LANCOM SYSTEMS

lancom-systems.com

LCOS FX 10.12

Top efficiency for your network security

LCOS FX

LCOS FX 10.12 brings numerous improvements and features to your LANCOM R&S®Unified Firewalls. A new feature is support for the VPN standard „WireGuard“, which enables simple and efficient administration of VPN connections and offers high data throughput. You can also create firewall rules based on DNS. The graphical display of all important system parameters gives you a quick overview of firewall performance and load. And by automatically sending security reports by e-mail, you can optimize the monitoring and security of your network.

- → WireGuard
- → DNS-based firewall rules
- → Hardware monitoring
- → Sending security reports by e-mail

LANCOM SYSTEMS

lancom-systems.com

LCOS FX 10.12

LCOS FX 10.12 Highlights	
WireGuard	LANCOM R&S®Unified Firewalls now support the VPN standard „WireGuard“ for simple, fast, and efficient administration of VPN connections. The use of the noise protocol ensures an efficient handshake that effectively accelerates the establishment of VPN connections. In addition, high data throughput is achieved by reducing encryption parameters.
DNS-based firewall rules	As of LCOS FX 10.12, create firewall rules over and between DNS objects for easier management of dynamic and software-based networks. The use of host names instead of fixed IP addresses makes the creation of firewall rules particularly efficient.
Hardware monitoring	The graphical display of all critical system parameters, such as CPU, RAM, and hard disk utilization, provides a quick and comprehensive overview of the performance and workload of the LANCOM R&S®Unified Firewalls. The assignment of resource consumption to features and processes makes it possible to quickly identify bottlenecks and weak points and to take targeted optimization measures.
Sending security reports by e-mail	Efficient archiving and auditing is made possible by automatically sending security reporting by e-mail at configurable intervals. This offers a clear advantage in terms of monitoring and security of your network, as relevant security information is provided promptly and reliably.
Weitere Features	
BGP extensions	Multihop BGP support for transmitting BGP packets through an IPSec tunnel Selection of destination tables for learned routes to use policy-based routing with BGP
LLDP monitoring	Support of Link-Layer Discovery Protocol both as sender and receiver including display of currently visible neighbors
Export of protocols	System, alarm, and audit logs can be exported as PDF, HTML or CSV

LANCOM SYSTEMS

lancom-systems.com

LCOS FX 10.12

LCOS FX 10.11	
Migration of the content-filtering and anti-spam services	With LCOS FX version 10.11, content filtering and anti-spam services are provided by a new, specialized OEM partner. As far as possible, the migration will be automated. However, in some cases the categories cannot always be exchanged exactly, so you should check your Content-Filter configuration afterwards and make decisions manually if the assignments are unclear. Depending on the type of management and the number of your LANCOM R&S®Unified Firewalls, there are different migration alternatives: → Migration of a single LANCOM R&S®Unified Firewall → Migration of multiple LANCOM R&S®Unified Firewalls using the LANCOM web tool created for this purpose → Migration of LANCOM R&S®Unified Firewalls managed via the LANCOM Management Cloud This addendum to LCOS FX 10.11 explains how you can conveniently migrate your LANCOM R&S®Unified Firewalls in a way that is tailored to your situation.
LCOS FX 10.10 Highlights	
Add-in Generator	Quickly and easily multiply your ideal configuration from one Unified Firewall to any number of UFs managed by the LANCOM Management Cloud (LMC). Using the new Add-in Generator, you can easily generate entire add-ins or even individual add-in sections from the audit log of an initially configured Unified Firewall.
Further features	
BGP support for IPSec connections	By supporting BGP on active IPSec connections, you benefit from better load balancing and resilience. For this purpose, routes are announced only on active VPN tunnels.
Let's Encrypt for the reverse proxy	Now it is even easier to enable public access to internal (web) services such as Microsoft Exchange. The reverse proxy of the Unified Firewalls supports Let's Encrypt. This means that free and trusted certificates can be integrated and automatically be renewed via the Unified Firewalls in just a few simple steps.
Selection of the source connection for DNS servers	It is now possible to select, for example, a provider-specific DNS server per upstream in multi-WAN scenarios. DNS servers known via PPP as well as DHCP are now always automatically addressed via the appropriate line.
LCOS FX 10.9 Highlights	
BGP	With the use of the routing protocol BGP (Border Gateway Protocol), you now benefit from even more efficiency and stability in your networking scenarios. Comparable to a navigation system, BGP enables fast and dynamic distribution of routes by exchanging the best paths from the firewalls' routing tables so that packets can be distributed optimally over the network paths. Even if individual nodes or entire network sections fail, your components will find a way to maintain networking via BGP.
DNS Web Filter	Even in times of hybrid working with the use of user-owned devices (BYOD), you can rely on your business integrity. DNS queries that pass through the DNS server of the LANCOM R&S®Unified Firewalls are identified, classified, and filtered according to their categories or self-configured blacklists and whitelists. This DNS-based protection enables your LANCOM R&S®Unified Firewall to block unwanted and harmful page views – even on devices that are not managed by the respective organization. Especially in BYOD scenarios, as is common in school networks, this protects your network from phishing attacks or the unnoticed downloading of malicious software.
Further features	
Config Rollout	The config rollout of the LANCOM Management Cloud to the LANCOM R&S®Unified Firewalls has been significantly accelerated.
Senden von Debug-Informationen	In support cases, debug information can be sent directly from the Web client to the support team.
LCOS FX 10.8 Highlights	
Traffic Shaping	Traffic Shaping enables full control over the packet flow of your data traffic, thus guaranteeing that the applications that are important to you always perform at the best quality. For example, you can define a guaranteed or maximum bandwidth per desktop connection, as well as line prioritization. It is also possible to preconfigure common scenarios, such as VoIP telephony or video conferencing, so Traffic Shaping not only increases the quality of your prioritized data traffic, while also saving configuration time.
Maximum protection of minors	LCOS FX 10.8 maximizes the protection of underage end users, e.g. in schools or youth facilities. For example, the official website list of the „Bundesprüfstelle für jugendgefährdende Medien" (German Federal Review Board, BPjM) is now also part of the content filter of LANCOM R&S®Unified Firewalls. This means that URLs whose content is officially classified as harmful are not accessible to the relevant target group in Germany. Continuous updates and extensions of this list are guaranteed.

LANCOM SYSTEMS

lancom-systems.com

LCOS FX 10.12

LCOS FX 10.7 Highlights	
Re-Design Certificate Management	Until now, certificate management has been a time-consuming challenge for administrators. In order to simplify the handling considerably, LANCOM offers you a multitude of improvements for efficient certificate management with LCOS FX 10.7. The redesign offers full support for deep certificate hierarchies, flexible configuration options for key usage attributes and subject alternate names, and practical templates that can be used as templates for similar certificates. In addition, support for elliptic curve certificates and new hash algorithms means you are well prepared for future technologies.
Netmap	Network extension couldn't be easier! Thanks to Netmap (also called 1 to 1 NAT or N : N NAT), entire networks can now be mapped to other address ranges. This is a huge advantage whenever network extensions (for example due to expansions or company takeovers) are carried out and IT subnets between different locations overlap. Instead of adapting or reconfiguring entire networks or network areas, conflicts can simply be resolved with a few clicks by a suitable mapping on the firewall.
LCOS FX 10.6 Highlights	
Extended feature set for cloud-managed firewalls (Support of these features in the LANCOM Management Cloud will follow soon)	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.
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.

LCOS FX 10.12

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 10.12

General function overview

Features	Basic License	Full License	Feature description
Administration	√	√	Object-oriented configuration Role-based administration IP-based access restriction for SSH and web client
Anti-Spam **		√	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
Anti-Virus *		√	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)
Application Management **		√	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)
Backup and restore	√	√	Local or remote access Automatic import during installation Automatic and scheduled backups Automatic upload (FTP, SCP) Disaster recovery from USB drive
Bridge mode	√	√	Layer-2 firewall Spanning Tree (bridge ID, port costs) Unlimited number of interfaces per bridge
Content Filter		√	URL and content filter (incl. BPjM filter) Customizable rules for users Blacklists / whitelists Import / export of URL lists Category-based website blocking (individually definable) Online scan technology Based on HTTP(S) proxy Override function
DNS Web Filter		√	Filter by domain and content (incl. BPjM filter) Blacklists / Whitelists Import / export domain lists Category-based blocking of websites (individually configurable) Online scanning technology Based on DNS
Dynamic routing	√	√	Exterior BGP Internal BGP Announced routes configurable
HA (High Availability) ***	√	√	A second Unified Firewall of the same type is required Stateful failover Active/passive Hot standby
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

* Not available for LANCOM R&S®Unified Firewall UF-50
** Not available for LANCOM R&S®Unified Firewall UF-50 and UF-100
*** Not available for LANCOM R&S®Unified Firewall UF-50 and UF-100

LCOS FX 10.12

General function overview

Features	Basic License	Full License	Feature description
IPSec	√	√	Full-tunnel mode Policy-based or route-based IPSec IKEv1 (deprecated, upgrade to v2 strongly recommended), IKEv2 PSK (pre-shared key) / certificates DPD (Dead Peer Detection) NAT-T XAUTH, EAP Download portal for client configuration packages
LAN-/WAN support	√	√	Ethernet 10 / 100 / 1,000 / 10,000 / 40,000 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
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 Exportable executive report (PDF, HTML, CSV) Delivery of the Executive Report via e-mail Dashboard Hardware Monitoring
Packet filter	√	√	Stateful filter Rule objects based on source IP, source interface, DNS name, users / groups, VPN Rule connection based on protocol and destination port
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
SSL-VPN	√	√	Routing mode VPN Bridging mode VPN TCP/UDP Specification of WINS and DNS servers
Static routing	√	√	Freely configurable Multiple gateways configurable Policy-based routing based on input interface, source IP, output interface, destination IP
Traffic Shaping	√	√	Priority min. / max. bandwidth definable per traffic group (Quality of Service) Traffic grouping based on source application / destination / port / DSCP Different Traffic Shaping profiles selectable per WAN connection
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)
VLAN	√	√	4,096 VLANs per interface 802.1q header tagging (packet-based tagged VLANs) Compatible with bridging
VPN	√	√	User authentication High availability Site-to-site and client-to-site Client configuration packages

lancom-systems.com

LCOS FX 10.12

General function overview			
Features	**Basic License**	**Full License**	**Feature description**
Web interface	√	√	Self-explanatory functions Convenient wizard for initial setup Overview of the entire network Overview of all active services Browser-based, platform-independent View filtering based on custom tags
Wireguard	√	√	Quick and easy to configure Site-to-site, choice between 2 Unified Firewalls or Unified Firewall and third-party products Client-to-site with Windows, Linux, Android, iOS State-of-the-art cryptography protocols
X.509 certificates	√	√	Support of certificates based on RSA / Eliptic Curves CRL (Certificate Revocation List) Multi-CA support Multi-host certificate support Certificate templates import / export via PEM / PKCS12 / DER

LANCOM Systems GmbH
Adenauerstr. 20/B2
52146 Wuerselen | Germany
info@lancom.de
www.lancom-systems.com