Release Notes

LCOS FX
10.13 RU8

Table of contents

1. Preface

The LANCOM family of operating systems—LCOS, LCOS SX, LCOS LX, and LCOS FX—forms the trusted basis for the entire LANCOM range of products. Within the scope of the hardware specified by the products, the latest firmware version is available for all LANCOM products and is offered by LANCOM Systems for download free of charge.

This document describes the innovations within software release LCOS FX 10.13 RU8.

2. The release tag in the software name

Release Candidate (RC)
A Release Candidate has been extensively tested by LANCOM and includes new LCOS featurses. It is suitable for testing and is not recommended for use in productive environments.

Release Version (REL)
The release version has been extensively and successfully tested in practice. It contains new features and improvements over previous LANCOM operating system versions and is therefore recommended for use in productive environments.

Release Update (RU)
A release update is a further development of an initial release version in productive environments and contains minor improvements, security fixes, bug fixes and smaller features.

Security Update (SU)
Contains important security fixes for the respective LANCOM operating system version and ensures that your security level remains very high on an ongoing basis in your productive environment.

3. Supported hardware

Version 10.13 RU8 supports the following 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 10.13 RU8 supports the following virtual appliances:

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

Version 10.13 RU8 supports the following hypervisors:

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

4. History LCOS FX

LCOS FX improvements 10.13 RU8

Note

Please note that the reverse proxy is not included in a Basic license. Use of the Reverse Proxy within the Basic license is therefore outside the contractual scope of the license. As of version 11.1, it will no longer be possible to use the Reverse Proxy with the Basic license. Please perform an upgrade to a Full license in time, so that the Reverse Proxy can still be used.

Bugfixes

- → After a role change of an HA cluster managed by the LMC, the slave firewall (temporary master firewall) incorrectly reported to the LMC with its own serial number instead of the serial number of the master firewall. As a result, the HA cluster could no longer communicate with the LMC and could therefore no longer be managed via the LMC.
- → After changing the DNS settings (e.g. adding a DNS server), it could happen after a restart of the Unified Firewall that the DNS service no longer worked and therefore no DNS resolution was possible via the Unified Firewall.
- → Due to excessive time spent checking for SPAM emails, it could happen that emails were received twice when using the mail proxy.
- → Unified Firewall models with 4GB memory (e.g. UF-60 & UF-160) could experience very high total memory usage due to high memory usage of the Suricata service. A newer Suricata version has improved this behavior.
- → After an update to LCOS FX 10.13 RU7, the Unified Firewall used port 0 instead of the standard port 22 for the automatic backup via SCP. As a result, the automatic backup no longer worked.
- → After restarting a Unified Firewall with an Internet connection via DHCP, it could happen that the DHCP service (dhcpd) was not active on the interface used. As a result, the interface could not obtain an IP address via DHCP and the Internet connection was not functional.

LCOS FX improvements 10.13 RU7

Bugfixes

→ As of LCOS FX 10.13 RU7, protocols in the Suricata service are inactive in order to reduce the memory consumption of the service.

→ If the activation of a configuration that was otherwise successfully rolled out from the LMC to the Unified Firewall failed, the configuration was not rolled back. Any inconsistencies that may arise from this could lead to errors in subsequent rollouts.

→ It could happen that a DHCP address and the route were not removed when a DHCP client received a new lease. This resulted in an IP address conflict, as both the old and the new lease were offered on the ETH port.
In addition, in scenarios in which the Unified Firewall was configured as a DHCP client, it could happen that the firewall did not receive an IP address via DHCP when the DHCP network address on the server was changed.
As a result, DNS problems could also occur when switching from one WAN connection to another WAN connection.

→ With very large desktop objects (e.g. host groups), the rule service (x-rulesd) crashed when applying the firewall rules. This could lead to problems with the configuration rollout from the LMC, among other things.

→ Even if application management or the HTTP proxy was or should have been deactivated, the Certification Authority (CA) for SSL inspection was validated. This meant that application management could not be deactivated if an expired certificate was used.

→ In IPsec with EAP-TLS authentication, the IPsec service could be terminated unexpectedly.

→ It could happen that VPN connections were abruptly disconnected by the Unified Firewall and then re-established due to a faulty self-check timer.

→ After installing a license file, a UF-1060 device was reported as a UF-960 device.

LCOS FX improvements 10.13 RU6

Bugfixes

→ Due to the bug fix introduced in LCOS FX 10.13 RU5 for the ‘Host Header Forgeries’ in connection with the transparent HTTP proxy, it could happen that no website could be accessed.

LCOS FX improvements 10.13 RU5

Improvements

→ **Support for the BGP ‘next-hop-self’ attribute**
The ‘next-hop-self’ attribute is usually used by eBGP routers. When a route is learned from eBGP, the eBGP router replaces the ‘next-hop’ attribute with its own direction before forwarding the route to its iBGP peers. This is necessary because iBGP routers are not able to reach routers that are not part of their own AS.

→ **Support for BFG IP prefix lists**
IP prefix lists provide a powerful mechanism for controlling both the input and output of routing information. For each peer, it is possible to define individually which routing information should be passed on to this peer and which routing information should be learned from a peer.

Note: Both settings can only be configured via the REST API or LMC add-ins.

Bugfixes

→ Although forwarded connections that were blocked by the Unified Firewall were included in the local statistics of the firewall, these messages were not forwarded to the log in the LANCOM Management Cloud (LMC).

→ The Squid proxy server has been updated with the latest security patches.

→ So-called ‘host header forgeries’ could occur with the Squid proxy server in transparent mode. These occurred more frequently with connections to cloud services and ensured that the services could not be reached if the transparent HTTPS proxy was activated.

→ In a scenario in which ‚Let‘s encrypt‘ certificates were used with a reverse proxy, the proxy was non-functional.

LCOS FX improvements 10.13 RU4

New features

→ Support for the Unified Firewall UF-1060
As a high-performance 2U appliance (100 Gbps firewall and 12 Gbps UTM throughput), the UF-1060 complements the portfolio of Unified Firewalls. Additionally, with its 8 expansion slots, it offers full port flexibility for a variety of customer requirements.

Bugfixes

→ Due to a misbehavior in the communication of the IPSec service, it could happen that the routes could not be applied with route-based IPSec, although the IPSec tunnel was established.

→ When rolling out several thousand block rules via the LMC, a rollout error could occur because writing the rules to the ‘iptables’ took too long.
A new feature has been implemented that allows block rules to be written to the ‘nftables’ using an add-in script, which is much faster. With UF-60 and UF-160, a maximum of 5,000 block rules can be imported in this way and from UF-260 a maximum of 10,000 block rules.

LCOS FX improvements 10.13 RU3

Note

The protocol for the LMC WEBconfig tunnel has been reimplemented. This leads to incompatibility with older versions of the LMC Devicetunnel (service-devicetunnel). Firewalls that are managed via the Public LMC can be updated directly.
For firewalls that are managed via private LMCs, it must be ensured that the version of the LMC is at least 1.00.163.0 (or service-devicetunnel version 16.2.4 or higher, accessible via 'System information / Service information / Show information') before firewalls are updated.

Bugfixes

- → A security vulnerability in the SSH protocol has been fixed ('Terrapin' security vulnerability/CVE-2023-48795).
- → If a group object was created for host groups in which there was a hostname entry that was part of a network that also belonged to the group, the object was created correctly in the frontend, but it had no function because it had no content in the backend of the Unified Firewall.
- → If an SNAT was stored for a host object or a host group in the direction of the WAN and was to be masked behind a WAN IP address that differed from the default WAN IP address, the SNAT did not take effect and it was still masked behind the default WAN IP address.
- → A superordinate process generated so many subordinate processes on a LANCOM R&S®Unified Firewall UF-60 LTE that no further processes could be started because the maximum had been reached. This led to an immediate shutdown or restart of the unified firewall.
- → After updating the Unified Firewall to LCOS FX 10.13 RU1 or higher, the VPN interfaces were no longer present in the associated routing entries for the IPSec connections rolled out by the LMC. This meant that no more data traffic could be transmitted via these VPN connections.
- → When using host and network groups, the entries for the app filter service (gpAppFilterd) were not always created in the iptables. As a result, data was not routed via the correct connection using application routing and applications were not blocked via the application filter.
- → If, in a scenario with a WAN backup, a connection was switched from the main to the backup connection, the Unified Firewall continued to attempt to establish an IPSec connection via the main WAN connection. As a result, the IPSec connection could not be established as long as the backup WAN connection was active.

LCOS FX improvements 10.13 RU2

Bugfixes

→ When using an IPSec connection and port forwarding at the same time, packets sent via the IPSec connection for the ports used in port forwarding were sent to the port forwarding destination instead of the actual destination. This led to restricted communication via the VPN connection.

→ If the mail proxy was activated in the configuration of the Unified Firewall after an update to LCOS FX 10.13 Rel or 10.13 RU1, a mail server (e. g. Microsoft Exchange) could no longer receive e-mails. If the inbound proxy (SMTP-IN) was deactivated, e-mail reception worked again.

→ After logging in with read authorization on the web interface of the Unified Firewall, connections between desktop objects were no longer displayed.

→ An update to the Squid proxy has fixed a vulnerability in the web proxy that allowed attackers to smuggle data through the proxy using request/response packets in HTTPS 1.1 or ICAP.

→ If a curl command with POST data was entered as a heartbeat via the web interface, the Unified Firewall did not assemble the command correctly. As a result, the command was not executed and was instead acknowledged with error messages.

→ When using the UTM features ‘Antispam and Contentfilter’, it could happen that the responsible process (bdamserver) utilized a CPU core to 100 %. This resulted in websites being opened very slowly.

→ With the VPN service (xipsecd), it could happen that duplicate instances were displayed for a VPN tunnel configuration.

LCOS FX improvements 10.13 RU1

Note

Due to an adaptation of the REST API, the LMC add-ins must also be adapted accordingly.

Bugfixes

→ After an update to LCOS FX 10.13 REL, it could happen that the rules for IPSec connections could no longer be written. As a result, communication via IPSec connections was only possible to a limited extent or not at all.

→ After installing an LCOS FX 10.13 Rel ISO file and importing a backup file with an error-free DNS configuration, the DNS name resolution of the Unified Firewall no longer worked. As a result, anti-virus signatures, for example, could no longer be updated.

LCOS FX improvements 10.13 Rel

Bugfixes

→ After configuring an IPSec connection via the LMC, it could happen after some runtime that monitoring information was not always transmitted to the LMC. This resulted in the monitoring information in the LMC being incomplete.

→ When the Content Filter was used in DNS web filter mode, it could happen that DNS requests from devices in the local network were blocked. As a result, the requested resources could not be accessed by the devices.

→ In individual cases, it could happen that the route of a WAN connection with transfer network was not written to the associated routing table. In such a case, access from the transfer network to the Unified Firewall was not possible, because the Unified Firewall sent the response to the default gateway in the transfer network instead of to the requesting device.

→ If a configuration menu was called whose feature was not included in the license used (e.g. IDS/IPS on a UF-60 Unified Firewall), the menu was displayed in read mode with missing write permissions.
For corresponding configuration menus, a message is now displayed that the feature is not supported by the license.

→ Apple devices with iOS 17.0.3 could not establish an IPsec VPN connection via default iOS profile to the Unified Firewall, because the security profile of the Unfied Firewall did not match. The encryption profile ‘AES-GCM 256 bit with 128 bit ICV’ has now been added to the firewall configuration so that VPN connections can be established again.

→ If the web client certificate was replaced in the ‘Firewall / Firewall access / Web client’ menu, the new certificate was retained until the firewall was restarted. After the restart, the certificate was reset to the default LCOS FX certificate.

→ It could happen that firmware updates were executed although they were supposed to be installed at a different time according to the configured schedule. This behavior occurred especially when a configuration was rolled out from the LMC to the Unified Firewall.

LCOS FX improvements 10.13 RC1

New features

→ **New dialog for connecting desktop objects**

The redesigned dialog for connecting desktop objects provides an optimized overview for complex firewall rules including inheritance. The new feature includes the display of rules defined between parent objects in the table view. This enhanced view allows you to see the entire hierarchy of rules at a glance, while taking into account both selected services and the rules between parent objects.

Further improvements

→ For route-based IPSec connections, the MTU can be set to solve packet size issues in some scenarios.

→ For monitoring WAN connections, tcp_probe can be used with hostnames.

→ Curl can be used to monitor WAN connections.

Bugfixes

→ Due to a change in the encryption algorithms of the OpenVPN client as of version 2.6.0, it was not possible to establish VPN connections to the Unified Firewall. The OpenVPN client from version 2.6.0 can now be used.

→ A WEBconfig tunnel established between the LMC and a Unified Firewall lost connection to the device when a desktop object was clicked in the configuration interface.

→ The line monitoring of a WAN connection via ‘tcp_probe’ did not work correctly. In a backup scenario, this resulted in the Unified Firewall not detecting a failure of the main line and not switching to the backup connection.

→ After a firmware update to LCOS FX 10.12, an activated notification function was deactivated and had to be reactivated manually.

→ In a load balancer scenario, IP packets were sent to a WAN connection even if it was offline.

→ It was not possible to use SNMPv3 with the 3DES privacy protocol. The selection for 3DES has now been removed from the configuration.

→ Exception rules could also be created for IDS/IPS if a user profile had ‘read-only’ permissions or if the Unified Firewall license had expired.

→ When using a backup connection, it could happen that traffic from an IPsec connection was sent to the backup connection even though it was not established.

→ For ‘Multi-WAN weighting’, values between 1 and 256 could be assigned, although the kernel only allows a maximum value of 253. If a value between 254 and 256 was stored, the Internet connection did not work.
Now only values between 1 and 253 can be assigned.

→ Re-keying with the hash algorithm SHA1 led to a connection termination and subsequent reestablishment for an IPSec connection.
Furthermore, the Unified Firewall selected the worse algorithm for an IPsec connection with multiple hash algorithms (e.g. SHA-256 when using SHA-256 and SHA-512).

→ In individual cases it could happen that the service ‘suricata’ generated a lot of error messages and stored them on the hard disk until it was full.

Additional information

→ SHA1, MD5, and 3DES have been removed from all IPSec default profiles. If you use IPSec connections with deprecated remote peers, SHA1, MD5, and 3DES can still be used with custom profiles. For security reasons, the use of SHA1, MD5, and 3DES is strongly discouraged!

5. Further information

→ Backups of versions 9.6, 9.8 und 10.X are supported.
→ Devices with less than 4 GB of RAM can not execute all UTM features simultaneously.

6. Disclaimer

LANCOM Systems GmbH does not take any guarantee and liability for software not developed, manufactured or distributed by LANCOM Systems GmbH, especially not for shareware and other extraneous software.

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