Release Notes

LCOS FX
11.1 RU7

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 RU7.

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 RU7 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 RU7 unterstützt die folgenden virtuellen Appliances:

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

Version 11.1 RU7 unterstützt die folgenden Hypervisor:

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

4. Historie LCOS FX

LCOS FX Änderungen 11.1 RU7

Korrekturen & Anpassungen

→ Bei Chromium-basierten Browsern (z.B. Google Chrome oder Microsoft Edge) konnte es vorkommen, dass Desktop-Interaktionen im Webclient verzögert ausgeführt wurden.

→ Nach einem Konfigurations-Rollout über die LMC wurde die Liste der konfigurierten Syslog-Server gelöscht. Dadurch wurden System-Ereignisse nicht mehr an die Syslog-Server versendet.

→ Bei Verwendung von Host-/Netzwerk-Gruppen mit unterschiedlichen Interfaces sowie VPN-Gruppen mit unterschiedlichen Verbindungstypen (route-based IPsec und policy-based IPsec) wurde in den Paketfilter-Regeln jede Kombination aus IP-Adressen und Interfaces gebildet. Dies führte dazu, dass die Kommunikation in Netzwerke möglich war, obwohl dies in der Regel nicht erlaubt wurde (CVE-2025-67832).
Nach einem Update auf LCOS FX 11.1 RU7 wird nun bei betroffenen Konfigurationen eine Meldung ausgegeben, dass die Paketfilter-Regeln jetzt strikter gehandhabt werden und die Kommunikation daher gegebenenfalls nicht mehr funktioniert.

→ Wenn ein Regelsatz mehreren IPsec-Verbindungen zugewiesen wurde, von denen mindestens eine Verbindung nicht aufgebaut war, konnte der Dienst für die Regelerzeugung (x-rulesd) das Interface-Objekt für die VPN-Verbindungen nicht erstellen. Dies führte dazu, dass der Regelsatz für die VPN-Verbindungen nicht angewandt wurde und die Kommunikation nicht möglich oder stark eingeschränkt war.

→ Der Dienst für IDS / IDPS (ixsd) erstellt bei Signatur-Updates immer einen eigenen Sub-Prozess. Nach erfolgtem Update wurden die Sub-Prozesse nicht beendet und der Speicher nicht freigegeben. Dadurch konnte es zu einer erhöhten RAM-Auslastung kommen.

LCOS FX Änderungen 11.1 RU6

Korrekturen

→ Wenn die Länge einer durch den URL-/Content-Filter blockierten URL die maximal unterstützte Länge überstieg (z.B. durch Verwendung von SafeSearch und Enkodierung von blockierten URLs), führte dies zu einem Absturz des Dienstes „squid“. Bis zu einem Neustart von „squid“ war dann über den HTTPS-Proxy keine Kommunikation möglich.

→ In seltenen Fällen konnte es vorkommen, dass der Strongswan-Dienst „charon-systemd“ die CPU sehr stark auslastete. Dies konnte u.A. dazu führen, dass Verbindungen abbrachen und die Unified Firewall nicht mehr oder nur sehr langsam auf Anfragen reagierte.

→ Es konnte vorkommen, dass der Datenbankdienst „redis“ den RAM sowie die Festplatte sehr stark auslastete. Dies konnte u.A zu Verbindungs-Abbrüchen und unvermittelten Neustarts der Unified Firewall führen.

→ In einem Szenario mit einer statisch konfigurierten Internet-Verbindung und einer Backup-Verbindung mit DHCP wurde im Backup-Fall fälschlicherweise der DNS-Server der ersten Verbindung verwendet. Wenn dieser DNS-Server über die Backup-Verbindung nicht erreichbar war, führte dies dazu, dass die DNS-Auflösung nicht funktionierte.

→ Wenn eine Internet-Verbindung mit konfigurierter Zeitbeschränkung ausfiel (etwa durch eine Störung), wurde diese Verbindung nach dem Ausfall nicht wieder aufgebaut, obwohl die Zeitbeschränkung noch nicht galt.

→ Die Datenbank „Redis“ wurde aktualisiert, wodurch die im CVE-2025-49844 beschriebene Sicherheitslücke behoben wurde.

LCOS FX Änderungen 11.1 SU5

Korrekturen

→ Die Sicherheitslücke ‚Heap Buffer Overflow in Squid' (CVE-2025-54574) wurde behoben.

LCOS FX Änderungen 11.1 RU4

Korrekturen

→ Bei jedem Erneuern von Let‘s Encrypt-Zertifikaten wurde eine neue Log-Datei erstellt, statt die bestehende zu überschreiben.
Es wird jetzt nur noch eine Log-Datei erstellt und diese bei Bedarf überschrieben.

→ Bei LTA-Benutzern, denen genau 128 Berechtigungs-Profile zugewiesen werden sollten, schlug die Zuweisung der Berechtigungs-Profile fehl. Dies führte dazu, dass der Zugriff auf die zugewiesenen Ressourcen nicht möglich war.

→ Beim Ausrollen von Netzwerken und IPsec-Verbindungen über die LMC wurde für jede Kombination aus Quell-Objekt, Ziel-Objekt und Protokoll eine Regel in der nftables chain ‚forward.prefilter.ipsec‘ angelegt. Wurden sehr viele Netzwerke ausgerollt, führte dies bei Datenübertragung über die Internet-Verbindung zu einer stark erhöhten CPU-Auslastung, was in einer stark reduzierten Übertragungsgeschwindigkeit resultierte.

→ Der Dienst ‚gpNetworkd‘ erstellte bei jedem Verbindungs-Aufbau eine neue iptables-Regel, auch wenn diese bereits vorhanden war. Wenn die Internet-Verbindung immer wieder auf- und abgebaut wurde (etwa bei einem Flapping), konnte dies zu einer stark erhöhten CPU-Last durch den Dienst ‚ksoftirqd‘ führen.

→ Nach einem Update auf LCOS FX 11.1 Rel konnte es bei aktivem URL-Sanitize oder Safesearch zu Abstürzen des Dienstes für den HTTPS-Proxy kommen (Squid). Dies führte bis zu einem Neustart des HTTPS-Proxy dazu, dass Webseiten nicht mehr aufgerufen werden konnten.

LCOS FX Änderungen 11.1 RU3

Neue Features

→ Der Voice-over-IP-Helper ist jetzt konfigurierbar.

Korrekturen

→ Nach einem Update auf LCOS FX 11.1 RU1 wurden bei jedem Auf- und Abbau einer IPsec-Verbindung (betrifft auch das Rekeying) alle Regeln für den eingehenden Datenverkehr (nftables input rules) neugeladen. Durch diesen Vorgang kam es zu Paket-Verlusten und die CPU wurde stark ausgelastet. Dies führte zu Performance-Verlusten.

→ War die Antivirus-Funktion der Firewall aktiv, die Antispam-Funktion aber deaktiviert, wurde das Update der Antivirus-Definitionen zwar erfolgreich durchgeführt. Im Webinterface wurde in diesem Fall bei „Updates“ dauerhaft die Meldung „Läuft gerade“ angezeigt.

→ Es konnte vorkommen, dass nicht alle Warnmeldungen aus dem Alarm-Protokoll in der LMC-API und im SIEM-Dienst (Security Information and Event Management) auftauchten. Dies führte dazu, dass die Meldungen nicht an das SIEM-System weitergeleitet wurden.

→ Bei Verwendung von PPPoE- oder WWAN-Verbindungen konnte es vorkommen, dass DHCP-Leases nicht an die LMC übermittelt und somit dort nicht angezeigt wurden.

→ In LCOS FX 11.1 RU2 wurde der VoIP-Helper eingeführt, welcher dauerhaft aktiv war. In Szenarien, bei denen die SIP-Geräte (z.B. eine TK-Anlage oder ein SBC) selbst einen NAT-Helper verwendeten, konnte es dadurch zu Problemen mit der SIP-Signalisierung oder auch bei der Sprachübertragung kommen. Der VoIP-Helper ist jetzt in der Standard-Einstellung deaktiviert und kann in dem Menü „Erweiterte Einstellungen“ bei Bedarf aktiviert werden.

→ Nach einem Update auf LCOS FX 11.1 RU2 wurde die IPv4-Adresse entweder gar nicht oder nur stark verzögert an den DynDNS-Dienst der LMC weitergeleitet. Dadurch war auch der Zugriff über den DynDNS-Namen (z.B. eine eingehende VPN-Verbindung) entweder gar nicht oder erst zeitverzögert möglich.

LCOS FX Änderungen 11.1 RU2

Neue Features

→ Unterstützung für LANCOM R&S®Unified Firewall UF-560

→ Die Firewall sendet den Grund für den letzten Neustart an die LMC, damit dieser in den Geräte-Logs der LMC erscheint.

Korrekturen

→ Nach einem Update auf LCOS FX 11.1 RU1 konnte mit einer LANCOM R&S®Unified Firewall UF-50 keine Verbindung zur LMC hergestellt werden.

→ Mit aktivem Application Filter und dafür aktiven Logs in der LANCOM R&S®Unified Firewall wurden keine Statistiken geführt oder Log-Einträge erstellt.

→ Wenn auf einer LANCOM R&S®Unified Firewall ein DHCP Relay gelöscht wurde, wurde dies im Webinterface korrekt angezeigt; im Backend war der Eintrag aber weiterhin vorhanden.

→ Nach einem Update auf LCOS FX 11.1 Rel konnte die ‚Wake on LAN'-Funktion, welche über die Unified Firewall für bestimmte Benutzer bereitgestellt wird, nicht mehr verwendet werden. Ebenso konnten sich Benutzer dann nicht mehr korrekt am internen Portal anmelden und es wurde ein Verbindungsfehler angezeigt.

→ Wurde in LCOS FX 11.1 Rel oder LCOS FX 11.1 RU1 der Mail-Proxy verwendet, war in den Mailfilter-Einstellungen der Adressenfilter ‚Whitelist' ohne Funktion.

→ Bei Verwendung der Whitelist für den Mail-Proxy wurden auch E-Mails versendet, welche nicht in der Whitelist enthalten waren.

→ Der Antivirus-Dienst (bdamserver) speicherte Informationen in einer einzelnen Log-Datei, statt diese nach Erreichen einer bestimmten Datei-Größe in ein weiteres Log zu speichern und das alte Log zu komprimieren (logrotate). Dies führte nach einiger Laufzeit dazu, dass die Log-Datei sehr groß wurde.

→ Mitglieder einer Host-Gruppe auf dem Desktop wurden unter ‚Zusätzliche Objekte' doppelt angezeit, wobei für die doppelten Einträge die UUID als Name angezeigt wurde.

→ Benutzerdefinierte Dienste wurden in der Desktop-Konfiguration des Executive Reports nicht angezeigt. Dies galt auch für benutzerdefinierte Objekte, die in der LMC erstellt wurden.

→ Wenn die API-Dokumentation der Unified Firewall über einen LMC-Webtunnel aufgerufen werden sollte, kam es zu einer Fehlermeldung und die API-Dokumentation wurde nicht angezeigt.

→ Die Überprüfung einer IPv6-Internetverbindung mit der Anwendung ‚curl' war funktionslos.

→ Die Lizenzierung einer vFirewall, welche auf einer Kernel-basierten Virtual Machine (KVM) des Herstellers Hetzner installiert war, konnte nicht durchgeführt werden, da das System keine Seriennummer für die Firewall generierte.

→ Ein WAN-Verbindungstest mit Type ‚tcp_probe' bzw. ‚tcp_probev6' und den voreingestellten Standard-Argumenten (53 8.8.8.8 bzw. 2001:4860:4860::8888) funkionierte nicht.

→ In einem Szenario mit Traffic-Shaping, in welchem Limits für die WAN-Schnittstelle angegeben waren, konnte es vorkommen, dass ein konfiguriertes Outbound-Download-Limit für einen Client nicht beachtet und infolgedessen ein unlimitierter Download verwendet wurde.

→ In einem Szenario mit Traffic-Shaping, zwei WAN-Verbindungen und regelbasiertem Routing für HTTP- und HTTPS-Traffic konnte es vorkommen, dass für den HTTP-Traffic eines Clients über die zweite WAN-Verbindung ein falscher Limit-Wert verwendet wurde.

→ Beim Erstellen einer IPv6-Verbindung zu einem VLAN-Interface erschien bei der Interface-Auswahl die Fehlermeldung, dass der gewählte Verbindungstyp ungültig sei.

→ In der Datei ‚openapi.json' waren Duplikate von einigen Parametern vorhanden, was bei der Verwendung der OpenAPI-Kommandozeile oder von OpenAPI-Diff-Tools zu Problemen führen konnte.

→ Wenn der ‚HAProxy'-Dienst nicht konfiguriert war, konnte es vorkommen, dass dieser regelmäßig neu startete.

LCOS FX Änderungen 11.1 RU1

Neue Features

→ **TCP Load Balancer**
Mittels TCP Load Balancer können beliebige TCP-Verbindungen auf mehrere Backend-Server hinter der Firewall verteilt werden. Dank einer aktiven Überwachung der Server werden Verbindungen immer nur auf funktionsfähige Server weitergeleitet.

Korrekturen

→ Nach einem Update auf LCOS FX 11.1 Rel verwendete die Unified Firewall für das automatische Backup per SCP den Port 0 statt des Standard-Ports 22. Dadurch funktionierte das automatische Backup nicht mehr.
→ Wenn ein Netzwerk erstellt wurde, welches ein GPON-Interface verwenden sollte, so erhielt man bei der Interface-Auswahl die Fehlermeldung, dass das gewählte Interface bereits in einer Bridge verwendet wurde. In der Folge konnte keine Verbindung konfiguriert werden.
→ Wenn auf einer Unified Firewall eine statische IPv6-WAN-Verbindung aktiv war, funktionierte bei DHCPv4-Verbindungen, die auf dem gleichen Interface konfiguriert waren, die DNS-Funktion nicht mehr.
→ In der Version LCOS FX 11.1 Rel konnte es vorkommen, dass es beim Erstellen eines Reverse Proxy-Eintrags mit LetsEncrypt zu einem Timeout beim Erstellen des LetEncrypt-Zertifikats kam. Ebenso konnte dies beim Erneuern eines Zertifikats über das Webinterface auftreten.
→ Wenn in der Liste der Reverse-Proxies sehr viele Einträge vorhanden waren und diese über das externe Web-Interface verfügbar gemacht wurden, konnten dort einige Einträge nicht angezeigt werden, weil kein Scrolling möglich war.
→ Das beim Backup einer per LMC verwalteten Unified Firewall mitgesicherte LMC-Gerätezertifikat wird beim Re-Import nur noch übernommen, wenn kein LMC-Gerätezertifikat in der Unified Firewall vorhanden ist.
→ Nach einer Aktualisierung auf LCOS FX 11.1 Rel wurden die Daten des aktualiserten Gerätes nicht mehr im Command Center angezeigt.
→ Bei einer konfigurierten DHCPv6-WAN-Verbindung wurde keine Default-Route angelegt. In der Folge war die Verbindung nicht funktionsfähig.
→ Nach der Einrichtung einer Internetverbindung mit IPv6 und Adressvergabe via DHCP war nach einem Neustart der Unified Firewall die Default-Route nicht mehr vorhanden. Dies führte dazu, dass per IPv6 keine Kommunikation mehr mit dem Internet möglich war.
→ Gruppen, welche weitere Gruppen mit Benutzern enthielten (Nested Groups) wurden nicht von der SAML-Implementierung unterstützt und konnten deshalb

Interface.“ ausgegeben. Dadurch konnte die Verbindung nicht gespeichert werden.

→ Versuchte ein Benutzer ohne Berechtigung für das Reverse-Proxy-Frontend auf die hinterlegte Webseite zuzugreifen, erfolgte ein Redirect auf die Login-Seite. Dabei wurde die Login-Seite immer wieder neu geladen.

→ Wurde nach der Konfiguration der SAML-Parameter die Schaltfläche ‚Jetzt synchronisieren‘ betätigt, ohne die Konfiguration vorher zu speichern, hatte dies keine Auswirkungen.
Bei einem Klick auf die Schaltfläche ‚Jetzt synchronisieren‘ wird die Konfiguration jetzt validiert und gespeichert und die Synchronisierung anschließend ausgeführt.

→ Auf einer LANCOM Unified Firewall UF-60 LTE konnte es vorkommen, dass Prozesse nicht korrekt beendet und der Speicher nicht freigegeben wurde. Dies führte zu einem unvermittelten Neustart der Unified Firewall.

→ Die im Sicherheits-Profil ‚LANCOM LCOS Default IKEv2‘ verwendeten Verschlüsselungs-Algorithmen stimmten nicht mit den im LCOS vorhandenen Standard-Einstellungen überein. Dadurch konnte es bei Verwendung dieses Profils vorkommen, dass VPN-Verbindungen mit LANCOM Routern mit LCOS sowie mit dem LANCOM Advanced VPN Client nicht funktionierten oder es zu Verbindungsabbrüchen kam.

→ Sendete ein DHCP-Relay Daten über eine VPN-Verbindung, deren Internet-Verbindung die IP-Parameter per PPP bezog, funktionierte nach einem Neustart der Unified Firewall das DHCP-Relay nicht mehr.

→ In einer Shaping-Konfiguration für das Traffic-Shaping wurden eingegebene Werte nach dem Speichern multipliziert mit 1000 angezeigt (z. B. 5 MBit eingegeben, 5.000 MBit angezeigt). Es handelte sich dabei lediglich um einen Anzeigefehler.

→ War die Option ‚Fehlerhaft gescannte Dateien blockieren‘ in den Antivirus-Einstellungen aktiv (Standard-Einstellung), konnte es sporadisch vorkommen, dass auch korrekt gescannte Webseiten ohne Malware durch die Antivirus-Engine blockiert wurden. Dabei wurde die Fehlermeldung „The request has been blocked. The requested URL could not be retrieved due to an anti virus engine failure.“ ausgegeben.

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