Verbindung zur Reduktion des Konfigurationsaufwands
- Option zur Anbindung externer DHCP- und RADIUS-Server
- Unterstützung von Hub-and-Spoke-Architekturen
- Möglichkeit, die externe Tunnel-IP-Adresse spezifisch zu konfigurieren

E-Mail-Benachrichtigungen

- Direkte Information über wichtige Ereignisse per E-Mail, wahlweise sofort oder aggregiert über Zeit (konfigurierbar pro Ereignistyp)
- Ereignisse
  - Internetverbindung unterbrochen / wiederhergestellt
  - IPSec Site-to-Site-Tunnel unterbrochen / wiederhergestellt
  - High Availability Switch-over
  - Firewall Neustart erwartet / unerwartet
- Optionaler Versand über Mail-Relay
- Optionaler verschlüsselter Versand mittels SMIME

Verbesserungen

- Benutzerspezifische Applikationsfilter-Regeln
  - Kombination von Benutzerauthentifizierung und Applikationsfilter
  - Spezifische Applikationsprofile für einzelne Benutzer oder Gruppen
  - Anbindung an Active-Directory (Zuordnung zu einer Gruppe / Abteilung ergibt direkt die passenden Applikationsfilterregeln)
- Die Konfiguration und Logs können auf den Auslieferungszustand zurückgesetzt werden.
- Der Linux-Kernel wurde aktualisiert auf 4.19.69.
- Die SNMP-Statistiken zeigen nun auch virtuelle Netzwerkschnittstellen, zum Beispiel VLANs an.
- Die SNMP-Statistiken zeigen nun auch Firewall-Alarme an.
- Der Browser lädt den Webclient automatisch neu, wenn die Verbindung verloren wurde.
- Der automatische Logout des Webclient wird auch bei Mausbewegungen zurückgesetzt.
- Die aktuell aktive Lizenz kann jetzt unter Firewall > Lizenz heruntergeladen werden.

Korrekturen

- Es wurde ein Problem in der Speicherverwaltung behoben, das zu unerwarteten Neustarts führen konnte.

- Stabilitätsprobleme bei hoher Anzahl von IPSec-Tunneln wurden behoben.
- Ein Kerberos-Ticket wird jetzt auch bei Großbuchstaben im Hostnamen korrekt erstellt.
- Zu geringer Timeout für TCP-Verbindungen
- Die Statistiken funktionieren auch nach Deaktivieren des High-Avalibility-Modus.
- Der High-Avalibility-Modus wurde für Installationen ohne DNS-Auflösung angepasst.
- Es wurde das Problem behoben, dass der Webproxy unter Umständen nicht startet.
- Verbesserung der Handhabung von Timeouts in der Benutzerauthentifizierung per Weblogin
- Stabilitätsprobleme mit bestimmten VPNSSL Site-to-Site-Verbindungen wurden behoben.
- Anti-Virus auf der UF-50 wird in allen Situationen korrekt deaktiviert.
- Einige überflüssige Logeinträge wurden entfernt.
- Die Handhabung von per DHCP bezogenen DNS-Servern wurde korrigiert.
- Verbesserte Stabilität des Weblogin-Dienstes für Benutzerauthentifizierung
- Die Internet-Verbindung kann im Internet-Objekt sofort nach dem Entfernen wieder ausgewählt werden.
- Alle Firewall-Dienste ignorieren getrennte Internet-Verbindungen.
- Es wurde die automatische Regel entfernt, die TCP mit Verbindungen mit MSS unter 512 blockiert.

Zusätztliche Informationen

- Verschärfte Passwort-Richtlinien für Administratoren des Webclients und für das Konsolen-Passwort
  - mindestens 8 Zeichen
  - mindestens 3 Zeichenklassen (Groß-, Kleinbuchstaben, Ziffern, Sonderzeichen)
- Das Standard-Backup wurde für Auslieferung und Neuinstallation angepasst
  - eth0 bezieht IP-Adresse und Standardgateway per DHCP
  - eth1 bis eth3 aktivieren den DHCP-Server zur vereinfachten Ersteinrichtung
- Die LANCOM Support IPs wurden zu den vorkonfigurierten IPs für Webclient- und SSH-Zugriff hinzugefügt.
- Custom-Skripte werden beim Upgrade deaktiviert.

LCOS FX-Änderungen 10.3.3

Verbesserungen

- Deutsches Handbuch hinzugefügt
- Handbuch auf V10.3 aktualisiert
- Unterstützung für die neue Hardware-Revision der UF-100/200 hinzugefügt

Korrekturen

- Problem behoben, das dazu führen konnte, dass Hardware-Appliances die UUID der virtuellen Maschine im Lizenzdialog anzeigen.
- Problem behoben, das dazu führen konnte, dass die Synchronisation bei Hochverfügbarkeit fehlschlug.
- Problem im Mailproxy behoben, wenn die Client-seitige Verbindung zu früh geschlossen wurde.
- Problem behoben, das dazu führte, dass bereits installierte Patches wieder installierbar waren.

LCOS FX-Änderungen 10.3.2

Korrekturen

- Es wurde ein Problem mit der Lizenzbehandlung behoben, das dazu führen konnte, dass Appliances die Lizenz verlieren
- Der Status von IPsec Site-to-Site wird in allen Fällen korrekt erkannt
- Der DNS-Server wird nach Erhalt des DHCP-Leases korrekt neu gestartet
- Ausführliche Mailproxy-Protokollierung entfernt
- Hochverfügbarkeit behandelt Umlaute in Netzwerkverbindungen nun korrekt

LCOS FX-Änderungen 10.3.1

Verbesserungen

- Sicherheitsupdate des Linux-Kernels auf Version 4.19.53 zur Behebung der Sicherheitslücke CVE-2019-11477

LCOS FX-Änderungen 10.3.0

Neue Funktionen

- Alarmprotokoll
  - Warnmeldungen werden separat protokolliert
    Umfasst blockierte Verbindungen, akzeptierte Verbindungen, Malware, IDS/IPS, Web-Filter, URL-/Contentfilter, Anti-Spam und den Application Filter
  - Komplexe Filterkombinationen vereinfacht durch AND-, OR-, NOT-Operatoren
    Smart-Filter, der die Erstellung präziser Anfragen ermöglicht, indem spezielle Attribute, wie Portnummern und Quell-IP-Adressen zur Suchanfrage hinzugefügt werden können

- Online-Updates im High-Availability-Modus möglich
- Sicherheitsupdate des Linux-Kernels auf Version 4.19.29

Verbesserungen

- Versionsübergreifende Lizenzen
- Verbesserte Leistung der Protokollanzeige
- Drop-down-Listen in der Netzwerkschnittstelle zeigen die dazugehörigen Verbindungen und IP-Adressen an.
- Aktualisierung der vordefinierten Dienste
- Optimierte Bedienbarkeit beim Erstellen von DMZ-Regeln
- Automatische Abmeldung vom Webclient nach 10 Minuten
- Konfigurierbares Verhalten beim Auslaufen der Lizenz
- Verbesserte Stabilität der IPSec-Tunnel
- Verbesserte Stabilität und Leistung des E-Mail-Proxys
- Ausstehende Konfigurationsänderungen der Desktop-Regeln werden beim Abmelden gespeichert.
- Die Log-Datenbank wurde zur Gewährleistung der Systemstabilität auf ca. 8 Gbyte begrenzt; die ältesten Einträge werden gelöscht.

Weitere Informationen

- Das Verhalten bei Ablauf der Lizenz hat sich im Vergleich zu V9.X geändert. Wenn Sie von Version V9.X migrieren, navigieren Sie zu „Firewall" > „Lizenz", um dieses Verhalten zu konfigurieren.
- Standardmäßig suchen LANCOM R&S®Unified Firewalls täglich nach Software-Updates. Navigieren Sie zu „Firewall" > „Updates-Einstellungen", um das Intervall anzupassen.
- Backups der Versionen 9.4 bis 9.8, 10.0, 10.1 und 10.2 werden unterstützt.
- Geräte mit weniger als 4 Gbyte RAM können nicht alle UTM-Features gleichzeitig ausführen.

Entfernte Funktionen

Die folgenden Funktionen sind in Version 10.3.0 nicht verfügbar:

- VPN-Verbindungen über PPTP
- E-Mail-Reporting
- LAN-Accounting
- VPN-SSL-Bridges
- Desktopnotizen
- Dynamisches Routing
- Verbindungsspezifische DNS-Server
- Zentralisierte Verwaltung der LANCOM R&S®Unified Firewalls über das gateprotect Command Center. Nutzen Sie stattdessen das LANCOM R&S®UF Command Center.

LCOS FX-Änderungen 10.2.3

Verbesserungen

- Der Reverse-Proxy unterstützt Outlook Anywhere
- Administratoren können vom HTTP-Proxy akzeptierte Webserver-Chiffren anpassen
- Sicherheitsupdate des Linux-Kernels auf Version 4.14.103
- Verbesserte Verarbeitung großer Contentfilter-Blacklisten
- Verbesserte Responsivität des Infobereichs
- Verbesserte Leistung des Mailproxys
- Reduzierte Festplattenbeanspruchung
- Verbessere Backup-Kompatibilität
- Verbesserter Import von mehrstufigen Zertifikatsketten

LCOS FX-Änderungen 10.2.2

Verbesserungen

- Optimierte Web-Proxy-Logfile-Verarbeitung
- Verbesserte Backup-Migration

LCOS FX-Änderungen 10.2.1

Verbesserungen

- Feingranulare, IP-basierte Zugriffskontrolle für SSH- und Webclient-Management-Schnittstellen
- Konfigurierbare Listening-Ports für SSH- und Webclient-Management-Schnittstellen
- Infobereich mit detaillierten Informationen zu den Desktopknoten
- Whitelist für den E-Mail-Proxy, um bestimmte Sender / Empfänger vom Virenscan auszuschließen
- Konfigurierbares HTTPS-Zertifikat für den Webclient
- Einige veraltete Verschlüsselungsverfahren werden vom SSL-Proxy nicht mehr unterstützt.

LCOS FX 10.2.0

Neue Features

- Integration von Avira Antivirus:
  - Avira Protection Cloud: maschinelles Lernen und Sandboxing
- IDS/IPS:
  - Verbesserte Leistung dank neuer IDS/IPS-Engine
  - Vereinfachte IDS/IPS-Konfiguration mit einer Regelausschlussliste zur Eliminierung falsch-positiver Ergebnisse
- Statistik:
  - Sicherheitsmeldungen
  - Traffic-Zähler
- Protokollierung:
  - Sicherheitsmeldungen
- Upgrade des Web-Proxys:
  - Verbesserte HTTPS-Unterstützung
  - Verbesserte Leistung
- Upgrade des FTP-Proxys
- Upgrade des Reverse-Proxys
- Unterstützung von Link Aggregation/Bonding von Ethernet-Schnittstellen

Verbesserungen

- Durchsuchbares Beschreibungsfeld für Desktop-Objekte und Firewall-Regeln
- Dienste können gruppiert werden.
- Desktopobjekte für „Host-/Netzwerkgruppen“ können Hosts und Netzwerke enthalten.
- Desktopobjekte können getaggt und nach Tags gefiltert werden.
- Desktopkonfigurationen (d.h. eine Übersicht der Desktop-Objekte und Firewall-Regeln) können in die Dateiformate PDF und HTML exportiert werden.
- Verbindungsverfolgung in Echtzeit
- DNS-Suchdomains können über DHCP gepusht werden.
- Der Webclient erlaubt den Offline-Upload von Updates.

4. Installationsanleitung zum Update auf LCOS FX 10.5 RU2

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.

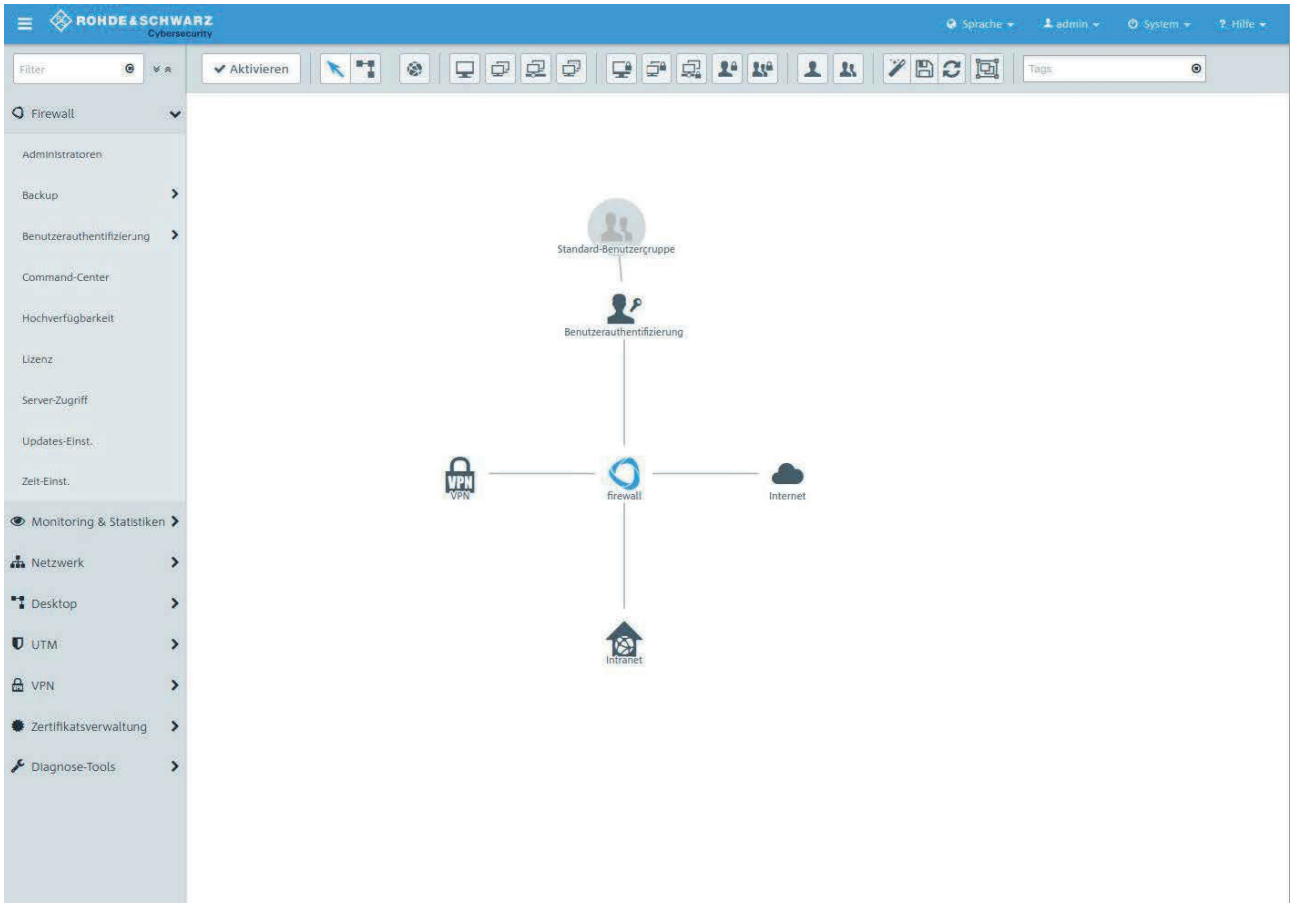
Über den Auto-Updater in der Weboberfläche Ihrer LANCOM R&S®Unified Firewall ist jeweils die nächsthöhere Minor Update-Version zur schrittweisen Aktualisierung verfügbar.

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

Hinweis 2:

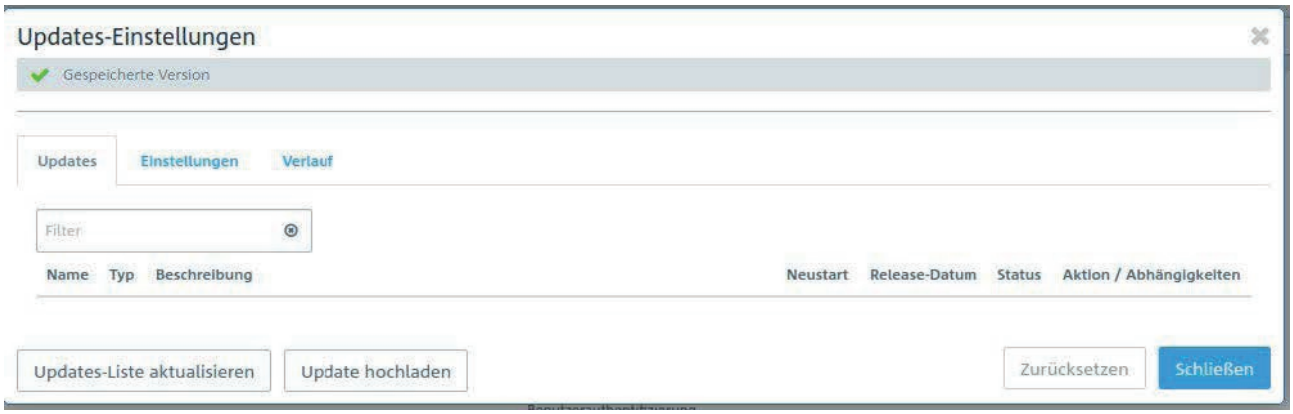
Um Arbeitsabläufe nicht zu behindern, führen Sie das Update zunächst in einer Testumgebung aus und nicht in einem realen Setting.

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“.

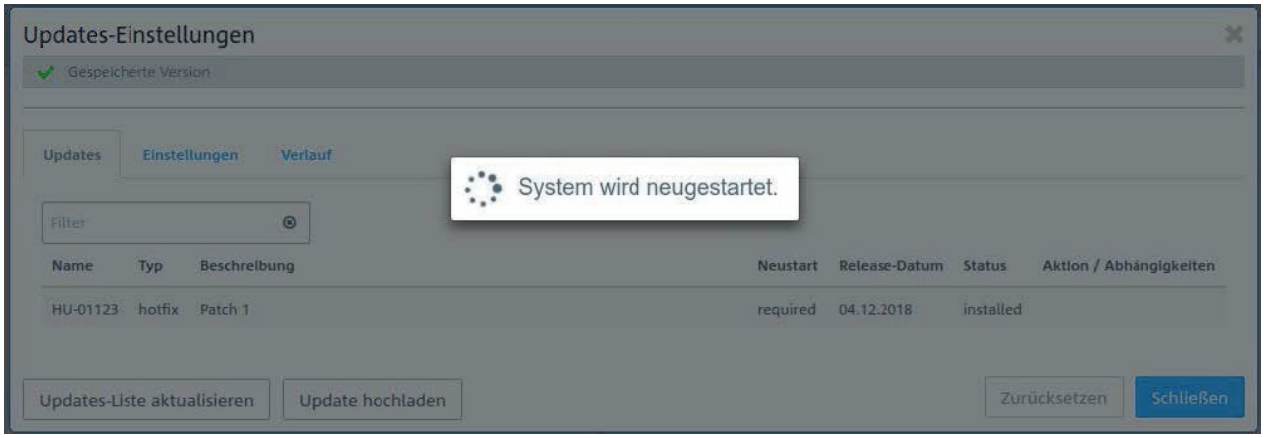


Wählen Sie die zu installierende Firmware-Datei aus der Liste und klicken Sie auf “Installieren”.

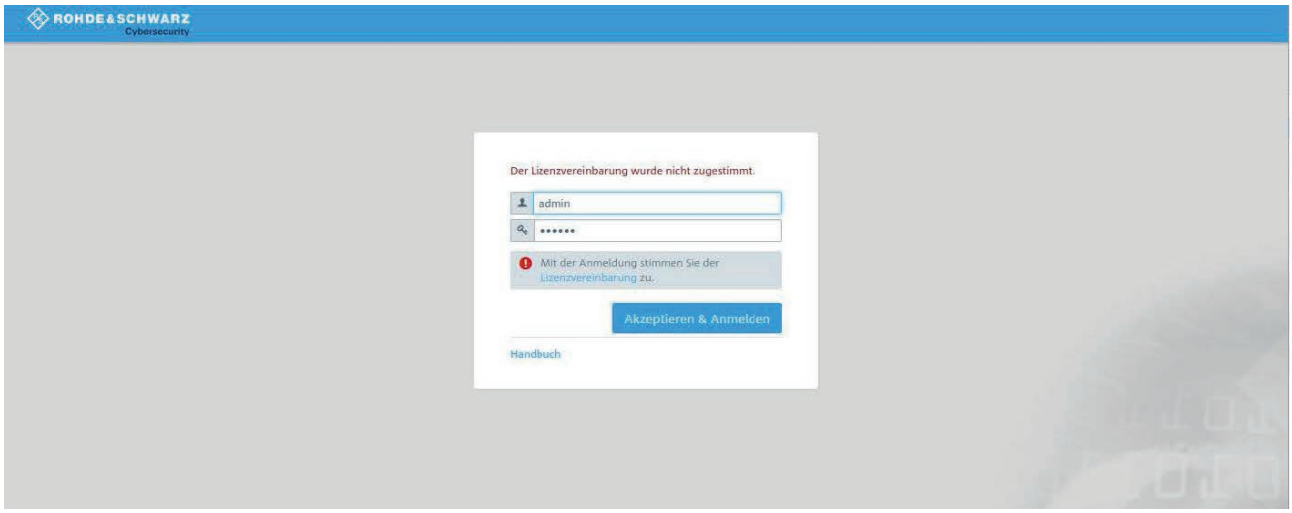
Der Status der Aktion ändert sich auf „Wird installiert...“

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

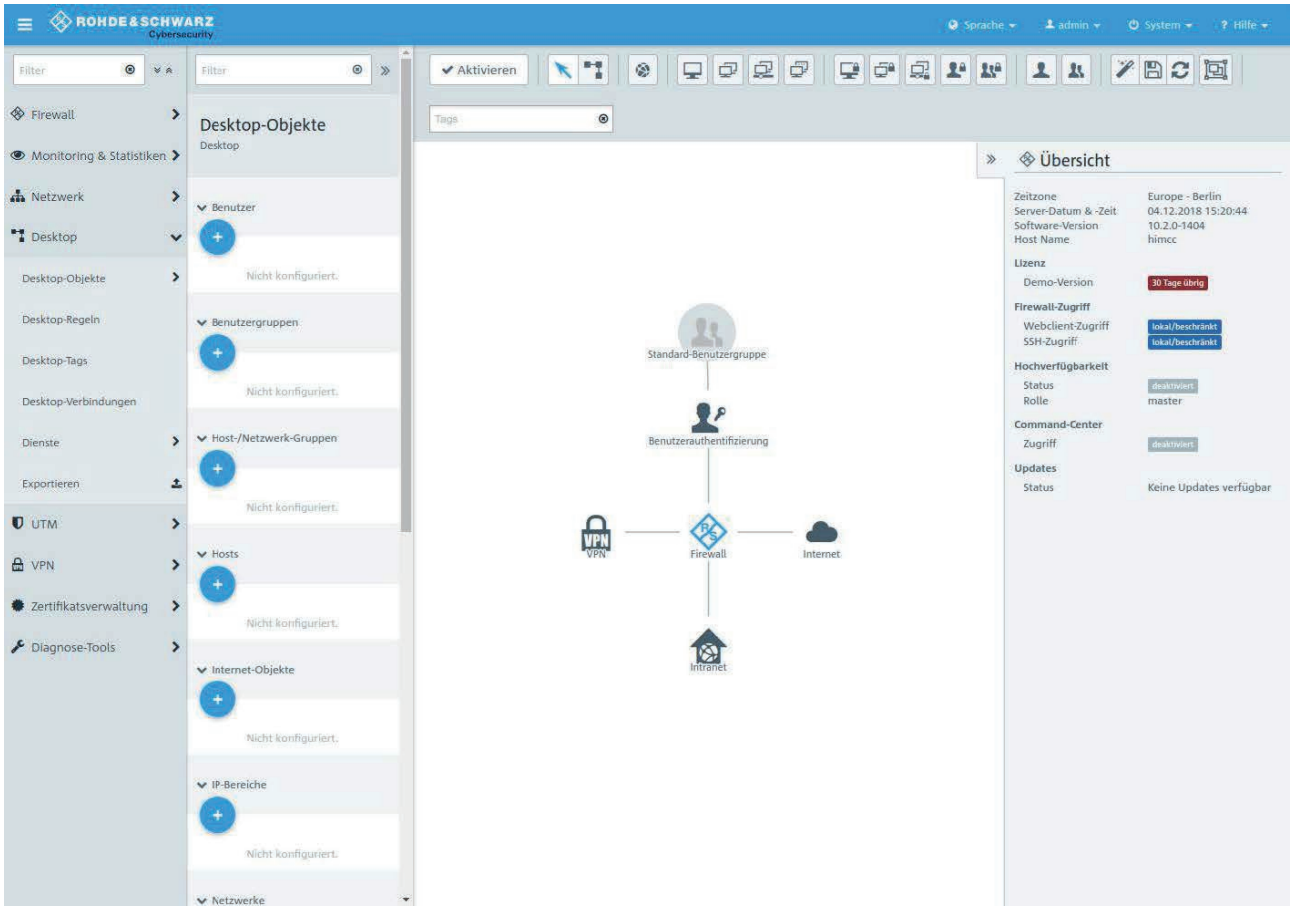
Das System wird neugestartet.



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 9.4 bis 9.8, 10.0, 10.1 und 10.2 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.