LANCOM Release Notes

LCOS FX 10.4

LANCOM Systems GmbH
Adenauerstrasse 20 / B2
52146 Wuerselen
Germany

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

November 1st, 2019, CBuersch

Table of Contents

1. Preface

LCOS FX is the operating system for all LANCOM R&S®Unified Firewalls. In the context of the hardware given by the products the at a time latest LCOS FX version is available for all LANCOM R&S®Unified Firewalls and is available free of charge for download from LANCOM Systems.

This document describes the innovations within LCOS FX software release 10.4, as well as the improvements since the previous version.

2. Supported hardware

Version 10.4 supports the following 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 supports the following virtual appliances:

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

Version 10.4 supports the following hypervisors:

- Vmware ESX
- Microsoft HyperV
- Oracle Virtualbox

3. Installation instructions for updating to LCOS FX 10.4

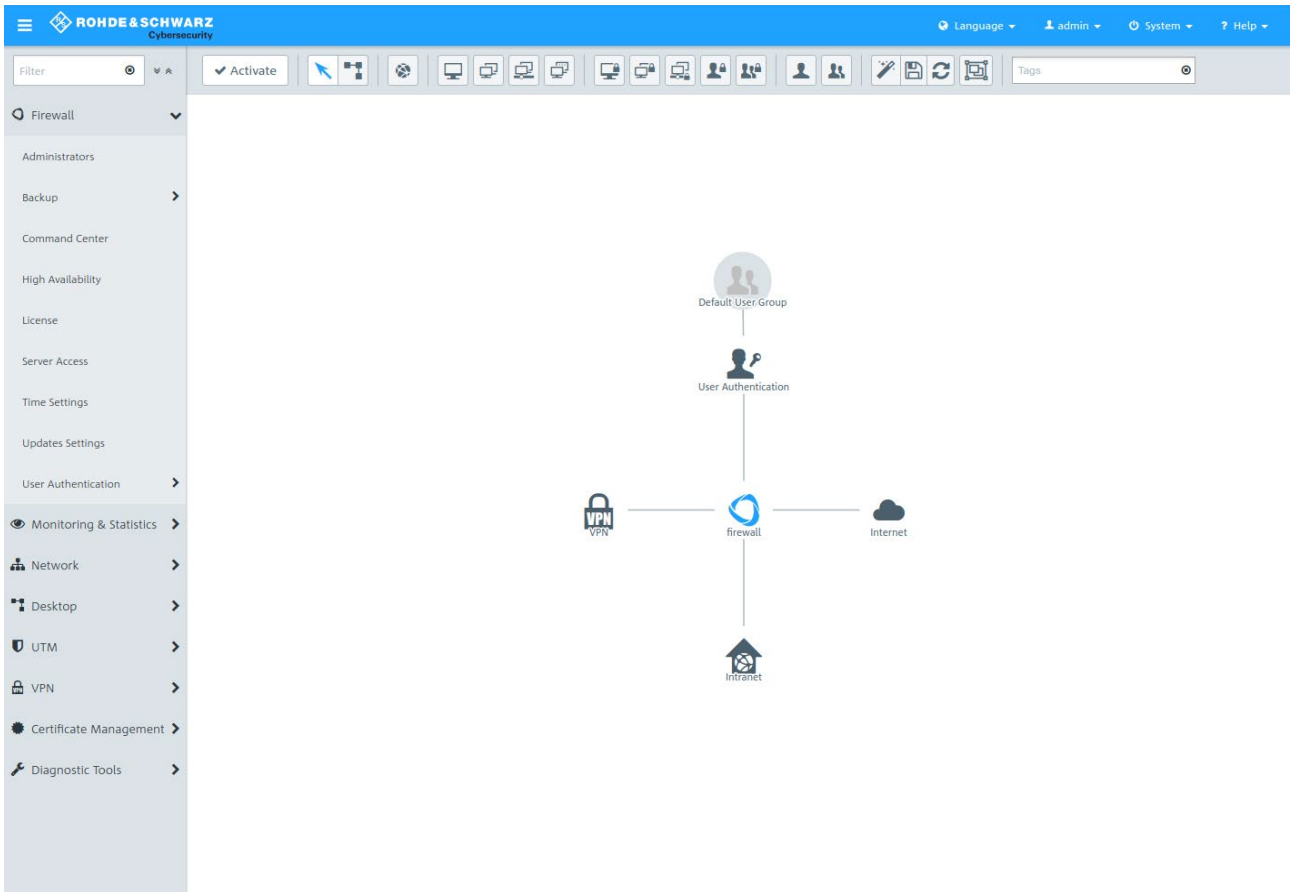
Note 1:

If there is not yet a working 10.2.0 firewall installation, please setup a simple 10.2.0 firewall installation with Internet connection first (see document „First installation steps"). An Internet connection is mandatory to receive updates.
Via the auto updater on the web interface of your LANCOM R&S®Unified Firewall the respectively newer minor update version is available for step-by-step updating.
Please follow the subsequently described steps in this manual to update your device to the latest LCOS FX version.

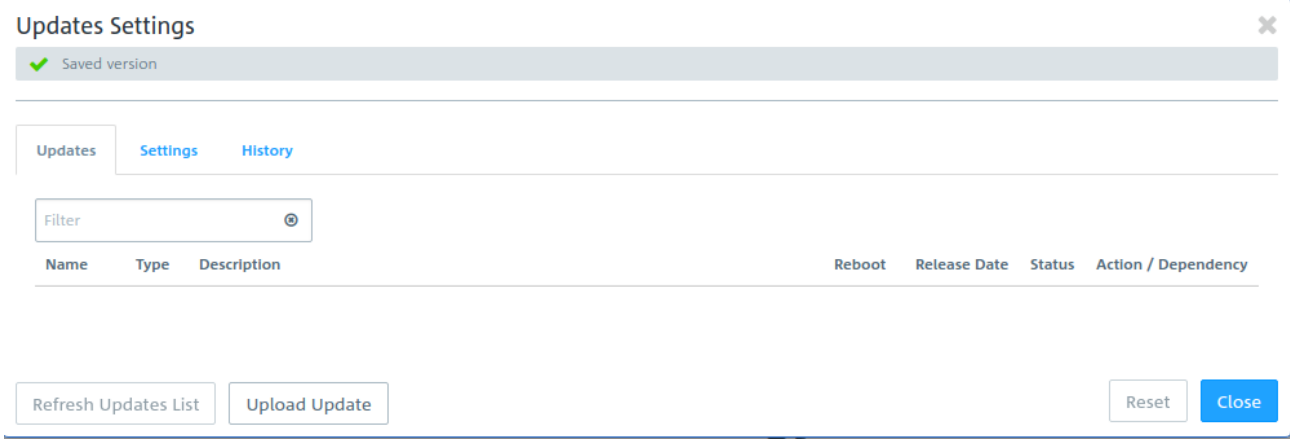
Note 2:

In order to not hinder any workflows, please first install the update in a testing environment and not in a productive setting.

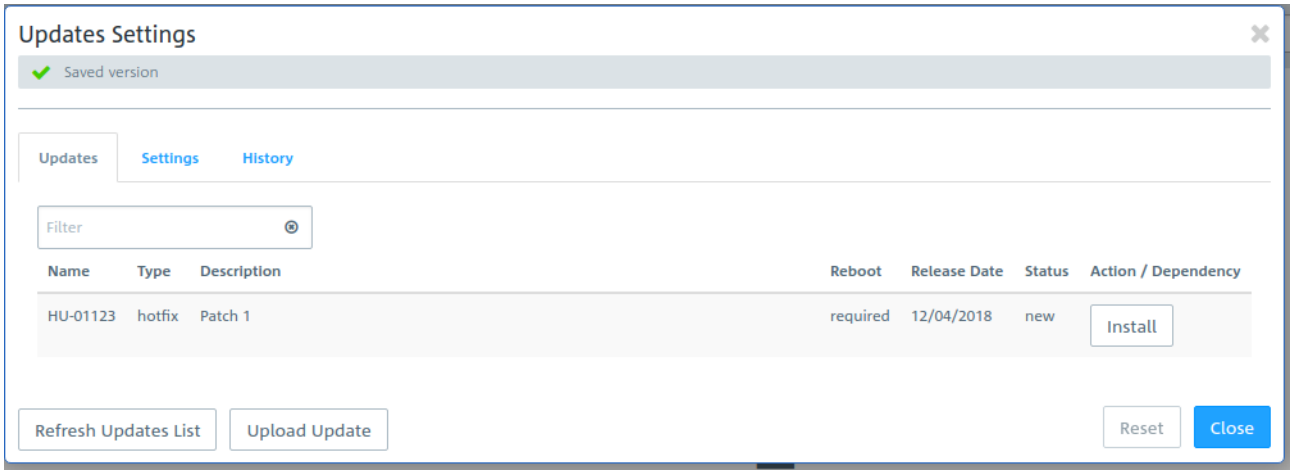
In the navigation bar on the left side, select “Updates Settings“ under the first item “Firewall“.



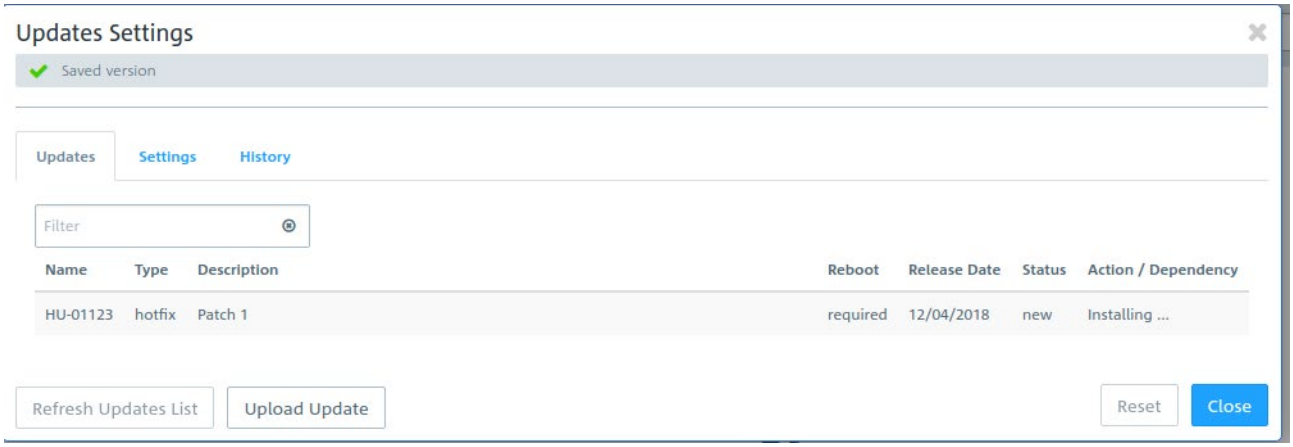
In the opening window “Updates Settings“ press the button “Refresh Updates List“ under the tab “Updates“.



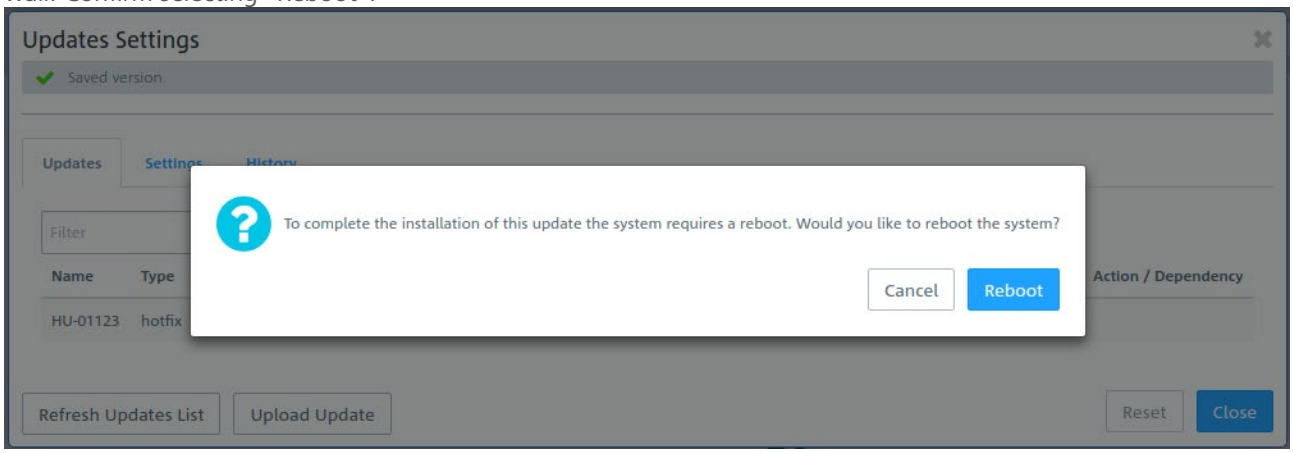
From the list, select the firmware file to install and press the “Install” button.



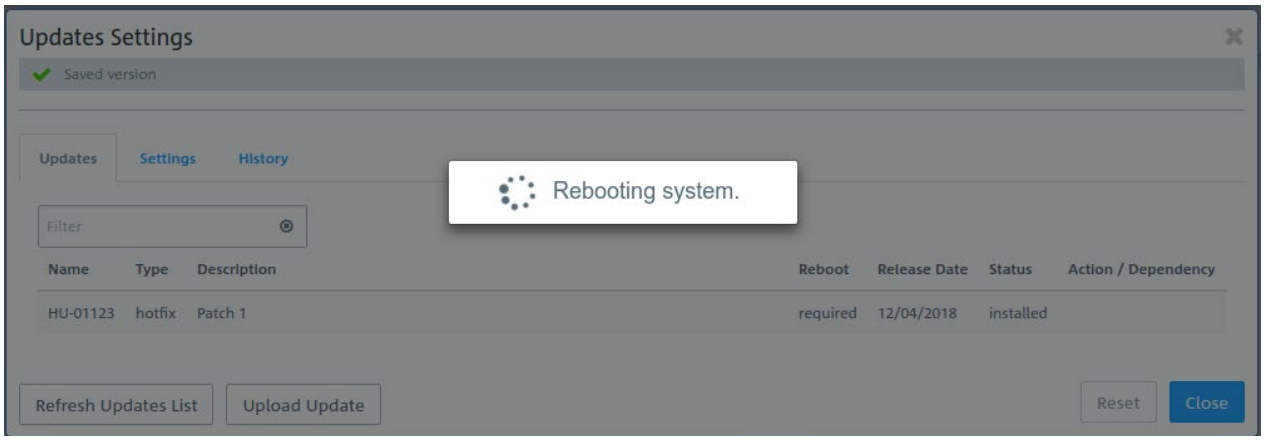
The status of the action changes to “Installing...”



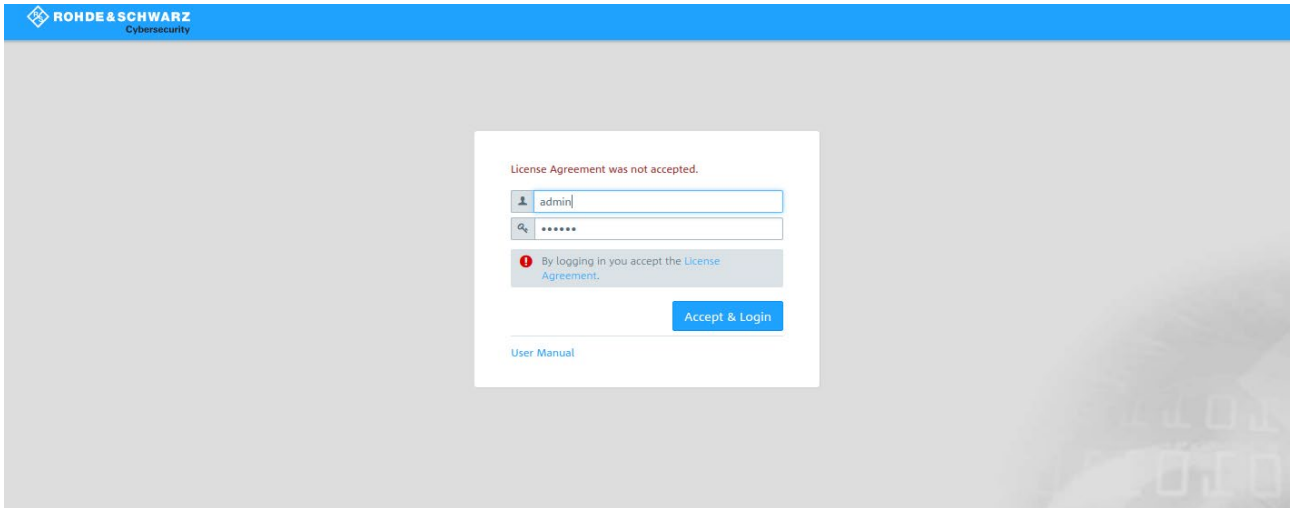
After the installation has completed a popup dialogue window appears displaying a request for rebooting the firewall. Confirm selecting “Reboot”.



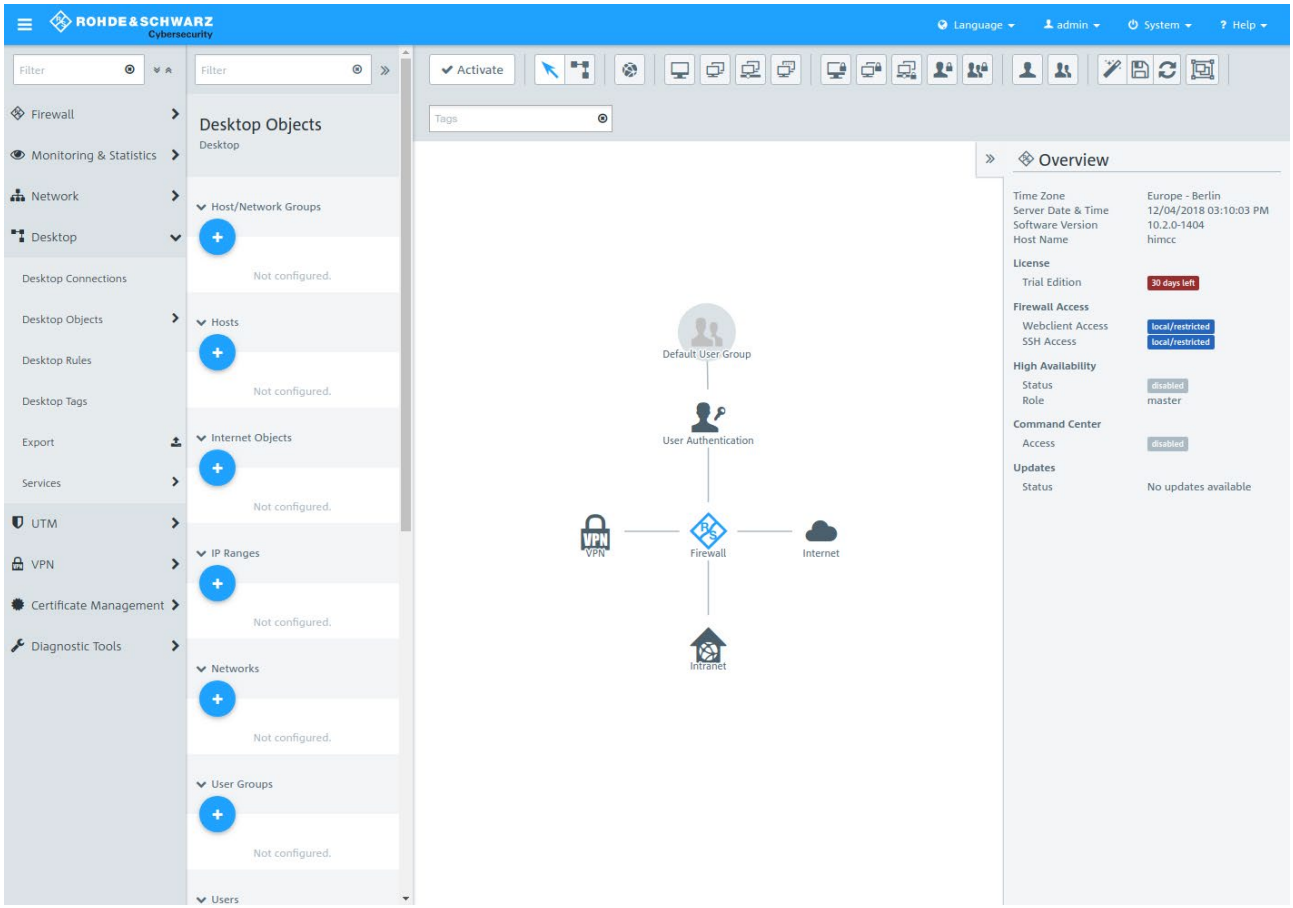
The system is rebooted.



After the firewall reboot the login window appears. When typing in your login credentials you are asked to accept the license agreement.



After having logged in, the desktop of your LANCOM R&S®Unified Firewall opens. You will notice the info bar on the right side. Here you can see information about the current software version and others.



LANCOM Systems

4. History LCOS FX

LCOS FX changes 10.3.3 > 10.4

New features

Initial setup wizard

Setup your firewall in less than 5 minutes, including Internet access, local networks, and UTM features.

In 4 simple steps the wizard configures:

- Firewall hostname
- Internet access
- Local networks
  - IP addresses
  - DHCP servers
  - Internet access rules
- UTM features (anti-malware, IDS/IPS, URL- and Content-Filter)

Integration to the LANCOM Management Cloud

- **SD-SECURITY**
  - Enables cross-site application managment
  - Configure application access only once per network for easy rollout to all sites
- **Monitoring**
  - Device status (hardware load, interface throughput, ..)
  - Security status (blocked connections, blocked contents like malware)
- **Webclient tunnel**
  - Easy access to the complete firewall management interface
- **Cloud-ready**
  - As from LCOS FX 10.4 all newly delivered Unified Firewalls are cloud-ready.
  - Simply connect and manage instantly via the LMC

New IPSec implementation

- Comfortable handling due to reusable security profiles for IKE and ESP
- Predefined profiles for common clients (Windows 10, iOS, Android, LANCOM Advanced VPN Client) and servers (LCOS FX 10.4, LCOS 10.30 or newer)
- Configuration export for the LANCOM Advanced VPN Client
- Configuration of multiple networks in one connection to reduce configuration efforts
- Option for connecting external DHCP- and RADIUS servers
- Support for Hub-and-Spoke architectures
- Option to specifically configure the external tunnel IP address

E-mail notifications

- Direct information about important events by e-mail, optionally immediate or time-aggregated (configurable per event type)
- Events
  - Internet connection broken / reconnected
  - IPSec Site-to-Site tunnel broken / reconnected
  - High availability switch-over
  - Firewall restart expected / unexpected
- Optional: delivery via mail relay
- Optional: encrypted delivery using SMIME

Improvements

- User-specific application filter rules
  - Combination of user authentication and application filter
  - Specific application profiles for single users or groups
    Connection to active directory (assignment to a group / department directly creates the appropriate application filter rules)
- Configuration and logs can be reset to delivery condition.
- Linux kernel updated to 4.19.69
- SNMP statistics show virtual network interfaces too, e.g. VLANs.
- SNMP statistics show firewall alarms.
- The browser reloads the webclient automatically after the connection has been lost.
- The automatic webclient logout is reset on mouse movement, too.
- The currently active license can now be downloaded under Firewall > License.

Bugfixes

- Fixed an issue within the memory management which could cause unexpected restarts.
- Fixed stability issues with a high amount of IPSec tunnels.
- A Kerberos-Ticket is now created accurately even with capital letters within the hostname.
- Timeout to small for TCP connections
- Statistics are working after disabling the high avalibility mode.
- The high avalability mode has been modified for installations without DNS resolve.
- The ‘web proxy did not start’ issue has been fixed.
- Improvements for the timeout handling of the user authentication at weblogin
- Stability issues with particular VPNSSL site-to-site connections have been fixed.
- The Anti-virus on the UF-50 is now accurately disabled in all cases.
- Some redundant log entries have been removed.
- The handling of DNS servers which have been obtained by DHCP has been corrected.
- The stability of the weblogin service for user authentication has been improved.

- The Internet connection can be selected from the Internet object right after deleting.
- All firewall services ignore disconnected Internet connections.
- Removed an automatic rule for blocking TCP connections with MSS less than 512.

Additional Information

- Stronger password guidelines for webclient administrators and for the console password
  - minimum of 8 characters
  - minimum of 3 character types (upper case, lower case, digits, special characters)
- Modified standard backup for delivery and initial installation
  - eth0 obtains the IP address and default gateway by DHCP
  - eth1 to eth3 enable the DHCP server for simplified initial setup
- Added the LANCOM support IPs to the preconfigured IPs for webclient- and SSH access.
- Custom scripts are disabled when upgrading.

LCOS FX changes 10.3.2 > 10.3.3

Improvements

- Added German manual
- Updated manual to V10.3
- Added support for new UF-100/200 hardware revision

Bugfixes

- Fixed issue which could result in hardware appliances displaying virtual machine UUID in license dialog
- Fixed issue which could result in failing synchronization in High Availability
- Fixed issue in mailproxy if client side closes connection too early
- Fixed issue which lead to already installed patches being installable again

LCOS FX changes 10.3.1 > 10.3.2

Bugfixes

- Fixed problem with license handling which could result in an appliances losing the license
- Status of IPsec site-to-site is correctly recognized in all cases
- DNS server is correctly restarted after receiving DHCP lease
- Removed verbose mailproxy logging
- High availability now handles Umlauts in network connections correctly

LCOS FX changes 10.3.0 > 10.3.1

Improvements

- Linux kernel security update to version 4.19.53 to fix the vulnerability CVE-2019-11477

LCOS FX changes 10.2.3 > 10.3.0

New features

- Alert log
  - Alerts are logged separately
    Covers blocked connections, finished connections, malware, IDS/IPS, web filter, URL/Content filter, anti-spam and the application filter
  - Easy-to-build complex filter queries with AND, OR, NOT operators
    Smart filter proposals allow for constructing precise queries, matching specific alert attributes such as port numbers and source IP addresses

- Online updates are possible in HA mode
- Linux kernel security update to version 4.19.29

Improvements

- Licenses compatible across versions
- Improved performance of log view
- Network interface drop-down lists show attached connections and IP addresses.
- Updated pre-defined services
- Improved usability of DMZ rule creation
- Automatic log-out from web client after 10 minutes
- Configurable end-of-license behavior
- Improved stability of IPSec tunnels
- Improved stability and performance of mail proxy
- Pending changes on the rule desktop are saved on log-out
- Log database size is now capped at approx. 8 Gbyte to ensure system stability; the oldest log entries are deleted.

Additional information

- The end-of-license behavior changed compared to V9.X.
  If you migrate from version V9.X, navigate to “Firewall” > “License” to adapt the end-of-license behavior.
- By default, LANCOM R&S®Unified Firewalls check for software updates once per day. Navigate to “Firewall” > “Updates Settings” to change this interval.
- Backup import supports the migration from versions V9.4 to V9.8 and V10.0, V10.1 and V10.2.
- Devices with less than 4 Gbyte RAM do not support all UTM features to be activated simultaneously.

Discontinued features

The following features are no longer available in LANCOM R&S®Unified Firewalls version 10.3.0:

- PPTP VPN connections
- E-Mail reporting
- LAN accounting
- VPN SSL bridges
- Desktop notes
- Dynamic routing
- Connection-specific DNS servers
- Centralized management of the LANCOM R&S®Unified Firewalls using the gateprotect Command Center. Instead, use the LANCOM R&S®UF Command Center.

LCOS FX changes 10.2.2 > 10.2.3

Improvements

- Allow Outlook Anywhere to traverse the reverse proxy
- Administrators can adjust upstream ciphers that are accepted by the HTTP proxy.
- Linux kernel security update to version 4.14.103
- Improved handling of large content filter blacklists
- Increased responsiveness of the Info area
- Increased mail proxy performance
- Reduced hard disk write-load
- Improved backup compatibility
- Improved import of multi-tier certificate chains

LCOS FX changes 10.2.1 > 10.2.2

Improvements

- Optimized web-proxy logfile handling
- Improved backup migration

LCOS FX changes 10.2.0 > 10.2.1

Improvements

- Fine-grained IP-based access control for SSH and webclient management interfaces
- Configurable listening ports for SSH and webclient management interfaces
- Info area to show detailed information on desktop nodes
- Whitelist for e-mail proxy to exclude particular senders/receivers from virus scan
- Configurable HTTPS certificate for the webclient
- SSL proxy support dropped for various outdated ciphers

LCOS FX 10.2.0

New features

- Integration of Avira Antivirus:
  - Avira Protection Cloud: machine learning and sandboxing
- IDS/IPS:
  - Improved performance thanks to a new IDS/IPS engine
  - Simplified IDS/IPS configuration including a rule exception list for eliminating false-positive results
- Statistics:
  - Security messages
  - Traffic counter
- Protocols:
  - Security messages
- Web proxy upgrade:
  - Improved HTTPS support
  - Improved performance
- FTP proxy upgrade
- Reverse proxy upgrade
- Support for link aggregation/bonding of ethernet interfaces

Improvements

- Searchable description field for desktop objects and firewall rules
- Services can be grouped.
- Desktop objects for "Host-/Network groups" can contain hosts and networks.
- Desktop objects can be tagged and filtered by tags.
- Desktop configurations (i.e. an overview of the dektop objects and firewall rules) can be exported to the file formats PDF and HTML.
- Realtime connection tracking
- DNS search domains can be pushed vie DHCP.
- The webclient supports the offline upload of updates.

5. Further information

- Backups of versions 9.4 to 9.8, 10.0, 10.1, and 10.2 are supported.
- Devices with less than 4 Gbytes of RAM can not execute all UTM features simultaneously.

6. Known issues

- System- and audit protocols are not synced when operating in high availability mode.
- Some monitoring information is not yet available:
  - User login status
  - Network interfaces load

7. 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.