

LANCOM R&S® Unified Firewalls

Netzwerksicherheit by Design

Mit LANCOM R&S® Unified Firewalls vervollständigen Sie Ihr Netzwerk um die wichtige Eigenschaft Cybersecurity. Diese einfach zu bedienenden Komplettlösungen sind auf die individuellen Sicherheitsbedürfnisse kleiner und mittelständischer Unternehmen maßgeschneidert. Dank state-of-the-art Sicherheitstechnologien und Unified Threat Management (UTM) sorgen diese Next-Generation Firewalls für zuverlässige Cybersicherheit. Eine Besonderheit: Das innovative grafische Bedienkonzept bietet einen klaren Überblick über alle gesicherten Bereiche im Unternehmen. Bislang komplexe und zeitaufwendige Konfigurationstätigkeiten werden erheblich vereinfacht, da sich sämtliche Sicherheitsvorgaben systematisch designen und in Kraft setzen lassen.

- Intuitive Netzwerkvisualisierung für einfachste Umsetzung und Einhaltung von Sicherheits- und Compliance-Vorgaben
- Detaillierte Filterung und Kontrolle von Anwendungen und Protokollen
- Schutz vor Spam, Viren und Malware sowie komplexen Cyberangriffen
- State-of-the-art Sicherheitstechniken wie R&S®PACE2 Deep Packet Inspection
- Präventive Sicherheit vor noch nicht bekannten Bedrohungen durch integriertes Sandboxing und Machine Learning
- IT-Security "Made in Germany" und garantierte Backdoor-Freiheit
- Optional als Virtual Appliances erhältlich
- Bewährter Bezug und Support über LANCOM
- Integration in die LANCOM Management Cloud in Vorbereitung

LANCOM R&S® Unified Firewalls

Benutzerfreundlichkeit und höchste Sicherheit

Die zunehmenden Cyber Risiken führen zu höheren Anforderungen an die Unternehmenssicherheit, den Datenschutz und die Verfügbarkeit komplexer IT-Systeme. Die LANCOM R&S® Unified Firewalls sind Next-Generation Firewalls, die komplette Cybersicherheit dank Unified Threat Management (UTM) bieten. Dies umfasst auch den Einsatz modernster Cybersecurity-Technologien wie Sandboxing und maschinellem Lernen. Zusätzlich bleibt dank des Einsatzes von Clustering und redundanter Hardware die IT im Unternehmen jederzeit verfügbar.

Intuitives Web-Interface

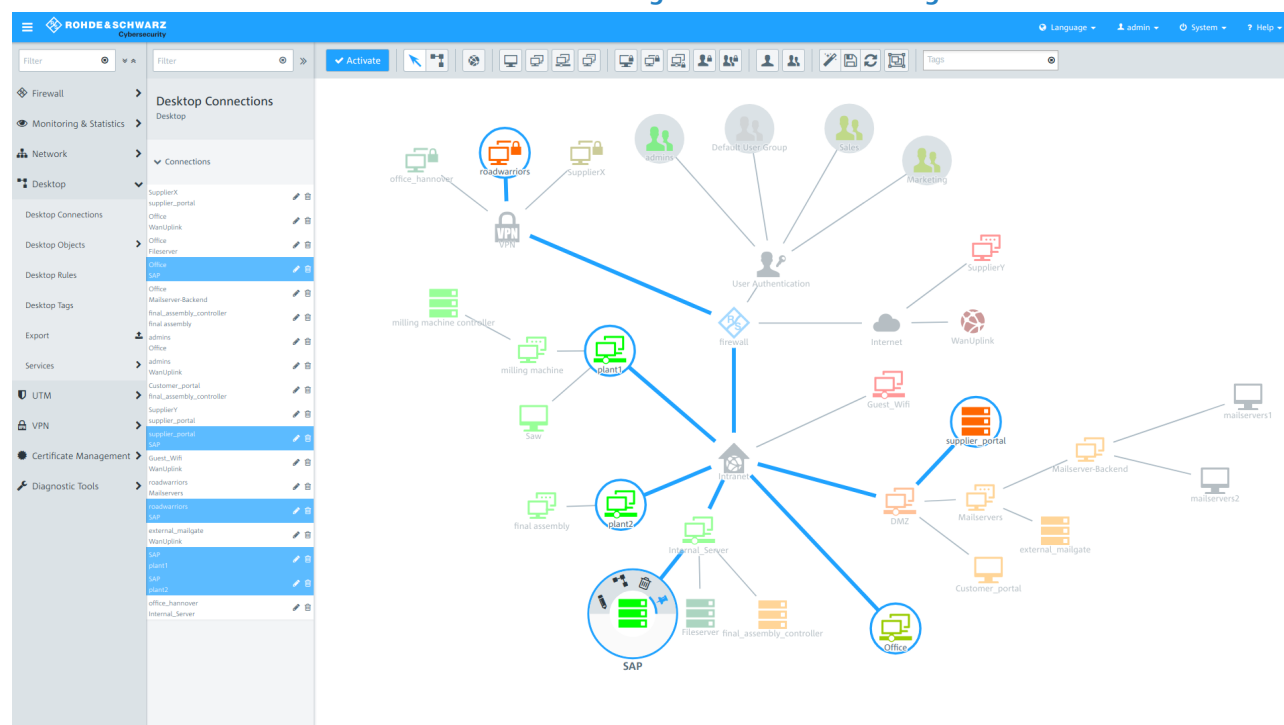
Die Benutzerfreundlichkeit des Web-Interfaces der LANCOM R&S® Unified Firewalls unterstützt den Anwender bei der Bereitstellung höchster Cybersicherheit. Menschliche Fehler bei der Konfiguration der Firewall können stark reduziert werden, da alle Firewall-Regeln des Netzwerks klar und übersichtlich grafisch dargestellt werden. Diese zentrale Managementkonsole im Browser ermöglicht sowohl eine sehr gute Feinabstimmung als auch einen umfassenden Überblick über gesicherte Geräte und Verbindungen im

Netzwerk. Dies erleichtert nicht nur die Umsetzung von Sicherheitsvorgaben, sondern verschafft auch Zeitersparnis durch einfachsten Zusammenschluss von Regeln. Dank eines schonenden Umgangs mit Ressourcen können Kosten gespart und die Produktivität gesteigert werden. Umfangreiche Audit- und Compliance-Berichte sorgen zudem für höchste Transparenz.

Cloud-basierter Schutz vor Viren und Malware

Für die effektive Abwehr von Malware und Viren bietet die Firewall verlässliche Erkennung von verdächtigen Dateien. Zum Schutz vor noch nicht bekannten Bedrohungen („Zero-Day-Exploits“) werden verdächtige Dateien in eine geschützte Cloud geladen. In dieser getrennten Umgebung werden sie sicher und zuverlässig getestet (Sandboxing). Eine Analyse mit Hilfe von maschinellem Lernen der dritten Generation, beruhend auf Milliarden von Stichproben, ermöglichen das Scannen und proaktive Blockieren auf Basis des Verhaltens. Die verwendete Cloud ist in Deutschland gehostet und entspricht den europäischen Datenschutzrichtlinien.

Screenshot des Web-Interface zum Erstellen und Management von Firewall-Regeln



LANCOM R&S® Unified Firewalls

SSL Inspection: Abwehr von komplexen Cyberangriffen über verschlüsselte Kanäle

Die zunehmende Verschlüsselung des Datenverkehrs ist unter dem Gesichtspunkt der Geheimhaltung begrüßenswert, beinhaltet jedoch auch das Risiko, dass Schadsoftware über verschlüsselte Kanäle in die Systeme eindringt. Dank SSL Inspection können auch bei verschlüsselten Datenpaketen Scans, Filterung und Anwendungserkennung zum Einsatz kommen sowie Sicherheitsvorgaben erfolgreich umgesetzt werden.

Deep Packet Inspection: detaillierte Filterung und Kontrolle von Anwendungen und Protokollen

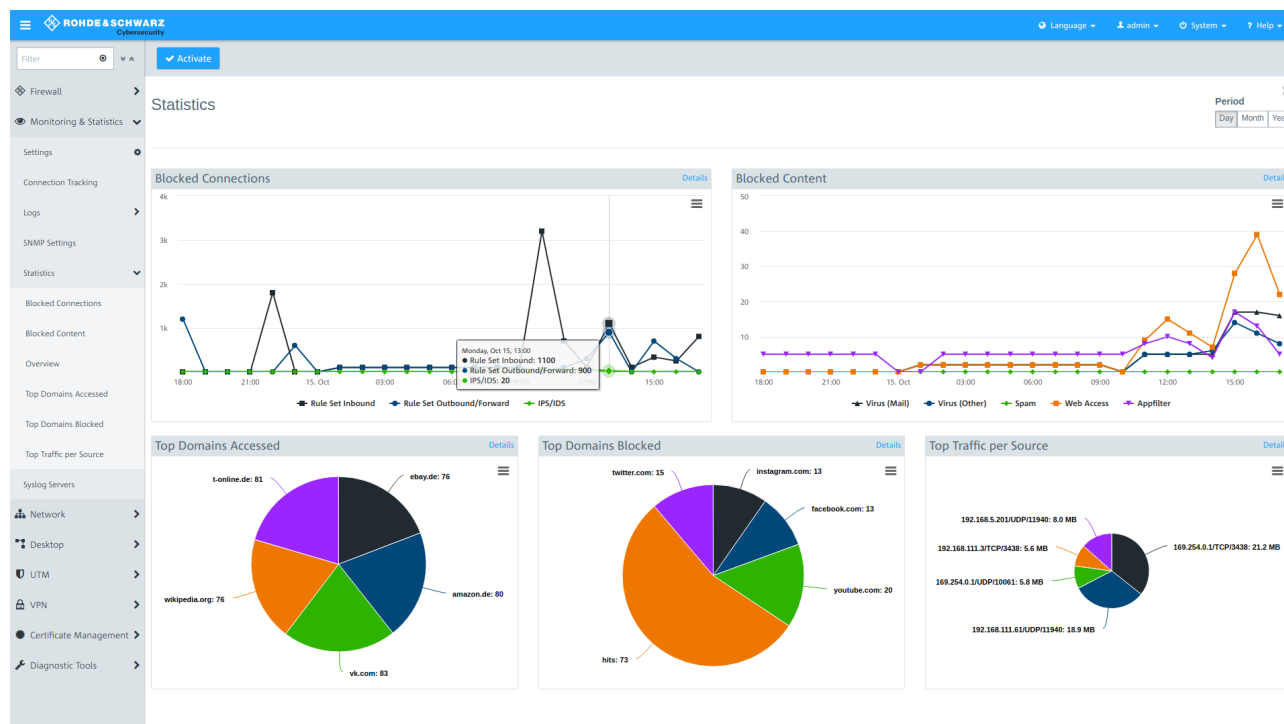
Für den Schutz vor komplexen Cyberangriffen bieten die Firewalls den Einblick in verschlüsselten Datenverkehr über Deep Packet Inspection (DPI). Dank der branchenführenden

R&S®PACE2 DPI Engine ermöglichen die UTM-Firewalls eine präzise Klassifizierung des Netzwerkverkehrs, der eingesetzten Protokolle und Anwendungen sowie Schutz vor Datenlecks und Datenverlust (Data Loss Prevention, DLP). Über feinkörnige Sicherheitsrichtlinien wird die Verwendung von bestimmten Anwendungen wie Streaming-Diensten oder Browsern aktiv geregelt.

Network & Security „Made in Germany“

LANCOM R&S® Unified Firewalls sind Next-Generation Firewalls, die in Deutschland entwickelt und programmiert werden. Durch Ihre UTM-Funktionen ergänzen sie bestehende LANCOM Netzwerkinfrastrukturen optimal um den Aspekt der IT-Security. Das bedeutet zukunftsicher Schutz für Unternehmensnetzwerke und „no Backdoors“.

Screenshot der Statistiken im Web-Interface



LANCOM R&S® Unified Firewalls

Eigenschaften Appliances					
R&S® Unified Firewalls	R&S®UF-100	R&S®UF-200	R&S®UF-300	R&S®UF-500	R&S®UF-900
Netzwerkschnittstellen					
Ports	4x GE Kupfer	4x GE Kupfer	8x GE Kupfer	14x GE Kupfer	8x GE Kupfer + 2 Module
Systemleistung					
IPS- / IDS-Durchsatz (MBit/s)	-	550	635	1.295	3.780
Firewall-Durchsatz (MBit/s)	3.800 (UDP)	3.800 (UDP)	7.700 (UDP)	13.400 (UDP)	60.000 (UDP)
VPN-Durchsatz (MBit/s)	430 (IPSec)	430 (IPSec)	620 (IPSec)	1.260 (IPSec)	4.280 (IPSec)
Gleichzeitige Sessions	1.000.000	1.000.000	1.000.000	2.000.000	16.700.000
Neue Sessions pro Sekunde	11.000	11.000	13.000	33.000	130.000
Anzahl Benutzer	5-30 gleichzeitige User	5-30 gleichzeitige User	30-100 gleichzeitige User	100-200 gleichzeitige User	100 gleichzeitige User, erweiterbar in 100er-Schritten auf max. 500
Leistung					
Eingangsspannung (V)	100-240	100-240	100-240	100-240	100-240
Leistungsaufnahme (W)	36	36	150	150	2x300
Betriebsumgebung					
Betriebstemperatur (°C)	0-40	0-40	0-40	0-40	0-40
Relative Luftfeuchtigkeit (%)	5-90	5-90	20-90	20-90	5-90
Abmessungen					
BxHxT (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

Zur Dimensionierung siehe LANCOM Techpaper Unified Firewall Sizing Guide.

Eigenschaften Virtual Appliances				
R&S® Unified Firewalls	R&S®UF-200 Virtual Appliance	R&S®UF-300 Virtual Appliance	R&S®UF-500 Virtual Appliance	R&S®UF-900 Virtual Appliance
Netzwerkschnittstellen				
Konfigurierbare Ports	4	8	14	24
Systemleistung				
Anzahl Benutzer	5-30 gleichzeitige User	30-100 gleichzeitige User	100-200 gleichzeitige User	100 gleichzeitige User, erweiterbar in 100er-Schritten auf max. 500

Zur Dimensionierung siehe LANCOM Techpaper Unified Firewall Sizing Guide. Die Performance der Virtual Appliances ist abhängig von der eingesetzten Hardware.

LANCOM R&S® Unified Firewalls

Features	
Webfilter	<ul style="list-style-type: none"> Filtern nach URL und Inhalt Anpassbare Regeln für Benutzer Blacklists / Whitelists Import / Export von URL-Listen Blockiert angegebene Dateitypen Kategoriebasiertes blockieren von Websites (individuell konfigurierbar) Online-Scan-Technologie HTTP(S)-Proxy-Unterstützung Override-Funktion
Applikationskontrolle*	<ul style="list-style-type: none"> Layer-7-Paketfilter (DPI – Deep Packet Inspection) Filtern nach Applikationen (z. B. Facebook, YouTube, BitTorrent etc.) Blacklists / Whitelists Protokollvalidierung HTTP und IEC 104 Dekodierer R&S@PACE 2 (Protocol and Application Classification Engine) *) verfügbar für UF-200, UF-300, UF-500 und UF-900
Antivirus	<ul style="list-style-type: none"> HTTP/S, FTP, POP3/S, SMTP/S Ausnahmen konfigurierbar Mehrstufiges Scan-Konzept (lokal, sowie Cloud-basiert) Sandboxing Schnelle Klassifizierung von Zero-Day-Bedrohungen durch AI-Technologien (Machine Learning)
Antispam	<ul style="list-style-type: none"> POP3/S, SMTP/S Definierbare Scanstufen GlobalView Cloud unter Verwendung von Recurrent Pattern Detection (RPD) – Spamerkennung auf Basis des Verteilungsmusters der E-Mails Blacklists / Whitelists Automatische Zurückweisung / Löschung von E-Mails
IDS (Intrusion Detection System) / IPS (Intrusion Prevention System)*	<ul style="list-style-type: none"> Schutz vor DoS (Denial of Service), Portscan, Malware, Botnets, Exploits und Schwachstellen Mehr als 40.000 aktive Signaturen konfigurierbare Ausnahmen Scanning aller Schnittstellen *) verfügbar für UF-200, UF-300, UF-500 und UF-900
Proxies	<ul style="list-style-type: none"> HTTPS, FTP, POP3/S, SMTP/S, SIP HTTP (transparent / nicht transparent) Reverse Proxy Unterstützt Active Directory und lokale Benutzer Zeitgesteuert
LAN-/WAN-Unterstützung	<ul style="list-style-type: none"> Ethernet 10 / 100 / 1.000 / 10.000 MBit/s Anpassbare MTU (Ethernet/DSL) xDSL Multi-WAN (gewichtetes richtlinienbasiertes Routing / Failover) Lastverteilung Zeitliche Einschränkungen für Internetverbindungen Unterstützung sowohl für mehrere als auch dynamische DNS-Server DHCP DMZ SNAT
VLAN	<ul style="list-style-type: none"> 4096 VLANs pro Schnittstelle 802.1q Header-Tagging (paketbasierte tagged VLANs) Kompatibel mit Bridging
Bridge-Modus	<ul style="list-style-type: none"> Layer-2-Firewall-Funktion Spanning Tree (Bridge ID, Port-Kosten) Unbegrenzte Anzahl von Schnittstellen pro Bridge
Monitoring & Statistiken	<ul style="list-style-type: none"> Statistiken (IDS / IPS, Applikationskontrolle, Surfkontrolle, Antivirus / Antispam) Protokollierung zu externen Syslog-Servern Exportieren als CSV- und XLS-Dateien SNMP/v2c und v3 Connection Tracking
Administration	<ul style="list-style-type: none"> Objektorientierte Konfiguration Rollenbasierte Administration CLI (Command-line interface) über SSH Desktop als PDF und HTML speichern IP-Basierte Zugriffbeschränkung fuer SSH und Webclient
Web-Interface	<ul style="list-style-type: none"> Selbsterklärende Funktionen Überblick über das gesamte Netzwerk Übersicht über alle aktiven Dienste Browserbasiert und plattformunabhängig Optimales Filtern der Ansicht auf Grundlage benutzerdefinierter Tags
QoS	<ul style="list-style-type: none"> Garantierte QoS-Bandbreite konfigurierbar für Internetverbindungen QoS mit ToS-Flags QoS in VPN-Verbindungen

LANCOM R&S® Unified Firewalls

Features	
X.509-Zertifikate	CRL (Certificate Revocation List) – Zertifikatsperrliste für ungültige Zertifikate OCSP (Online Certificate Status Protocol) – Netzwerkprotokoll zur Statusvalidierung von X.509-Zertifikaten Multi-CA-Unterstützung Unterstützung von Multi-Host-Zertifikaten
VPN	Benutzerauthentifizierung Hochverfügbarkeit Assistenten für VPN und Zertifikate Site-to-Site und Client-to-Site Client-Konfigurationspakete
IPSec	Volltunnel-Modus IKEv1, IKEv2 PSK (Pre-Shared Key) / Zertifikate DPD (Dead Peer Detection) NAT-T XAUTH, L2TP Portkonfiguration
SSL	Routing-Modus VPN Bridge-Modus VPN TCP / UDP Spezifikation von WINS- und DNS-Servern
Backup und Wiederherstellung	Lokaler oder Fernzugriff Automatischer Import während der Installation Automatische und zeitbasierte Backups Automatischer Upload (FTP, SCP) Disaster-Recovery via USB-Stick
Benutzerauthentifizierung	Active Directory-Import Lokale Benutzerverwaltung Authentifizierung über Web oder Client Single Sign-On (Kerberos) Mehrere Anmeldungen Captive-Portal Terminal Server Support (über Remote Desktop IP Virtualisierung)
HA (High Availability)*	Voraussetzung ist der Einsatz einer zweiten Unified Firewall desselben Typs Stateful Failover Aktiv / Passiv Hot-Standby Link Aggregation *) verfügbar für UF-200, UF-300, UF-500 und UF-900
Garantie	
Garantieanspruch	3 Jahre
Optionen	
LANCOM Warranty Basic Option	Option zur Verlängerung der Herstellergarantie von 3 auf 5 Jahre
LANCOM Warranty Advanced Option	Option zur Verlängerung der Herstellergarantie von 3 auf 5 Jahre und einen Vorabaustausch bei Hardware-Defekt

Hardware Appliances

LANCOM R&S Unified Firewall UF-100	Art.-Nr. 55011
LANCOM R&S Unified Firewall UF-200	Art.-Nr. 55021
LANCOM R&S Unified Firewall UF-300	Art.-Nr. 55031
LANCOM R&S Unified Firewall UF-500	Art.-Nr. 55041
LANCOM R&S Unified Firewall UF-900	Art.-Nr. 55051

Virtual Appliances

LANCOM R&S UF-200 Virtual Appliance	Art.-Nr. 55022
LANCOM R&S UF-300 Virtual Appliance	Art.-Nr. 55032
LANCOM R&S UF-500 Virtual Appliance	Art.-Nr. 55042
LANCOM R&S UF-900 Virtual Appliance	Art.-Nr. 55052

Lizenzen

LANCOM R&S UF-100-1Y License (1 Year)	Art.-Nr. 55101
LANCOM R&S UF-100-3Y License (3 Years)	Art.-Nr. 55102
LANCOM R&S UF-100-5Y License (5 Years)	Art.-Nr. 55103
LANCOM R&S UF-200-1Y License (1 Year)	Art.-Nr. 55104
LANCOM R&S UF-200-3Y License (3 Years)	Art.-Nr. 55105
LANCOM R&S UF-200-5Y License (5 Years)	Art.-Nr. 55106
LANCOM R&S UF-300-1Y License (1 Year)	Art.-Nr. 55107
LANCOM R&S UF-300-3Y License (3 Years)	Art.-Nr. 55108
LANCOM R&S UF-300-5Y License (5 Years)	Art.-Nr. 55109
LANCOM R&S UF-500-1Y License (1 Year)	Art.-Nr. 55110
LANCOM R&S UF-500-3Y License (3 Years)	Art.-Nr. 55111
LANCOM R&S UF-500-5Y License (5 Years)	Art.-Nr. 55112
LANCOM R&S UF-900-1Y License (1 Year) (+100)	Art.-Nr. 55113
LANCOM R&S UF-900-3Y License (3 Years) (+100)	Art.-Nr. 55114
LANCOM R&S UF-900-5Y License (5 Years) (+100)	Art.-Nr. 55115