LANCOM Release Notes

LCOS FX

10.4 RU1

LANCOM Systems GmbH
Adenauerstrasse 20 / B2
52146 Würselen
Germany

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

25.11.2019, 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 10.4 RU1 sowie die Änderungen und Verbesserungen zur Vorversion.

2. Unterstützte Hardware

Version 10.4 RU1 unterstützt die folgenden Hardware Appliances:

- LANCOM R&S®Unified Firewalls UF-50/100/200/300/500/900
- R&S®UF-50/100/200/300/500/800/900/1000/1200/2000
- R&S®UF-T10
- R&S®GPO150
- R&S®GPA300/500
- R&S®GPX850
- R&S®GPZ1000/2500/5000
- 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 10.4 RU1 unterstützt die folgenden virtuellen Appliances:

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

Version 10.4 RU1 unterstützt die folgenden Hypervisor:

- Vmware ESX
- Microsoft HyperV
- Oracle Virtualbox

3. Historie LCOS FX

LCOS FX-Änderungen 10.4 > 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.
- IPv6 wurde deaktiviert.
- Die Anzahl der Log-Nachrichten aus der Anti-Malware Engine wurde verringert.

LCOS FX-Änderungen 10.3.3 > 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 10.3.2 > 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 10.3.1 > 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 10.3.0 > 10.3.1

Verbesserungen

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

LCOS FX-Änderungen 10.2.3 > 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 10.2.2 > 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 10.2.1 > 10.2.2

Verbesserungen

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

LCOS FX-Änderungen 10.2.0 > 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 10.4 RU1

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.

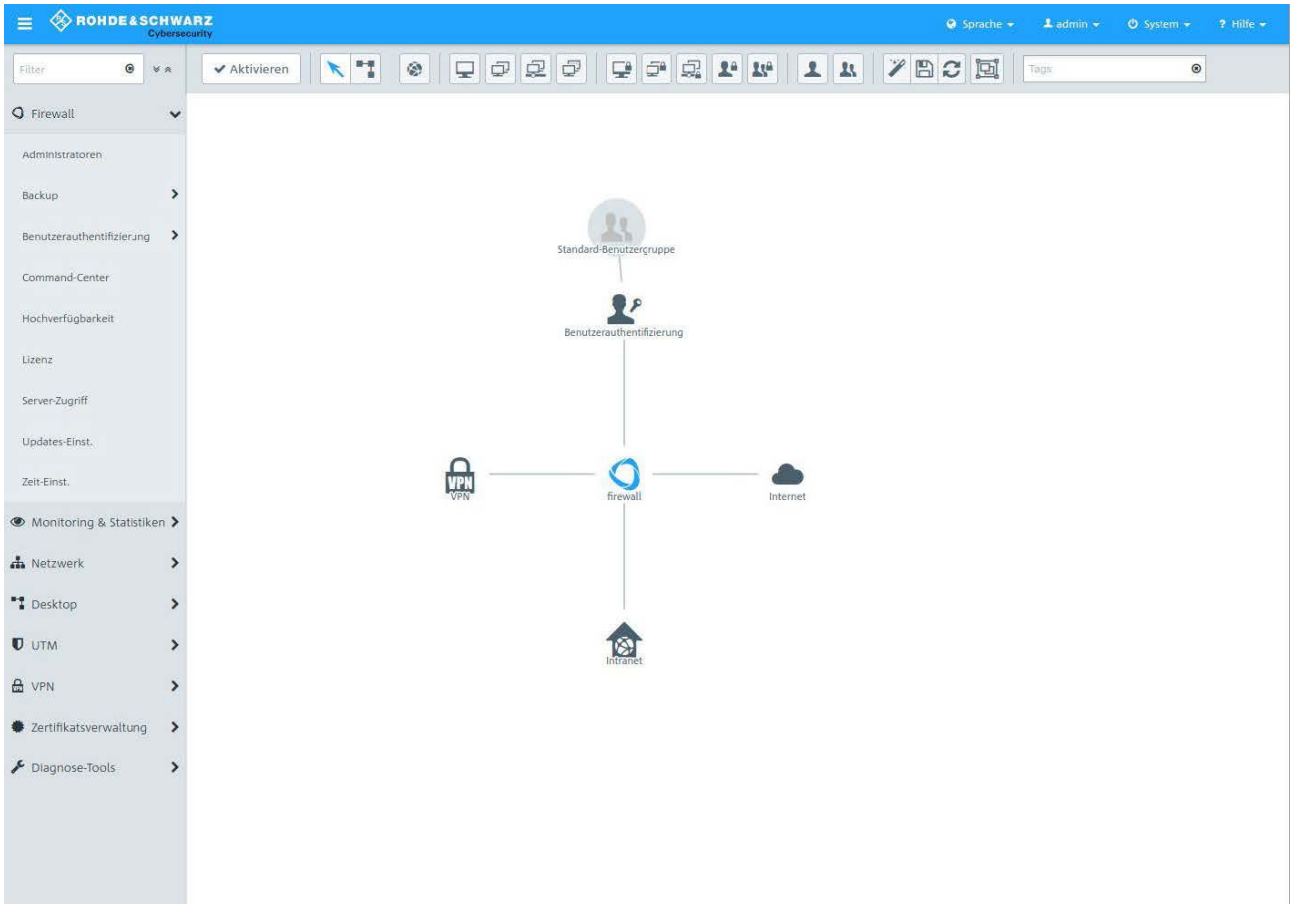
Über den Auto-Updater in der Weboberfläche Ihrer LANCOM R&S®Unified Firewall ist jeweils die nächsthöhere Minor Update-Version zur schrittweisen Aktualisierung verfügbar.

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

Hinweis 2:

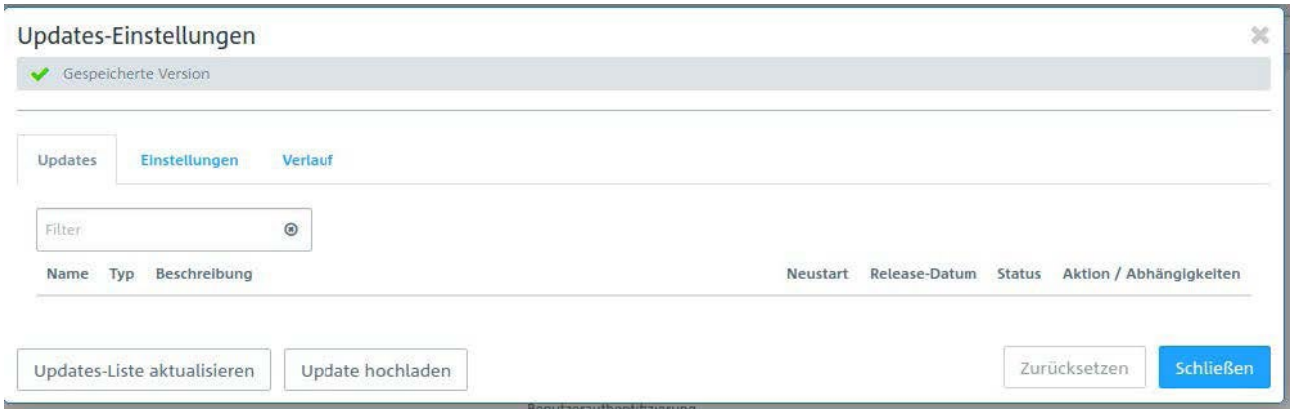
Um Arbeitsabläufe nicht zu behindern, führen Sie das Update zunächst in einer Testumgebung aus und nicht in einem realen Setting.

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



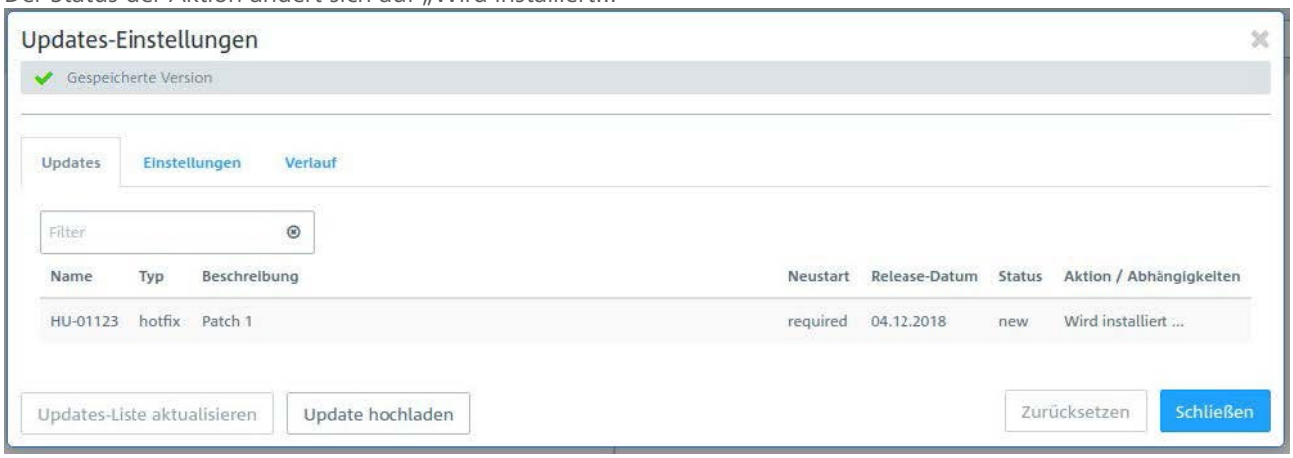
Im sich öffnenden Fenster „Updates-Einstellungen“ klicken Sie im Reiter „Updates“ auf die Schaltfläche „Updates-

Liste aktualisieren“.

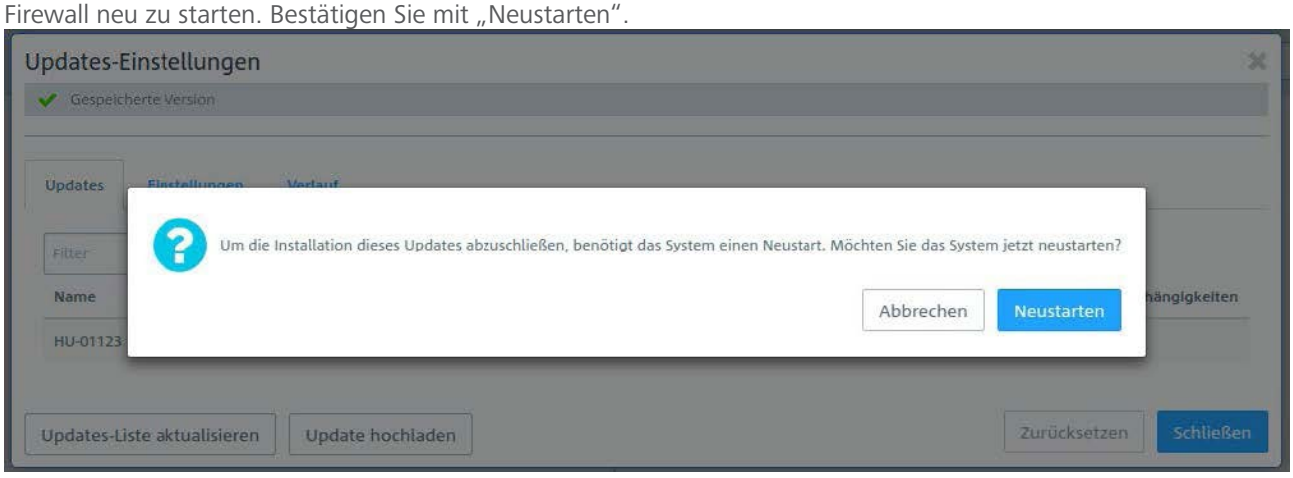


Wählen Sie die zu installierende Firmware-Datei aus der Liste und klicken Sie auf “Installieren”.

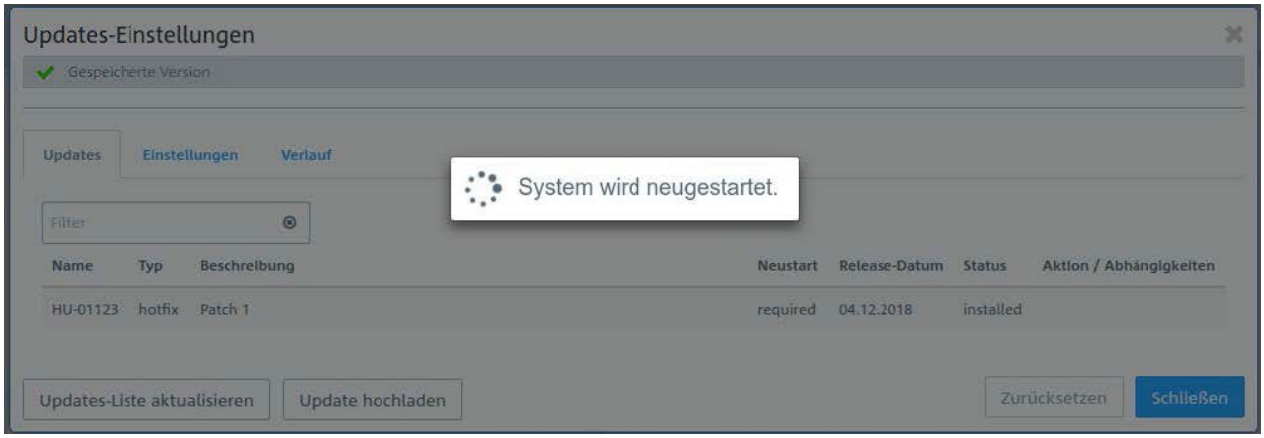
Der Status der Aktion ändert sich auf „Wird installiert...“



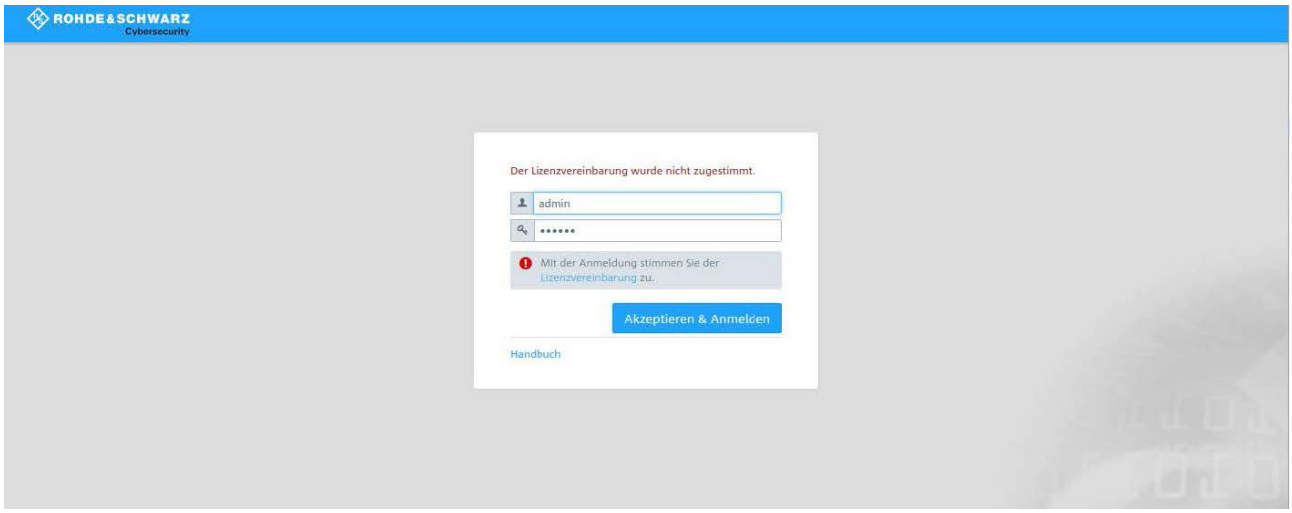
Nach Abschluss der Installation erscheint ein Popup-Dialogfenster, in welchem Sie aufgefordert werden, die Firewall neu zu starten. Bestätigen Sie mit „Neustarten“.



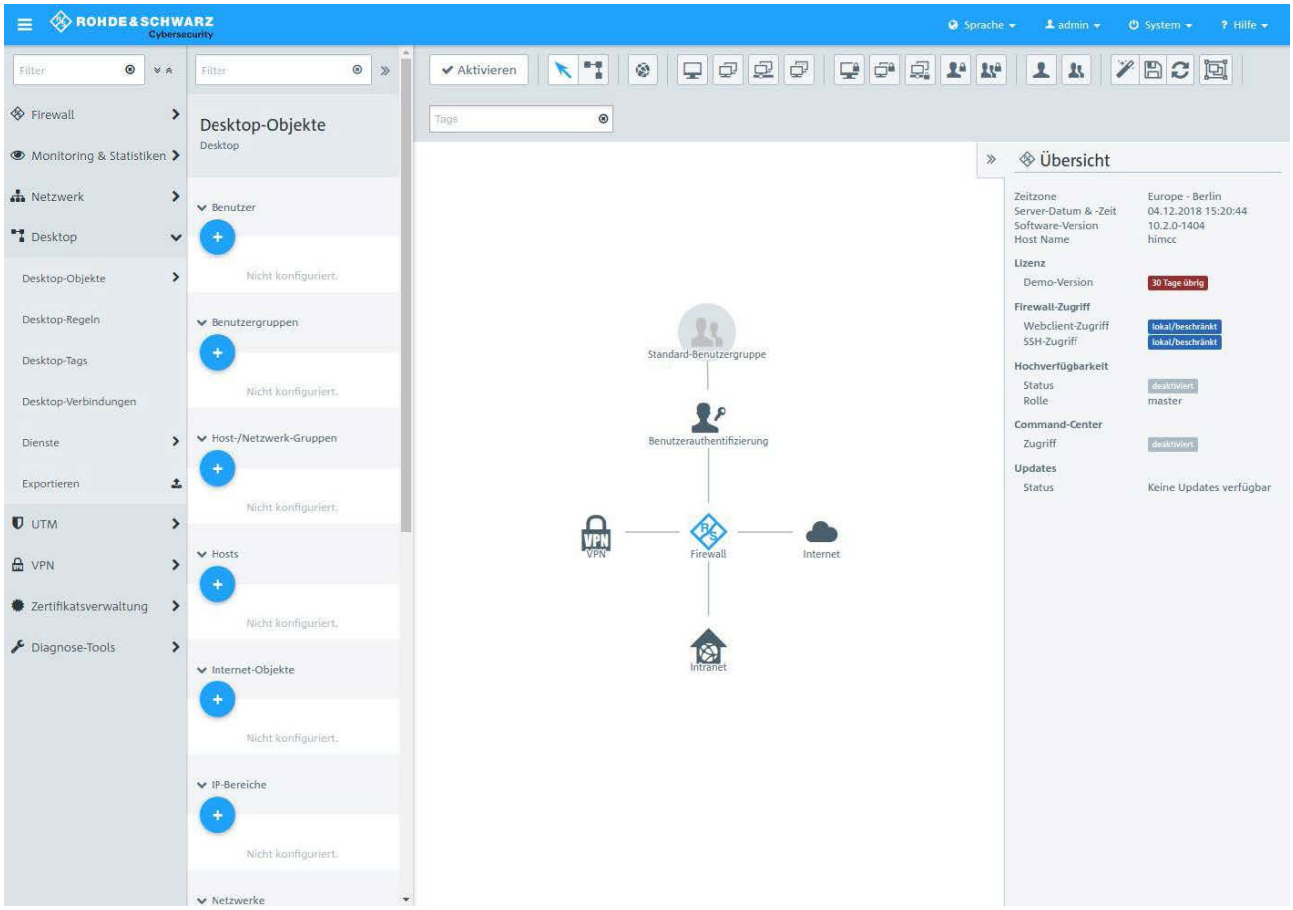
Das System wird neugestartet.



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.



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.

www.lancom-systems.de

LANCOM Systems GmbH I Adenauerstr. 20/B2 I 52146 Würselen I Deutschland I E-Mail info@lancom.de

LANCOM Systems