

LANCOM R&S® Unified Firewalls

Network security by design

LANCOM R&S® Unified Firewalls complement your network by the relevant feature of cybersecurity. These easy-to-operate all-round solutions are tailored to the specific security needs of small and medium-sized businesses. Thanks to state-of-the-art security technologies and unified threat management (UTM), these next-generation firewalls provide reliable cybersecurity. A prominent feature is the innovative graphical user interface granting a concise overview of all of the secured areas in the company's network. Formerly complex and time-consuming configurations are greatly simplified since security policies can be systematically designed and enforced.

- Intuitive network visualization enabling easy implementation of security and compliance policies
- Detailed filtering and validation of applications and protocols
- Protection against spam, viruses, malware, and complex cyber attacks
- State-of-the-art security technologies such as R&S®PACE2 deep packet inspection
- Protection against zero-day threats due to integrated sandboxing and machine learning
- IT security "Made in Germany" and guaranteed without backdoors
- Option for virtual appliances
- Tried-and-tested procurement and support from LANCOM
- Integration into the LANCOM Management Cloud in preparation

LANCOM R&S® Unified Firewalls

Easy to use, maximum security

The rise in cyber threats is leading to increasingly rigorous demands on corporate security, data protection, and the availability of complex IT systems. The LANCOM R&S® Unified Firewalls are next-generation firewalls that offer all-round cyber security thanks to unified threat management (UTM). This includes the use of advanced cyber-security technologies such as sandboxing and machine learning. Furthermore, clustering and the use of redundant hardware ensures that the company's IT remains available at all times (High Availability).

Intuitive web interface

The easy-to-use web-based user interface of the LANCOM R&S® Unified Firewalls empowers users to deliver the highest levels of cyber security. Human error in the configuration of the firewall is greatly reduced as the network firewall rules are clearly and graphically displayed. The browser-based centralized management GUI enables granular fine tuning

while providing a comprehensive overview of the secured devices and connections in the network. This not only facilitates the implementation of compliance policies but also saves time by allowing rules to be combined efficiently. The device is easy on resources, which saves on costs and improves productivity. Insights are gained due to comprehensive audit and compliance reports.

Cloud-based protection against viruses and malware

Effective defense against malware and viruses is ensured by the firewall, which reliably detects suspicious files. To protect against as-yet unknown threats (zero-day exploits), suspicious files are first loaded into a protected cloud. In this isolated sandbox environment, the files can be securely and reliably tested. Analyses using third-generation machine learning based on billions of samples scan and proactively block threats based on their behavior. The cloud is hosted in Germany and complies with the European General Data Protection Regulation ("GDPR").

Screenshot of the web interface for creating and managing firewall rules

The screenshot displays the LANCOM R&S web interface for managing firewall rules. The interface is divided into several sections:

- Header:** Includes the LANCOM R&S logo, user information (Language, admin, System), and Help options.
- Left Sidebar:** Contains navigation menus for Firewall, Monitoring & Statistics, Network, Desktop, Desktop Connections, Desktop Objects, Desktop Rules, Desktop Tags, Export, Services, UTM, VPN, Certificate Management, and Diagnostic Tools.
- Main Content Area:** Shows a central network diagram with a central 'firewall' node. Various devices and connections are represented, including:
 - Desktop Connections:** office_hannover, roadwarriors, supplierX, supplierY, Default User Group, Sales, Marketing, User Authentication, Internet, WanUplink.
 - UTM:** milling machine controller, milling machine, Saw, final assembly, final_assembly_controller, SAP, Internal_Server, Fileserver final_assembly_controller, Office.
 - VPN:** VPN.
 - Mail Services:** Mailserver-Backend, Mailserver, Mailserver-Backend, Mailserver1, Mailserver2, external_mailgate, Customer_portal.
 - Other:** Guest_WiFi, supplier_portal, CMZ, Customer_portal.
- Right Sidebar:** Lists various connections and rules, such as Supplier's_X, Supplier's_portal, Office, Wantlink, Office, Firewall, Office, SAP, Office, Mailserver-Backend, Final_assembly_controller, Final_assembly, admin, Office, admin, Wantlink, Customer_portal, final_assembly_controller, Supplier's_Y, Supplier's_portal, Supplier's_portal, SAP, Guest_WiFi, Wantlink, Wantlink, Mailserver, Mailserver-Backend, Mailserver1, Mailserver2, external_mailgate, Customer_portal, SAP, ysa11, SAP, ysa12, office_hannover, and Internal_Server.

LANCOM R&S® Unified Firewalls

SSL inspection: Defense against complex cyber attacks through encrypted channels

Data-traffic encryption is increasingly widespread and, although this is welcome from the privacy point of view, there is the risk that malware enter systems via encrypted channels. Thanks to SSL inspection, even encrypted data packets can be scanned and filtered, applications detected, and compliance policies successfully implemented.

Deep packet inspection: Granular filtering and validation of applications and protocols

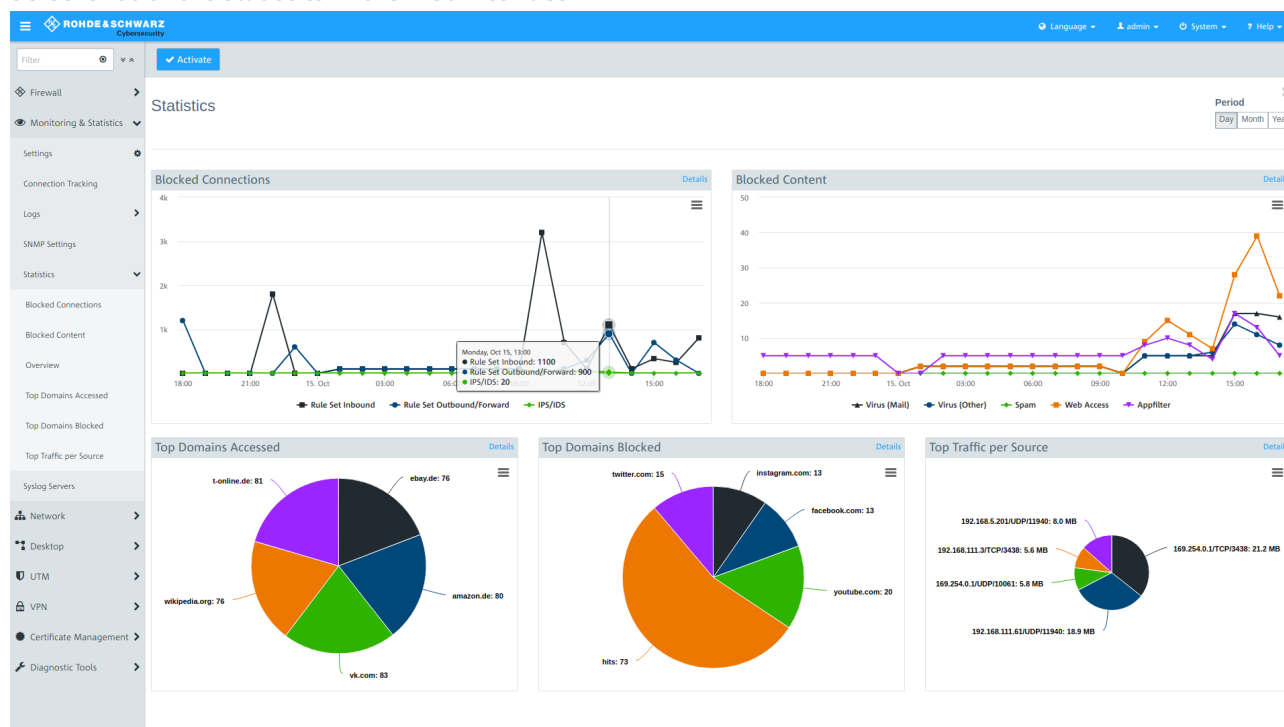
To protect against complex cyber attacks, the firewalls use deep packet inspection (DPI) providing insights into encrypted data traffic. Utilizing the industry-leading

R&S®PACE2 DPI engine, UTM firewalls enable accurate classification of network traffic, protocols and applications, as well as offer data loss prevention (DLP). Fine-grained security policies actively regulate the use of certain applications, such as streaming services or browsers.

Network & security “Made in Germany”

LANCOM R&S® Unified Firewalls are next-generation firewalls that are developed and programmed in Germany. Their UTM functions ideally complement existing LANCOM network infrastructures in terms of IT security. This constitutes a future-proof protection for corporate networks, guaranteed free of any backdoors.

Screenshot of the statistics in the web interface



LANCOM R&S® Unified Firewalls

Features: Appliances					
LANCOM R&S® Unified Firewalls	UF-100	UF-200	UF-300	UF-500	UF-900
Network interfaces					
Ports	4x GE copper	4x GE copper	8x GE copper	14x GE copper	8x GE copper (two slots for additional plug-in modules for 1G-ETH, 1G-SFP, and 10G-SFP+)
System performance					
IPS/IDS throughput (Mbps)	-	550	635	1,295	3,780
Firewall throughput (Mbps)	3,800 (UDP)	3,800 (UDP)	7,700 (UDP)	13,400 (UDP)	60,000 (UDP)
VPN throughput (Mbps)	430 (IPSec)	430 (IPSec)	620 (IPSec)	1,260 (IPSec)	4,280 (IPSec)
Concurrent sessions	1,000,000	1,000,000	1,000,000	2,000,000	16,700,000
New sessions per second	11,000	11,000	13,000	33,000	130,000
Number of users	5-30 concurrent users	5-30 concurrent users	30-100 concurrent users	100-200 concurrent users	100 concurrent users, extendable in steps of 100 to max. 500
Power					
Input voltage (V)	100-240	100-240	100-240	100-240	100-240
Power consumption (W)	36	36	150	150	2x300
Operating environment					
Operating temperature (°C)	0-40	0-40	0-40	0-40	0-40
Relative humidity (%)	5-90	5-90	20-90	20-90	5-90
Dimensions					
WxHxD (mm)	220 x 44 x 176	220 x 44 x 176	438 x 44 x 292	431 x 44 x 305	431 x 44 x 468

For dimensioning see LANCOM Techpaper Unified Firewall Sizing Guide.

Features: Virtual appliances				
LANCOM R&S® Unified Firewalls	UF-200 Virtual Appliance	UF-300 Virtual Appliance	UF-500 Virtual Appliance	UF-900 Virtual Appliance
Network interfaces				
Configurable switch ports	4	8	14	24
System performance				
Number of users	5-30 concurrent users	30-100 concurrent users	100-200 concurrent users	100 concurrent users, extendable in steps of 100 to max. 500

For dimensioning see LANCOM Techpaper Unified Firewall Sizing Guide. The performance of virtual appliances depends on the underlying hardware.

LANCOM R&S® Unified Firewalls

Features	
Web filter	<ul style="list-style-type: none"> URL and content filter Customizable rules for users Blacklists / whitelists Import / export of URL lists Blocks specified file types Category-based website blocking (individually definable) Online scan technology HTTP(S) proxy support Override function
Application control*	<ul style="list-style-type: none"> 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) <p>*) available for LANCOM R&S® Unified Firewall UF-200, UF-300, UF-500, and UF-900</p>
Antivirus	<ul style="list-style-type: none"> HTTP/S, FTP, POP3/S, SMTP/S Configurable exceptions Multi-level scanning (local and cloud-based) Sandboxing Fast classification of zero-day threats through AI technologies (machine learning)
Antispam	<ul style="list-style-type: none"> POP3/S, SMTP/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
IDS (Intrusion Detection System) / IPS (Intrusion Prevention System)*	<ul style="list-style-type: none"> Protection from DoS, port scans, malware, botnets, exploits, and vulnerabilities More than 40,000 active signatures Configurable exceptions Scans all interfaces <p>*) available for LANCOM R&S® Unified Firewall UF-200, UF-300, UF-500, and UF-900</p>
Proxies	<ul style="list-style-type: none"> HTTPS, FTP, POP3/S, SMTP/S, SIP HTTP (transparent/non-transparent) Reverse proxy Supports Active Directory and local users Time-controlled
LAN/WAN support	<ul style="list-style-type: none"> Ethernet 10/100/1,000/10,000 Mbps Configurable MTU (Ethernet/DSL) xDSL Multi-WAN (weighted policy-based routing/failover) Load balancing Time restrictions for Internet connections Multiple, dynamic DNS support DHCP DMZ SNAT
VLAN	<ul style="list-style-type: none"> 4096 VLANs per interface 802.1q header tagging (packet-based tagged VLANs) Compatible with bridging
Bridge mode	<ul style="list-style-type: none"> Layer-2 firewall Spanning Tree (bridge ID, port costs) Unlimited number of interfaces per bridge
Monitoring & statistics	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Self-explanatory functions Overview of the entire network Overview of all active services Browser-based, platform-independent View filtering based on custom tags
QoS	<ul style="list-style-type: none"> Guaranteed QoS bandwidth configurable for Internet connections QoS with ToS flags QoS in VPN connections

LANCOM R&S® Unified Firewalls

Features	
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 Wizards for VPN and certificates 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, LZTP Port configuration
SSL	Routing mode VPN Bridge 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 Link aggregation *) available for LANCOM R&S® Unified Firewall UF-200, UF-300, UF-500, and UF-900
Warranty	
Warranty claim	3 years
Accessories	
LANCOM R&S® Unified Firewall Rack Mount	Rack Mount for LANCOM R&S® Unified Firewall UF-100, UF-200. Inclusive for UF-300, UF-500 & UF-900.
LANCOM R&S® 8x 1G RJ45 Module	Plug-in module for LANCOM R&S® Unified Firewall UF-900, 8x 1G ETH / RJ45
LANCOM R&S® 4x 1G SFP Module	Plug-in module for LANCOM R&S® Unified Firewall UF-900, 4x 1G SFP
LANCOM R&S® 4x 10G SFP+ Module	Plug-in module for LANCOM R&S® Unified Firewall UF-900, 4x 10G SFP+
Options	
LANCOM Warranty Basic Option	Option for extending the manufacturer warranty from 3 to 5 years
LANCOM Warranty Advanced Option	Option for extending the manufacturer warranty from 3 to 5 years, and advanced replacement by the next working day on hardware failure

Hardware Appliances

LANCOM R&S® Unified Firewall UF-100	item no. 55011
LANCOM R&S® Unified Firewall UF-200	item no. 55021
LANCOM R&S® Unified Firewall UF-300	item no. 55031
LANCOM R&S® Unified Firewall UF-500	item no. 55041
LANCOM R&S® Unified Firewall UF-900	item no. 55051

Virtual Appliances

LANCOM R&S® UF-200 Virtual Appliance	item no. 55022
LANCOM R&S® UF-300 Virtual Appliance	item no. 55032
LANCOM R&S® UF-500 Virtual Appliance	item no. 55042
LANCOM R&S® UF-900 Virtual Appliance	item no. 55052

Licenses

LANCOM R&S® UF-100-1Y License (1 Year)	item no. 55101
LANCOM R&S® UF-100-3Y License (3 Years)	item no. 55102
LANCOM R&S® UF-100-5Y License (5 Years)	item no. 55103
LANCOM R&S® UF-200-1Y License (1 Year)	item no. 55104
LANCOM R&S® UF-200-3Y License (3 Years)	item no. 55105
LANCOM R&S® UF-200-5Y License (5 Years)	item no. 55106
LANCOM R&S® UF-300-1Y License (1 Year)	item no. 55107
LANCOM R&S® UF-300-3Y License (3 Years)	item no. 55108
LANCOM R&S® UF-300-5Y License (5 Years)	item no. 55109
LANCOM R&S® UF-500-1Y License (1 Year)	item no. 55110
LANCOM R&S® UF-500-3Y License (3 Years)	item no. 55111
LANCOM R&S® UF-500-5Y License (5 Years)	item no. 55112
LANCOM R&S® UF-900-1Y License (1 Year) (+100)	item no. 55113
LANCOM R&S® UF-900-3Y License (3 Years) (+100)	item no. 55114
LANCOM R&S® UF-900-5Y License (5 Years) (+100)	item no. 55115