Release Notes

LCOS FX

11.1 Rel

Inhaltsübersicht

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 Software Release LCOS FX 11.1 Rel.

2. Das Release-Tag in der Software-Bezeichnung

Release Candidate (RC)
Ein Release Candidate ist umfangreich von LANCOM getestet und enthält neue Betriebssystem-Features. Er dient als Praxistest und wird deshalb für den Einsatz in Produktivumgebungen nicht empfohlen.

Release-Version (Rel)
Das Release ist umfangreich geprüft und in der Praxis erfolgreich getestet. Es enthält neue Features und Verbesserungen bisheriger LANCOM Betriebssystem-Versionen und wird daher für den Einsatz in Produktivumgebungen empfohlen.

Release Update (RU)
Ein Release Update dient zur nachträglichen Weiterentwicklung einer initialen Release-Version in Produktivumgebungen und enthält Detailverbesserungen, Security Fixes, Bug Fixes und kleinere Features.

Security Update (SU)
Enthält wichtige Security Fixes des jeweiligen LANCOM Betriebssystem-Versionstandes und sichert Ihnen fortlaufend einen sehr hohen Sicherheitsstandard in Ihrer Produktivumgebung.

3. Unterstützte Hardware

Version 11.1 Rel unterstützt die folgenden Hardware Appliances:

- → LANCOM R&S®Unified Firewalls
  UF-50/60/60 LTE/T-60/100/160/200/260/300/360/500/760/900/910/1060
- → 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 11.1 Rel unterstützt die folgenden virtuellen Appliances:

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

Version 11.1 Rel unterstützt die folgenden Hypervisor:

- → VMware ESXi
- → Microsoft Hyper-V
- → Oracle VirtualBox
- → KVM

4. Historie LCOS FX

LCOS FX Änderungen 11.1 Rel

Verbesserungen

→ Traffic Shaping kann außer für Traffic-Gruppen auch direkt für Quell-Interfaces eingestellt werden.

→ Performance-Optimierung des Reverse Proxy

→ Die Engine für Application Filter und Application-based Routing erkennt ‚doctolib'.

Korrekturen

→ Im Alarm- und System-Log der Firmware-Version LCOS FX 11.1 RC1 war bei einem Antivirus-Vorfall nicht der Name des erkannten Virus zu sehen.

→ Wenn in der Firmware-Version LCOS FX 11.1 RC1 die Antivirus-Option ‚Dateien blockieren, wenn Scan fehlschlägt' deaktiviert war, wurden passwortgeschützte Dateien trotzdem von der Unified Firewall blockiert.

→ Auf der Meldungs-Seite zu einem gefundenen Virus war bei der Firmware-Version LCOS FX 11.1 RC1 der Name des erkannten Virus nicht enthalten.

→ Nachdem eine VPN-SSL-Verbindung umbenannt wurde, war die ‚Aktivieren'-Schaltfläche in der Menüleiste der Unified Firewall nicht blau eingefärbt.

→ In den Host- / Netzwerkgruppen wurde in der Firmware-Version LCOS FX 11.1 RC1 kein Beschreibungstext angezeigt, wenn Objekte hinzugefügt wurden, die nicht in der Liste vorhanden waren.

→ Nachdem eine Unified Firewall über den Webclient in die Werkseinstellungen zurück versetzt wurde, konnten im LetsEncrypt-Konfigurationsdialog keine Einstellungen mehr vorgenommen werden.

→ In LCOS FX 11.1 RC1 wurden für die IDS / IPS nicht alle Pufferinhalte berücksichtigt. Dies führte dazu, dass Datenverkehr teilweise nicht durch die IDS / IPS geprüft wurde.

→ Den IP-Protokollen 61, 63, 68, 99, 114 und 253 wurde in den benutzerdefinierten Diensten kein Name zugeordnet. Weiterhin wurde ein manuell hinterlegter Dienstname nicht in die Menüleiste übernommen.

→ Eine in LCOS FX 11.1 RC1 konfigurierte Proxy-Ausnahme für eine bestimmte Webseite in einem Routing-Profil für das Application-Management fand keine Anwendung. Dies führte dazu, dass die Webseite durch den Content Filter blockiert wurde.

→ Es war nicht möglich, über ein LMC Add-In einen weiteren Administrator in der Unified Firewall anzulegen. Der Rollout wurde mit der Fehlermeldung „None Type has no attribute username" quittiert.

→ Wurde der Dienst ‚suricata' (zuständig für die IDS / IPS) unvermittelt beendet, konnten lokale Dienste wie z.B. DNS von extern angesprochen und verwendet werden.

→ Eine in LCOS FX 11.1 RC1 hinterlegte IPv6-Adresse für das Default Gateway wurde nicht in den Statusinformationen des Internet-Objekts angezeigt.

→ Es konnte bei Verwendung des HTTP(S)-Proxy mit aktivem Antivirus sporadisch vorkommen, dass Webseiten blockiert wurden.
Es gibt jetzt die Möglichkeit, einen automatisierten Neustart des HTTP(S)-Proxy um Mitternacht über ein Skript zu aktivieren. Wenden Sie sich zwecks Bereitstellung der Skript-Datei bitte an den LANCOM Support.

→ Beim Erstellen eines Management-Berichts mit der Unified Firewall wurde die Anzahl der durch IDS / IPS blockierten Pakete grafisch nicht im Diagramm dargestellt.

→ Wenn auf einer Unified Firewall ein DHCP Relay-Server für ein Interface hinterlegt war und im Anschluss noch ein weiterer Eintrag für ein anderes Interface mit einem anderen DHCP Server hinterlegt wurde, funktionierte nur noch der neue Eintrag.

→ Wenn in der Firmware-Version LCOS FX 11.1 RC1 ein benutzerdefinierter Dienst erstellt wurde und nur ein Quellport angegeben werden sollte, funktionierte dies nicht, wenn lediglich eine Port-Nummer in das Feld ‚Quell-Port von' eingetragen wurde und das ‚Bis'-Feld leer blieb.

→ In den DNS-Server-Einstellungen konnten keine Hostnamen hinterlegt werden. Dadurch war es z.B. nicht möglich, den Hostnamen ‚wlc-address' zu hinterlegen.

→ Wurde der Reverse-Proxy sehr stark ausgelastet, konnte es vorkommen, dass der Reverse-Proxy nach einiger Zeit keine Pakete mehr weiterleitete.

→ Der SSO-Client (Single Sign On) konnte sich mit LCOS FX 11.1 RC1 nicht mehr mit der Unified Firewall verbinden, da der Port 6789 durch den Paketfilter blockiert wurde. Dadurch funktionierte Single Sign On nicht mehr.

→ In der Firmware LCOS FX 11.1 RC1 funktionierte der Mail-Proxy nicht mit der Standard-Certification Authority.

→ Mit LCOS FX 11.1 RC1 konnte es in einem HA-Cluster vorkommen, dass die PostgreSQL-Datenbank auf der Backup-Firewall nicht mehr funktionsfähig war. Dadurch brach die Synchronisation der Log-Datenbank zwischen Master- und Backup-Firewall ab. Weiterhin wurde die Festplatte der Backup-Firewall vollgeschrieben.

LCOS FX Änderungen 11.1 RC1

Neue Features

→ **IPv6 WAN**
Die Firewall kann damit an reinen IPv6-Anschlüssen oder gemischten IPv4/IPv6-Anschlüssen betrieben werden. Es können IPSec-VPN-Tunnel und Wireguard-VPN-Tunnel über IPv6 aufgebaut werden. Außerdem können Reverse Proxy Frontends über IPv6 angeboten werden und es kann über IPv6 auf den Webclient und SSH der Firewall zugegriffen werden.

→ **SAML-Authentifizierung**
Zusätzlich zu lokalen Benutzern und der LDAP-Anbindung kann die Firewall SAML-Authentifizierung nutzen, um Benutzer für benutzer- oder gruppenspezifische Regeln zu authentifizieren. Als IDP werden Keycloak und Microsoft Entra ID unterstützt.

→ **Reverse Proxy-Authentifizierung**
Dienste, die von der Firewall über den Reverse Proxy angeboten werden, können auf bestimmte Benutzer oder Gruppen beschränkt werden. Dabei werden sowohl lokale, als auch LDAP- und SAML-Benutzer und -Gruppen unterstützt

→ **HA Cluster-Übergabe bei Ausfall einer Netzwerk-Schnittstelle**
Bei Ausfall einer Netzwerkschnittstelle auf dem aktiven Cluster-Knoten übernimmt die andere Firewall, sofern die Schnittstelle auf der zweiten Maschine funktioniert.

→ **Neue Anti-Virus-Engine**
Für die Anti-Virus-Funktionalität wird Bitdefender genutzt, so wie bisher bereits für Anti-Spam und Content Filter.

→ **REST API-Dokumentation via OpenAPI**
Die REST API der Konfigurationsschnittstelle ist mithilfe von OpenAPI dokumentiert. Die Dokumentation kann live über den Browser eingesehen werden.

→ **Unterstützung allgemeiner IP-Protokolle**
Bei benutzerdefinierten Diensten ist es möglich Dienste für beliebige IP-Protokolle zu erstellen.

→ **Benutzerdefinierte Dienste mit Einschränkung des Quell-Ports**
Bei benutzerdefinierten Diensten ist es möglich bei TCP- oder UDP-basierten Diensten auch die erlaubten Quell Ports einzuschränken.

Verbesserungen

→ Die UF-260 unterstützt das LANCOM SFP-GPON-1 Modul.

→ Auf dem Regel-Desktop können Gruppen direkt auf Netzwerk- und Host-Objekte verweisen, um die doppelte Konfiguration der IP-Adressen zu vermeiden.

→ Der Reverse Proxy unterstützt jetzt Websockets.

→ Beim Reverse Proxy kann ein Timeout Richtung Backend-Server konfiguriert werden.

→ Beim Reverse Proxy kann HostHeader Preservation konfiguriert werden.

→ Es werden beliebige ACME-Server unterstützt.

→ Es ist möglich, Reverse Proxy Frontends an Wireguard-Verbindungen zu binden.

→ Es ist möglich, das externe Portal an Wireguard-Verbindungen zu binden.

Weitere Hinweise

→ Der VoIP Proxy wurde entfernt.

→ Der Import von Konfigurations-Backups wird nur noch ab Version 9.8 unterstützt.

→ Bitte beachten Sie, dass der Reverse Proxy in einer Basic-Lizenz nicht enthalten ist. Eine Nutzung des Reverse Proxy innerhalb der Basic-Lizenzierung ist daher außerhalb des vertraglichen Lizenzumfangs. Ab der Version 11.1 wird eine Nutzung des Reverse Proxys mit der Basic-Lizenz nicht mehr möglich sein. Bitte führen Sie rechtzeitig ein Upgrade auf die Full-Lizenz durch, damit Sie den Reverse Proxy weiterhin verwenden können.

→ Die Outlook Anywhere Option des Reverse Proxys wurde entfernt, da sie für aktuelle Microsoft Outlook / Exchange Versionen nicht mehr benötigt wird.

Korrekturen

→ Ein Benutzer mit „Read-Only“-Berechtigung konnte keinen Export des Backups sowie keinen Export einer VPN-SSL-Verbindung durchführen.
Der Export des Backups sowie der Export einer VPN-SSL-Verbindung ist jetzt auch mit „Read-Only“ Berechtigung möglich.

→ Wurde eine Unified Firewall mit aktivem IDS/IPS unerwartet heruntergefahren (etwa durch einen Stromausfall), konnte der Dienst für das Connection-Tracking (conntrackd) nicht mehr starten. Dies führte dazu, dass IDS/IPS nicht mehr funktionierte. Weiterhin konnte es zu einem unvermittelten Neustart kommen, wenn die IDS/IPS versuchte, auf den Dienst für das Connection-Tracking zuzugreifen.

→ Der Netfilter-Dienst (nftd) versuchte die Firewall-Regeln immer wieder zu schreiben, was in einer erhöhten RAM-Auslastung resultierte. Dies konnte auch dazu führen, dass Firewall-Regeln nicht geschrieben werden konnten.

→ Bei Verwendung der Multi-WAN-Gewichtung mit mehreren Internet-Verbindungen wurden die Internet-Verbindungen nicht korrekt priorisiert und der Großteil des Datenverkehrs über die Verbindung mit der niedrigeren Gewichtung versendet.

→ In einem HA-Cluster konnte es zu sporadischen Paket-Verlusten bei der Kommunikation über die Firewall kommen.

5. Weitere Informationen

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

6. 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.

LANCOM Systems GmbH
A Rohde & Schwarz Company
Adenauerstr. 20/B2
52146 Würselen | Deutschland
info@lancom.de | lancom-systems.de

LANCOM, LANCOM Systems, LCOS, LANcommunity und Hyper Integration sind eingetragene Marken. Alle anderen verwendeten Namen und Bezeichnungen können Marken oder eingetragene Marken ihrer jeweiligen Eigentümer sein. Dieses Dokument enthält zukunftsbezogene Aussagen zu Produkten und Produkteigenschaften. LANCOM Systems behält sich vor, diese jederzeit ohne Angaben von Gründen zu ändern. Keine Gewähr für technische Ungenauigkeiten und / oder Auslassungen. 11/2024