LCOS FX 10.6

Cloud-managed VPN and even more control

With the new release version LCOS FX 10.6, you get a real plus in convenience and control when operating your LANCOM R&S®Unified Firewalls: Among other things, more convenience is provided by a wide range of features for highly automated operation with the LANCOM Management Cloud (LMC). And for more control, zone management in DNS allows separate DNS configuration for individual networks.

- Extended feature set for cloud-managed firewalls
- Zone management for DNS

LCOS FX LANCOM Operating System

LCOS FX 10.6 highlights	
Extended feature set for cloud-managed firewalls*	LANCOM FX 10.6 upgrades the LANCOM R&S®Unified Firewalls with many additional functions for operation with the LANCOM Management Cloud (LMC) and turns them into a fully-fledged stand-alone VPN gateway for branch offices: From now on, secure VPN networking of sites, including network virtualization, is fully automated. Thanks to the support of LMC's DynDNS service, firewalls are also easily reached via a self-selected subdomain. Furthermore, applications can now also be blocked by the firewall in stand-alone mode at layer 7 level.
Zone management for DNS	From now on, the LANCOM R&S®Unified Firewalls support different DNS servers for different zones. In addition, the DNS configuration for individual networks can be adjusted separately. This allows separate DNS configuration for individual networks so that, for example, local zones can be accessed exclusively from the employee network and not from the guest network.

*Support of these features in the LANCOM Management Cloud will follow soon.

LCOS FX LANCOM Operating System

LCOS FX 10.5 highlights	
IMAP proxy	The IMAP protocol is especially interesting for users who do not operate their own e-mail server, but instead handle their e-mail traffic via an external service provider. E-mails are processed on the provider's server, so that the respective message is available in the same version on all end devices. Now, the LANCOM R&S®Unified Firewalls also have an IMAP proxy for the first time, which can be used to scan the entire mail traffic of the IMAP server for trojans, viruses, and other threats. Spam mails are detected and sorted out. Even zero-day protection is possible thanks to the use of sandboxing and machine learning of the firewalls.
Content-Filter Override	Especially in school networks a content filter is essential. Pupils should be protected from content that is harmful to young people or illegal, and even visiting otherwise unproblematic websites and content can quickly become a major factor of distraction in class. But although it makes sense to block YouTube, for example, during school hours, it can also make sense to use this service selectively. For this purpose, the teacher can now send a code to his pupils, which temporarily overrides the filter rule. As soon as the lesson is over, the filter rule is applied again and denies access to the website or application.
Application Based Routing	Recognized protocols and applications can be specifically routed using the PACE2 DPI Engine. Three different options are available for this. In a specific multi-WAN scenario, for example, the usable connection can be specifically selected for certain outgoing connections and, for example, streaming services can be routed via the slower line, while VPN, as the carrier of business-critical data traffic between the branch office and the headquarters, can be routed via the faster line. Trusted cloud applications can be excluded from the proxy or certain applications can be routed directly to the provider at the branch office instead of via IPSec tunnels, despite the fact that the rest of the Internet traffic is sent to the headquarters via a secure connection.
Further features	
Desktop search	DThe desktop tags filter is extended to the desktop filter. It can now be used to search for both desktop objects and desktop connections. Objects and connections that do not match are hidden. This function can be used to search for a variety of parameters such as the name of the relevant desktop object, IP addresses, networks and areas, VPN SSL connection names or proxy flags.
Creating rules from the protocol	New rules can be created directly from alarm or system log entries about denied access. If, for example, the firewall with the current rules blocks certain network traffic that is actually desired, a new rule can be created with a few clicks based on the corresponding protocol entry to allow traffic in the future.
Recovery points	Upgrading to the next firmware version is now no longer a cause for concern. A recovery point is automatically created before the process starts. If not everything works to your complete satisfaction after that, simply reset your firewall to the working initial state.
VPN-SSL bridging	With this function, two or more networks at different locations can now be securely and reliably connected on layer-2. The two networks that are separated from each other thus act as one network and communication of non-IP based protocols can take place in between.
Multiple administrators logged in	Now it is possible for multiple administrators to be logged in to the web client of the LANCOM R&S®Unified Firewall at the same time. Only the first administrator who logged in first is allowed to write to the web client and can thus make changes to the configuration. All other administrators are granted read-only rights. As soon as the first administrator logs off, the write permission is transferred to the next administrator logged in. A significant simplification, especially in larger administration teams.
LCOS FX 10.4 highlights	
Setup Wizard	With this release version, the firewall gains an intuitive installation wizard for easy initial configuration in under five minutes—a few clicks of the mouse is all it takes. Internet access and IP address assignment, as well as UTM features such as anti-malware, IDS/IPS, and URL & content filtering, are now set up quickly and easily.
Cloud-managed firewall	The LANCOM R&S®Unified Firewalls are now cloud-ready! Devices are connected to the LANCOM Management Cloud (LMC) by a simple yet secure PIN- or activation code-based pairing procedure. They then appear in the device overview, which offers clearly structured monitoring of the device status and also features an alerting function. A web tunnel provides access to the firewall management interface for remote configuration from the LMC.
Further features	
Layer 7 Application Management within the LANCOM Management Cloud	Via the LMC, firewalls can now be used stand-alone or in conjunction with LANCOM routers to create rules and then rolled out to the individual locations to block particular applications or allow direct access.
Ready-to-use integration of the LANCOM Advanced VPN Client	This firmware release makes it easy to create turnkey import profiles for the LANCOM Advanced VPN Client. These profiles are exported as *.ini files and can be imported into the client in just a few steps. This then uses the available connection medium to establish a secure VPN connection to the remote site.
Alerting and e-mail notification	As of this firmware version, the firewalls send e-mails with information about important events. This is performed either immediately when the event occurs, or in aggregated form. You can configure how often e-mails are sent for each type of event. Events include network disconnects, connection re-establishment, firewall restarts, or high availability switch-over.
User-specific application filter rules	As of this firmware release, the LANCOM R&S®Unified Firewalls also support the combination of user authentication and application filters. Specific application rules can be assigned to certain groups or even to individuals in the organization.

LCOS FX LANCOM Operating System

Features	Basic License	Full License	Feature description
Content Filter	UF-50 only	✓	URL and content filter Customizable rules for users Blacklists / whitelists Import / export of URL lists Category-based website blocking (individually definable) Online scan technology HTTP(S) proxy support Override function
Application control*		✓	Layer-7 packet filter (DPI) Filter by applications (e.g. Facebook, YouTube, BitTorrent, etc.) Blacklists / whitelists Protocol validation HTTP and IEC 104 decoder R&S®PACE 2 (Protocol and Application Classification Engine) *) available for LANCOM R&S®Unified Firewall UF-60, UF-160, UF-260, UF-300, UF-500, and UF-9XX
Antivirus*		✓	HTTP/S, FTP, POP3/S, SMTP/S, IMAP/S Configurable exceptions Multi-level scanning (local and cloud-based) Sandboxing Fast classification of zero-day threats through AI technologies (machine learning) *) available for LANCOM R&S®Unified Firewall UF-60, UF-160, UF-260, UF-300, UF-500, and UF-9XX
Antispam*		✓	POP3/S, SMTP/S, IMAP/S Configurable scan levels GlobalView Cloud using Recurrent Pattern Detection (RPD) – spam detection based on the e-mail distribution patterns Blacklists / whitelists Automatic e-mail rejection/deletion *) available for LANCOM R&S®Unified Firewall UF-60, UF-160, UF-260, UF-300, UF-500, and UF-9XX
IDS (Intrusion Detection System) / IPS (Intrusion Prevention System)*		✓	Protection from DoS, port scans, malware, botnets, exploits, and vulnerabilities More than 40,000 active signatures Configurable exceptions Scans all interfaces *) available for LANCOM R&S®Unified Firewall UF-60, UF-160, UF-260, UF-300, UF-500, and UF-9XX
Proxies	HTTP VoIP	✓	HTTPS, FTP, POP3/S, SMTP/S, IMAP/S, SIP HTTP (transparent/non-transparent) Reverse proxy Supports Active Directory and local users Time-controlled
LAN/WAN support	✓	✓	Ethernet 10/100/1,000/10,000 Mbps Configurable MTU (Ethernet/DSL) Link aggregation xDSL Multi-WAN (weighted policy-based routing/failover) Load balancing Time restrictions for Internet connections Multiple, dynamic DNS support DHCP DMZ SNAT
VLAN	✓	✓	4096 VLANs per interface 802.1q header tagging (packet-based tagged VLANs) Compatible with bridging
Bridge mode	✓	✓	Layer-2 firewall Spanning Tree (bridge ID, port costs) Unlimited number of interfaces per bridge
Monitoring & statistics	✓	✓	Statistics (IDS/IPS, application control, surf control, antivirus/antispam) Logging to external syslog servers Export as CSV and XLS files SNMP/v2c and v3 Connection tracking
Administration	✓	✓	Object-oriented configuration Role-based administration Command-line interface (SSH) Saves desktop as PDF and HTML IP-based access restriction for SSH and web client
Web interface	✓	✓	Self-explanatory functions Practical wizard for initial setup Overview of the entire network Overview of all active services Browser-based, platform-independent View filtering based on custom tags

LCOS FX LANCOM Operating System

Features	Basic License	Full License	Feature description
QoS	✓	✓	Guaranteed QoS bandwidth configurable for Internet connections QoS with ToS flags QoS in VPN connections
X.509 certificates	✓	✓	CRL (Certificate Revocation List) OCSP (Online Certificate Status Protocol) – network protocol for X.509 certificate status validation Multi-CA support Multi-host certificate support
VPN	✓	✓	User authentication High availability Site-to-site and client-to-site Client configuration packages
IPSec	✓	✓	Full-tunnel mode IKEv1, IKEv2 PSK (pre-shared key) / certificates DPD (Dead Peer Detection) NAT-T XAUTH, EAP Port configuration
SSL-VPN	✓	✓	Routing mode VPN Bridging mode VPN TCP/UDP Specification of WINS and DNS servers
Backup and restore	✓	✓	Local or remote access Automatic import during installation Automatic and scheduled backups Automatic upload (FTP, SCP) Disaster recovery from USB drive
User authentication	✓	✓	Active Directory import Local user administration Authentication via web or client Single sign-on (Kerberos) Multiple logins Captive portal Terminal Server Support (via Remote Desktop IP Virtualization)
HA (High availability)*	✓	✓	A second Unified Firewall of the same type is required Stateful failover Active/passive Hot standby *) available for LANCOM R&S®Unified Firewall UF-60, UF-160, UF-260, UF-300, UF-500, and UF-9XX

LANCOM, LANCOM Systems, LCOS, LANcommunity and Hyper Integration are registered trademarks. All other names or descriptions used may be trademarks or registered trademarks of their owners.
This document contains statements relating to future products and their attributes. LANCOM Systems reserves the right to change these without notice. No liability for technical errors and/or omissions.
05/2021