LANCOM
UNIFIED SECURITY
NETWORK. DATA. SECURED.

SecurITy
made in Germany

SECURE. **NETWORKS.**

**Trustworthy Network
Infrastructure & IT Security
Made in Germany**

LANCOM
Systems

SECURITY
MADE IN GERMANY

Since mid-2018, LANCOM and Rohde & Schwarz have cooperated closely to create a unique combination of trusted network infrastructure and IT security "Made in Germany". The new next-generation LANCOM R&S®Unified Firewalls supplement the secure and guaranteed backdoor-free connectivity from LANCOM with state-of-the-art security technologies and unified threat management – for future-proof cybersecurity solutions: Secure networks and secure data from a single source!
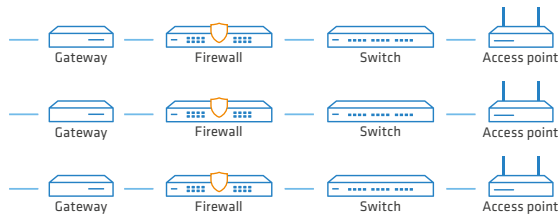

Through the integration of the Unified Firewalls into the LANCOM Management Cloud*, known as software-defined security, the entire infrastructure – consisting of connectivity and security – can then be centrally orchestrated across all LANCOM products.

*expected in the beginning of Q4/2019

NETWORK SECURITY BY DESIGN
LANCOM R&S®UNIFIED FIREWALLS

The LANCOM R&S®Unified Firewalls combine all functions of network security relevant today in one device – tailored to individual security needs. The innovative graphical user interface grants 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.
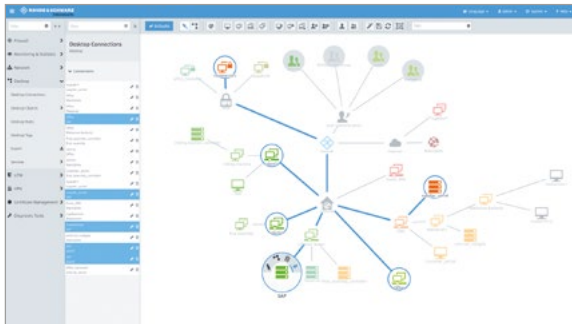
SECURITY IN-A-BOX

Modern security technologies guarantee reliable protection of networks and data against spam, viruses, and malware.

INTUITIVE NETWORK VISUALIZATION
For the easy implementation of security and compliance requirements

APPLICATION LAYER FIREWALL AND CONTROL
Layer-7 packet filter allows filtering by application (e.g. Facebook, Youtube, BitTorrent etc.) as well as the creation of blacklists or whitelists

SSL INSPECTION
Protection against complex cyber attacks by detecting malware in encrypted data streams

INTRUSION DETECTION & PREVENTION
Protection against direct attacks from outside the network

PREVENTIVE SAFETY
Reliable protection from zero-day threats by means of cloud-based sandboxing, machine learning, and Intrusion Detection & Prevention (IDS / IPS)

ANTI VIRUS
Sandboxing & machine learning in the cloud. Multi-level scanning (local and cloud-based)

IN ACTION
LANCOM R&S®UNIFIED FIREWALLS

Effective protection against malware and viruses is ensured by the firewall, which reliably detects suspicious files – in any scenario. The following examples show how to complement your new or existing network with cybersecurity.
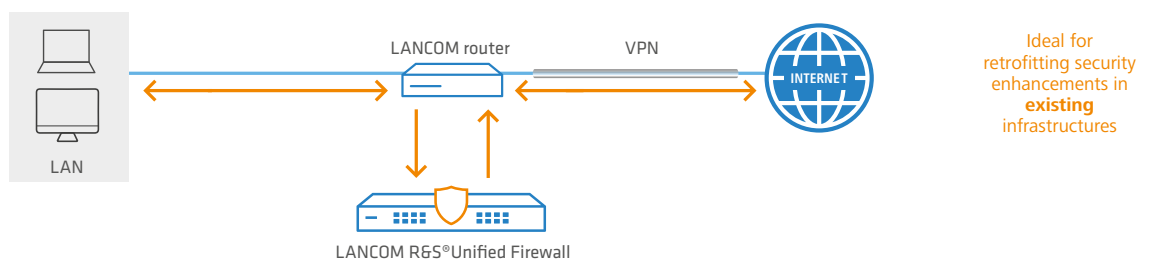
The LANCOM R&S®Unified Firewall as the link between WAN and LAN

For large corporate networks, it makes sense to position the firewall between the internal network and the LANCOM router. The advantage here is: The firewall can see and filter all of the traffic, internal and external. All of the traffic from the LAN is first passed through the firewall and then, depending on results of the inspection, directed to the router and to the Internet. Conversely, the only data to reach the internal network has been securely checked by the firewall.
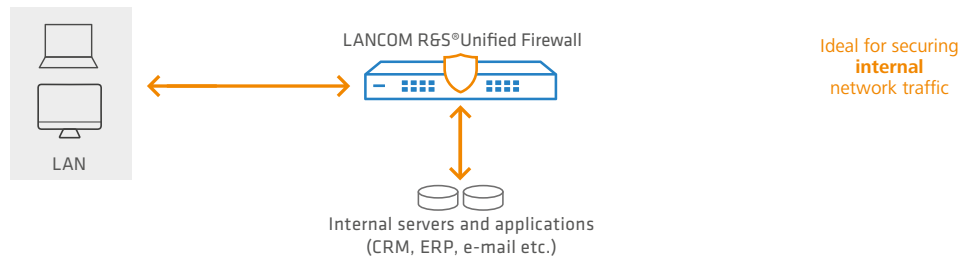

LAN — LANCOM R&S® Unified Firewall — LANCOM router — VPN — INTERNET

Ideal for implementing **new** network infrastructures
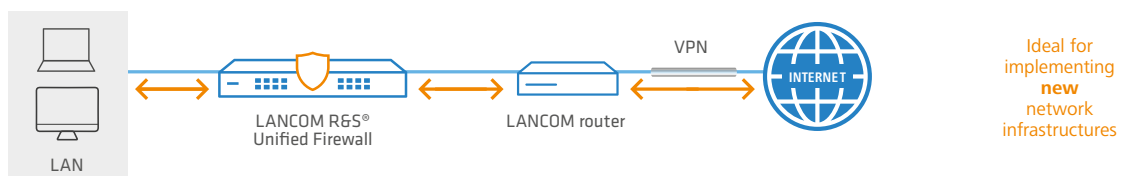
The LANCOM R&S®Unified Firewall in the „layer-3 loop"

To expand existing networks with a minimum of effort, the firewall can be conveniently integrated into the infrastructure simply by connecting it to a LANCOM router. Traffic from the internal network as well as from the Internet now completes a "loop" from the router to the firewall.

LAN — LANCOM router — VPN — INTERNET — LANCOM R&S®Unified Firewall

Ideal for retrofitting security enhancements in **existing** infrastructures

Security for your internal network

For access control for local servers and services within the LAN the LANCOM R&S®Unified Firewalls are available without activated UTM functions such as anti-malware, anti-spam, anti-virus, or IDS/IPS. Internal network traffic is controlled and forwarded rule-based by the detection of layer-7 protocols.

LANCOM R&S®Unified Firewall

LAN

Internal servers and applications
(CRM, ERP, e-mail etc.)

Ideal for securing **internal** network traffic

LANCOM R&S®Unified Firewalls – Model overview

Device	UF-50	UF-100	UF-200	UF-300	UF-500	UF-900
Network interfaces						
Ports	4x GE copper	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)	2,600 (UDP)	3,800 (UDP)	3,800 (UDP)	7,700 (UDP)	13,400 (UDP)	60,000 (UDP)
VPN throughput (Mbps)	200 (IPSec)	430 (IPSec)	430 (IPSec)	620 (IPSec)	1,260 (IPSec)	4,280 (IPSec)
Concurrent session	520,000	1,000,000	1,000,000	1,000,000	2,000,000	16,700,000
New sessions per second	8,000	11,000	11,000	13,000	33,000	130,000
Rec. number of users	1-10 concurrent users	5-30 concurrent user	5-30 concurrent users	30-100 concurrent users	100-200 concurrent users	100 concurrent users, extendable in steps of 100 to max. 500

The license models required to operate the Unified Firewalls are available for periods of 1, 3, or 5 years.

You can choose between two different license types:

> The **"Basic" licenses** enable device access and basic firewall features.

> The **"Full" licenses** supplement the "Basic" functions with the full range of UTM functions that are available for the device.

The models from UF-200 to UF-900 are also available as software appliances for the use in virtualized environments.

LANCOM
Systems