LCOS 10.94

R&S®LANCOM 1800EFW

Secure SD-WAN über Glasfaser und Wi-Fi 6

Starke Performance für kleinere Unternehmensstandorte mit hohem Datenaufkommen: Ausgestattet mit schnellem Wi-Fi 6 bindet dieses SD-WAN Gateway mobile Endgeräte zuverlässig und parallel in den 5 GHz- und 2,4 GHz-Bändern ins Netzwerk ein. Für schnelles Internet nutzt es über den integrierten SFP-Port die Performance moderner Glasfaseranschlüsse. Größtmögliche Flexibilität bezüglich der am Standort verfügbaren Internetleitungen wird über den Gigabit Ethernet WAN-Port gewährleistet. Mit ausgezeichnetem R&S®LANCOM IPSec-VPN, WireGuard-VPN und SD-WAN werden 5 (optional 25) Standorte und mobile Mitarbeiter sicher miteinander vernetzt.

- Highspeed-Internet über Glasfaser (GPON- und AON-Module separat erhältlich) und Gigabit Ethernet
- Dual-Band Concurrent Wi-Fi 6 mit bis zu 1.200 MBit/s bei 5 GHz und bis 575 MBit/s bei 2,4 GHz
- Secure SD-WAN – zentrale Cloud-Verwaltung mit sicherer Netztrennung, automatisierter Bereitstellung und intelligenter Pfadsteuerung
- 5 integrierte VPN-Kanäle (25 optional)
- Netzvirtualisierung mit bis zu 16 Netzen auf einem Gerät (ARF)
- Erweiterter Schutz mit dem Content Filter der R&S®LANCOM Security Essentials Option

R&S®LANCOM 1800EFW

Sichere, intelligente Standortvernetzung mit Secure SD-WAN

R&S®LANCOM Secure SD-WAN ermöglicht die zentral gesteuerte und sichere Vernetzung aller Standorte. In Kombination mit der R&S®LANCOM Management Cloud (R&S®LMC) lassen sich unternehmensweite Sicherheits- und Zugriffsrichtlinien umsetzen sowie Rollouts, Konfigurationen und Updates automatisiert beschleunigen. Verschlüsselte Auto-VPNs, High Scalability & Advanced Mesh VPNs, Dynamic Path Selection sowie Active/Active-WAN mit Load Balancing sorgen für resiliente, ausfallsichere Verbindungen.

Bandbreitenstarke WAN-Anbindung über Glasfaser

Der integrierte SFP-Port ermöglicht den Anschluss an FTTH-Glasfaseranschlüsse über ein optionales Transceiver-Modul (GPON/AON). Für den Betrieb externer Provider-Modems steht ein Gigabit-Ethernet-WAN-Port zur Verfügung.

Zuverlässige Einbindung drahtloser Clients mit Wi-Fi 6

Mobile Geräte erhalten über den WLAN-Router sicheren, direkten Zugang zum Netzwerk. Für stabile WLAN-Abdeckung ohne zusätzliche Hardware unterstützt Wi-Fi 6 (IEEE 802.11ax) parallel 2,4 GHz (bis zu 575 MBit/s) und 5 GHz (bis zu 1.200 MBit/s).

Mehrschichtige Sicherheit – automatisch integriert

Ab Werk ist eine SPI-Firewall im LCOS-Betriebssystem integriert (Built-in Security). Sichere Netzwerksegmentierung erfolgt über ARF und VLAN, während PQ-PSKs vor „Store-now-decrypt-later"-Angriffen schützen und auf Quantenresistenz vorbereiten.

Verschlüsselte Kommunikation über VPN

Das Gateway ermöglicht geschützte Internetverbindungen für mobile Mitarbeitende, Home-Offices und Standorte über 5 integrierte VPN-Kanäle (IPsec und WireGuard) und ist mit der R&S®LANCOM VPN Option auf bis zu 25 Kanäle erweiterbar.

Individuell erweiterbare Sicherheit mit Content Filter

Die R&S®LANCOM Security Essentials Option erweitert den Router um einen cloudbasierten Web- und Content-Filter gegen Phishing, Ransomware und schädlichen Webseiten und ist dank unbegrenzter Nutzeranzahl optimal für wachsende Netzwerke.

R&S®LANCOM 1800EFW

WLAN-Produktspezifikation	
Frequenzband 2,4 GHz und 5 GHz	2400-2483,5 MHz (ISM), 5150-5350 MHz und 5470-5725 MHz (landesspezifische Einschränkungen möglich)
Übertragungsraten IEEE 802.11ax	▶ bis zu 1200 MBit/s nach IEEE 802.11ax mit MCS11/QAM-1024 bei 5 GHz, 2x2 MIMO und 80 MHz Kanalbreite ▶ bis zu 575 MBit/s nach IEEE 802.11ax mit MCS11/QAM-1024 bei 2,4 GHz, 2x2 MIMO und 40 MHz Kanalbreite
Übertragungsraten IEEE 802.11ac	867 MBit/s nach IEEE 802.11ac mit MCS9 (Fallback bis auf 6,5 MBit/s mit MCS0). IEEE 802.11 ac/n/a-, IEEE 802.11ac/n- oder IEEE 802.11n/a-Kompatibilitätsmodus oder reiner IEEE 802.11ac-, reiner IEEE 802.11n- oder IEEE 802.11a-Betrieb einstellbar und Datenraten separat auswählbar
Übertragungsraten IEEE 802.11n	300 MBit/s nach IEEE 802.11n mit MCS15 (Fallback bis auf 6,5 MBit/s mit MCS0). IEEE 802.11a/n-, IEEE 802.11g/n-, IEEE 802.11b/g/n- oder IEEE 802.11b/g-Kompatibilitätsmodus oder reiner IEEE 802.11n-, IEEE 802.11a-, IEEE 802.11g- oder IEEE 802.11b-Betrieb einstellbar und Datenraten separat auswählbar
Übertragungsraten IEEE 802.11a/h	54 MBit/s nach IEEE 802.11a/h (Fallback auf 48, 36 , 24, 18, 12, 9, 6 MBit/s, Automatic Rate Selection), volle Kompatibilität mit TPC (Leistungseinstellung) und DFS (automatische Kanalwahl, Radarerkennung) und Datenraten separat auswählbar
Übertragungsraten IEEE 802.11b/g	54 MBit/s nach IEEE 802.11g (Fallback auf 48, 36, 24, 18, 12, 9, 6 MBit/s, Automatic Rate Selection) kompatibel zu IEEE 802.11b (11, 5,5, 2, 1 MBit/s, Automatic Rate Selection), IEEE 802.11b/g-Kompatibilitätsmodus oder reiner IEEE 802.11g- oder reiner IEEE 802.11b-Betrieb einstellbar
Ausgangsleistung am Radiomodul, 2,4 GHz und pro chain	▶ IEEE 802.11b: +25 dBm @ 1 MBit/s, +25 dBm @ 11 MBit/s ▶ IEEE 802.11g: +25 dBm @ 6 MBit/s, +24 dBm @ 54 MBit/s ▶ IEEE 802.11n: +25 dBm @ MCS0/20 MHz, +23 dBm @ MCS7/20 MHz ▶ IEEE 802.11ac/ax: +22 dBm @ MCS9/40 MHz, +20 dBm @ MCS11/40 MHz
Ausgangsleistung am Radiomodul, 5 GHz und pro chain	▶ IEEE 802.11a: +25 dBm @ 6 MBit/s, +22 dBm @ 54 MBit/s ▶ IEEE 802.11n: +25 dBm @ MCS0/20 MHz, +22 dBm @ MCS7/20 MHz ▶ IEEE 802.11ac/ax: +19 dBm @ MCS9/80 MHz, +18 dBm @ MCS11/80 MHz
Empfangsempfindlichkeit, 2,4 GHz	▶ IEEE 802.11b: -98 dBm @ 1 MBit/s, -90 dBm @ 11 MBit/s ▶ IEEE 802.11g: -95 dBm @ 6 MBit/s, -76 dBm @ 54 MBit/s ▶ IEEE 802.11n: -94 dBm @ MCS0/20 MHz, -74 dBm @ MCS7/20 MHz ▶ IEEE 802.11ac/ax: -67 dBm @ MCS9/40 MHz, -61 dBm @ MCS11/40 MHz
Empfangsempfindlichkeit, 5 GHz	▶ IEEE 802.11a: -94 dBm @ 6 MBit/s, -75 dBm @ 54 MBit/s ▶ IEEE 802.11n: -93 dBm @ MCS0/20 MHz, -73 dBm @ MCS7/20 MHz ▶ IEEE 802.11ac/ax: -63 dBm @ MCS9/80 MHz, -57 dBm @ MCS11/80 MHz
Funkkanäle 5 GHz	Bis zu 16 nicht überlappende Kanäle (verfügbare Kanäle je nach landesspezifischer Regulierung und mit automatischer, dynamischer DFS-Kanalwahl verbunden)
Funkkanäle 2,4 GHz	Bis zu 13 Kanäle, max. 3 nicht überlappend (landesspezifische Einschränkungen möglich)
Antennenanschlüsse	Zwei Reverse SMA-Antennenanschlüsse (RP-SMA female) für externe WLAN-Antennen
Multi-SSID	Insgesamt 14 unabhängige WLAN-Netze. WLAN-Netze können zeitgesteuert aktiviert und deaktiviert werden.
Gleichzeitige WLAN Clients	Bis zu 127 Clients (empfohlen)
Unterstützte WLAN-Standards	
IEEE-Standard	IEEE 802.11ax (Wi-Fi 6), IEEE 802.11ac Wave 2 (Wi-Fi 5), IEEE 802.11n (Wi-Fi 4), IEEE 802.11a, IEEE 802.11g, IEEE 802.11b, IEEE 802.11i, IEEE 802.1X, IEEE 802.11h, IEEE 802.11d, IEEE 802.11v
Standard IEEE 802.11ax (Wi-Fi 6)	
Unterstützte Funktionen	2x2 DL-MU-MIMO, DL-OFDMA, triggered target-wake-time, BSS coloring, QAM-1024, 80 MHz-Kanäle
Standard IEEE 802.11ac (Wi-Fi 5)	
Unterstützte Funktionen	2x2 MIMO, 80 MHz-Kanäle, MU-MIMO, QAM-256

R&S®LANCOM 1800EFW

Standard IEEE 802.11n (Wi-Fi 4)	
Unterstützte Funktionen	2x2 MIMO, 40 MHz-Kanäle, 20/40 MHz Koexistenz-Mechanismus im 2,4 GHz-Band, MAC Aggregierung, Block Acknowledgement, STBC (Space Time Block Coding), LDPC (Low Density Parity Check), MRC (Maximal Ratio Combining), Kurzes Guard Interval
WLAN-Betriebsarten	
Modus	WLAN Access Point (Stand-Alone oder R&S®LANCOM Management Cloud-gesteuert)
WLAN-Sicherheit	
Sicherheitsverfahren	WPA3-Personal, IEEE 802.1X (WPA3-Enterprise, WPA2-Enterprise), IEEE 802.11i (WPA2-Personal), WPA2™, WPA, WEP, IEEE 802.11w (Protected Management Frames), LEPS-MAC (R&S®LANCOM Enhanced Passphrase Security MAC), LEPS-U (R&S®LANCOM Enhanced Passphrase Security User)
Verschlüsselungsalgorithmen	AES-CCMP, AES-GCMP, TKIP, RC4 (nur bei WEP)
EAP-Typen (Authenticator)	EAP-TLS, EAP-TTLS/MSCHAPv2, PEAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC, EAP-FAST
Radius/EAP-Server	Benutzerverwaltung von MAC-Adressen, Bandbreitenbegrenzung, Passphrase, VLAN je Benutzer, Authentisierung von IEEE 802.1X Clients mittels EAP-TLS, EAP-TTLS, EAP-MD5, EAP-GTC, PEAP, MS-CHAP, MS-CHAPv2, Dynamic Peer Discovery
Sonstiges	WLAN-Protokollfilter (ACL), IP-Redirect von empfangenen Paketen aus dem WLAN, IEEE 802.1X Supplicant, Client Detection ("Rogue WLAN-Client Detection"), Wireless Intrusion Detection System (WIDS), RADIUS CoA (Change of Authorization)
R&S®LANCOM Active Radio Control	
Client Management	Steuerung von WLAN Clients auf den sinnvollsten Access Point unter Verwendung von 802.11k und 802.11v
Band Steering	Steuerung von 5 GHz Clients auf dieses leistungsstarke Frequenzband
Managed RF Optimization*	Auswahl optimaler WLAN-Kanäle durch den Administrator
Airtime Fairness	Verbesserte Ausnutzung der WLAN-Bandbreite
Adaptive Transmission Power	Automatische Anpassung der Sendeleistung für Backup-Szenarien in WLAN-Umgebungen
***) Hinweis**	Nur im Verbund mit WLAN-Controller
Roaming	
Roaming	IAPP (Inter Access Point Protocol), IEEE 802.11r (Fast Roaming), OKC (Opportunistic Key Caching)
Layer 2-Funktionen	
VLAN	4.096 IDs nach IEEE 802.1q, dynamische Zuweisung
Multicast	IGMP-Snooping, MLD-Snooping
Protokolle	Ethernet über GRE-Tunnel (EoGRE), L2TPv3, ARP-Lookup, LLDP, DHCP Option 82, IPv6-Router-Advertisement-Snooping, DHCPv6-Snooping, LDRA (Lightweight DHCPv6 Relay Agent), Spanning Tree, Rapid Spanning Tree, ARP, Proxy ARP, BOOTP, DHCP, LACP
OAM	Ethernet Link OAM 802.3ah, IEEE 802.1ag CFM
Layer 3-Funktionen	
Firewall	Stateful Inspection Firewall mit Paketfilterung, erweitertem Port-Forwarding, N:N IP-Adressumsetzung, Paket-Tagging, Unterstützung von DNS-Zielen, unterschiedlichen Aktionen und unterschiedlichen Benachrichtigungen
Quality of Service	Traffic Shaping, Bandbreitenreservierung, DiffServ/TOS, Paketgrößensteuerung, Layer 2-in-Layer 3-Tagging, Unterstützung von 8 QoS Queues (davon 6 frei konfigurierbar)
Sicherheit	Intrusion Prevention, IP-Spoofing, Access-Control-Listen, Denial-of-Service Protection, detailliert einstellbares Verhalten bzgl. Re-Assemblierung, Session-Recovery, PING, Stealth-Mode und AUTH-Port-Behandlung, URL-Blocker, Passwortschutz, programmierbarer Reset-Taster
PPP-Authentifizierungsmechanismen	PAP, CHAP, MS-CHAP und MS-CHAPv2
Hochverfügbarkeit/Redundanz	VRRP (Virtual Router Redundancy Protocol)

R&S®LANCOM 1800EFW

Layer 3-Funktionen	
Router	IPv4-, IPv6-, IPv4/IPv6 Dual Stack
SD-WAN Application-Routing	SD-WAN Application Routing in Verbindung mit der R&S®LANCOM Management Cloud
SD-WAN Dynamic Path Selection	SD-WAN Dynamic Path Selection in Verbindung mit der R&S®LANCOM Management Cloud
SD-WAN Zero Touch Deployment	Zero Touch Inbetriebnahme des Geräts in Verbindung mit der R&S®LANCOM Management Cloud
Router-Virtualisierung	ARF (Advanced Routing und Forwarding) mit bis zu 16 Kontexten
IPv4-Dienste	HTTP- und HTTPS-Server für die Konfiguration per Webinterface, DNS-Client, DNS-Server, DNS-Relay, DNS-Proxy, Dynamic DNS-Client, DHCP-Client, DHCP-Relay und DHCP-Server mit Autodetection, NTP-Client, SNTP-Server, Policy-based Routing, Bonjour-Proxy, RADIUS
IPv6-Dienste	HTTP- und HTTPS-Server für die Konfiguration per Webinterface, DHCPv6-Client, DHCPv6-Server, DHCPv6-Relay, DNS-Client, DNS-Server, Dynamic DNS-Client, NTP-Client, SNTP-Server, Bonjour-Proxy, RADIUS
Dynamische Routing-Protokolle	RIPv2, BGPv4, OSPFv2, LISP (Locator/ID Separation Protocol)
IPv4-Protokolle	DNS, HTTP, HTTPS, ICMP, NTP/SNTP, PPPoE (Server), RADIUS, RADSEC (Secure RADIUS), RTP, SNMPv1,v2c,v3, TFTP, TACACS+, IGMPv3
IPv6-Protokolle	NDP, Stateless Address Autoconfiguration (SLAAC), Stateful Address Autoconfiguration (mit DHCPv6), Router Advertisements, ICMPv6, DHCPv6, DNS, HTTP, HTTPS, PPPoE, RADIUS, SMTP, NTP, BGP, LISP, Syslog, SNMPv1,v2c,v3, MLDv2, PIM, NPTv6 (NAT66), VRRPv3
Multicast Routing	PIM (Protocol Independent Multicast), IGMP-Proxy, MLD-Proxy
WAN-Betriebsarten	VDSL, ADSL1, ADSL2 oder ADSL2+ mit externem Modem an einem ETH-Port (auch simultan zum LAN-Betrieb)
WAN-Protokolle	PPPoE, Multi-PPPoE, GRE, PPTP (PAC oder PNS), L2TPv2 (LAC oder LNS), L2TPv3 mit Ethernet-Pseudowire und IPoE (mit oder ohne DHCP), RIP-1, RIP-2, VLAN, IPv6 over PPP (IPv6 und IPv4/IPv6 Dual Stack Session), IP(v6)oE (Autokonfiguration, DHCPv6 oder Statisch)
Tunnelprotokolle (IPv4/IPv6)	6to4, 6in4, 6rd, Dual Stack Lite, 464XLAT
Sicherheit	
Intrusion Prevention	Überwachung und Sperrung von Login-Versuchen und Portscans
IP-Spoofing	Überprüfung der Quell-IP-Adressen auf allen Interfaces: nur die IP-Adressen des zuvor definierten IP-Netzes werden akzeptiert
Access-Control-Listen	Filterung anhand von IP- oder MAC-Adresse sowie zuvor definierten Protokollen für den Konfigurationszugang
Denial-of-Service Protection	Schutz vor Fragmentierungsfehlern und SYN-Flooding
Allgemein	Detailliert einstellbares Verhalten bzgl. Re-Assemblierung, Session-Recovery, PING, Stealth-Mode und AUTH-Port-Behandlung
URL-Blocker	Filtern von unerwünschten URLs anhand von DNS-Hitlisten sowie Wildcard-Filtern. Weiterreichende Möglichkeiten durch Nutzung der Security Essentials Option
Passwortschutz	Passwortgeschützter Konfigurationszugang für jedes Interface einstellbar
Zwei-Faktor-Authentifizierung	Zwei-Faktor-Authentifizierung (2FA) für das lokale Gerätemanagement über WEBconfig, SSH und Telnet mit externer Authenticator-App
Alarmierung	Alarmierung durch E-Mail, SNMP-Traps und SYSLOG
Authentifizierungsmechanismen	PAP, CHAP, MS-CHAP und MS-CHAP v2 als PPP-Authentifizierungsmechanismen
Programmierbarer Reset-Taster	Einstellbarer Reset-Taster für "ignore", "boot-only" und "reset-or-boot"
Hochverfügbarkeit / Redundanz	
VRRP	VRRP (Virtual Router Redundancy Protocol VRRPv2 und VRRPv3) zur herstellerübergreifenden Absicherung gegen Geräte- oder Gegenstellenausfall.
FirmSafe	Für absolut sichere Software-Upgrades durch zwei speicherbare Firmware-Versionen, inkl. Testmodus bei Firmware-Updates
Load-Balancing	Statische und dynamische Lastverteilung auf bis zu 4 WAN-Strecken (Inkl. Client-Binding).

R&S®LANCOM 1800EFW

Hochverfügbarkeit / Redundanz	
VPN-Redundanz	Backup von VPN-Verbindungen über verschiedene Hierarchie-Stufen hinweg, z.B. bei Wegfall eines zentralen VPN-Konzentrators und Ausweichen auf mehrere verteilte Gegenstellen. Beliebige Anzahl an Definitionen für VPN-Gegenstellen in der Konfiguration (Tunnel-Limit gilt nur für aktive Verbindungen). Bis zu 32 alternative Gegenstellen mit jeweils eigenem Routing-Tag als Backup oder zur Lastverteilung pro VPN-Gegenstelle. Die automatische Auswahl kann der Reihe nach, aufgrund der letzten erfolgreichen Verbindung oder zufällig (VPN-Load-Balancing) erfolgen
Leitungsüberwachung	Leitungsüberwachung mit LCP Echo Monitoring, Dead Peer Detection und bis zu 4 Adressen für Ende-zu-Ende-Überwachung mit ICMP-Polling
VPN	
IPSec over HTTPS	Ermöglicht IPSec VPN durch Firewalls in Netzen, für die z. B. Port 500 für IKE gesperrt ist, auf Basis von TCP über Port 443. Geeignet für Client-to-Site und Site-to-Site-Verbindungen. IPSec over HTTPS basiert auf der NCP VPN Path Finder Technology
Anzahl der VPN-Tunnel	5 Tunnel gleichzeitig aktiv (25 mit VPN-25 Option) bei Kombination von WireGuard- oder IPSec- mit PPTP-(MPPE) und L2TPv2-Tunneln, unbegrenzte Anzahl konfigurierbarer Gegenstellen. Konfiguration aller Gegenstellen über einen einzigen Eintrag möglich bei Nutzung von RAS User Template oder Proadaptive VPN.
Hardware-Beschleuniger	Integrierter Hardwarebeschleuniger für die 3DES/AES-Ver- und -Entschlüsselung
Echtzeituhr	Integrierte, gepufferte Echtzeituhr zur Speicherung der Uhrzeit bei Stromausfällen, sodass die zeitliche Validierung der Gültigkeit von Zertifikaten immer möglich ist
Zufallszahlen-Generator	Erzeugung echter Zufallszahlen in Hardware, z. B. zur Verbesserung der Generierung von Schlüsseln für Zertifikate direkt nach dem Einschalten
1-Click-VPN Client-Assistent	Erstellung von VPN-Client-Zugängen mit gleichzeitiger Erzeugung von Profilen für den R&S®LANCOM Advanced VPN Client mit einem Klick aus LANconfig heraus
1-Click-VPN Site-to-Site	Erzeugen von VPN-Verbindungen zwischen R&S®LANCOM-Routern per "Drag and Drop" mit einem Klick in LANconfig
IKE, IKEv2	IPSec-Schlüsselaustausch über Preshared Key oder Zertifikate (RSA-Signature, ECDSA-Signature, Digital-Signature)
Smart Certificate*	Komfortable Erstellung von digitalen X.509 Zertifikaten mittels einer eigenen Zertifizierungsstelle (SCEP-CA) via Weboberfläche oder SCEP.
Zertifikate	Unterstützung von X.509 digitalen mehrstufigen Zertifikaten, kompatibel z.B. zu Microsoft Server / Enterprise Server und OpenSSL. Secure Key Storage zur Sicherung eines privaten Schlüssels (PKCS#12) gegen Diebstahl.
Zertifikatsrollout	Automatisierte Erzeugung sowie Rollout und Verlängerung von Zertifikaten mit SCEP (Simple Certificate Enrollment Protocol) pro Zertifikatshierarchie
Certificate Revocation Lists (CRL)	Abruf von CRLs mittels HTTP pro Zertifikatshierarchie
OCSP Client	Prüfen von X.509-Zertifikaten anhand von OCSP (Online Certificate Status Protocol), in Echtzeit arbeitende Alternative zu CRLs
OCSP Server/Responder*	Bereitstellen von Gültigkeits-Informationen zu mittels Smart Certificate ausgestellten Zertifikaten via OCSP
XAUTH	XAUTH-Client zur Anmeldung von R&S®LANCOM Routern und Access Points an XAUTH-Servern inkl. IKE-Config-Mode. XAUTH-Server, der die Anmeldung von Clients per XAUTH an R&S®LANCOM Routern ermöglicht. Anbindung des XAUTH-Servers an RADIUS-Server zur Authentisierung von VPN-Zugängen pro Verbindung über eine zentrale Benutzerverwaltung. Authentisierung für VPN-Client-Zugänge via XAUTH mit RADIUS-Anbindung auch mit OTP-Tokens
RAS User Template	Konfiguration aller VPN-Client-Verbindungen im IKE-Config-Mode über einen einzigen Konfigurationseintrag
Proadaptive VPN	Automatisierte Konfiguration und dynamisches Anlegen aller notwendigen VPN- und Routing-Einträge anhand eines Default-Eintrags bei Site-to-Site Verbindungen.
Algorithmen	3DES (168 Bit), AES-CBC und -GCM (128, 192 und 256 Bit), RSA (1024-4096 Bit), ECDSA (P-256-, P-384-, P-521-Kurven) und Chacha20-Poly 1305. OpenSSL-Implementierung mit FIPS-140 zertifizierten Algorithmen. MD-5, SHA-1, SHA-256, SHA-384 oder SHA-512 Hashes
Post-Quantum-Sicherheit	Post-quantum Preshared Keys (PPK) für IKEv2
NAT-Traversal	Unterstützung von NAT-Traversal (NAT-T) für den VPN-Einsatz auf Strecken, die kein VPN-Passthrough unterstützen
MOBIKE	IKEv2 VPN-Clients können nahtlos zwischen verschiedenen Netzwerken wechseln (z. B. von WLAN zu Mobilfunk), ohne den VPN-Tunnel neu aufbauen zu müssen

R&S®LANCOM 1800EFW

VPN	
WireGuard	Unterstützung von WireGuard
R&S®LANCOM Dynamic VPN	Ermöglicht den VPN-Verbindungsaufbau von oder zu dynamischen IP-Adressen. Die IP-Adresse wird verschlüsselt mittels ICMP- oder UDP-Protokoll übertragen. Dynamische Einwahl von Gegenstellen mittels Verbindungs-Template
Dynamic DNS	Ermöglicht die Registrierung der IP-Adresse bei einem Dynamic-DNS-Provider, falls keine feste IP-Adresse für den VPN-Verbindungsaufbau verwendet wird
Spezifisches DNS-Forwarding	DNS-Forwarding einstellbar pro DNS-Domäne, z.B. zur Auflösung interner Namen durch eigenen DNS-Server im VPN und Auflösung externer Namen durch Internet-DNS-Server. Eintrag für Backup-DNS pro DNS-Weiterleitung
Split-DNS	Ermöglicht für IKEv2 das selektive Weiterleiten von Datenverkehr abhängig von der angesprochenen DNS-Domäne.
IPv4 VPN	Kopplung von IPv4 Netzwerken
IPv4 VPN über IPv6 WAN	Nutzung von IPv4 VPN über IPv6 WAN-Verbindungen
IPv6 VPN	Kopplung von IPv6 Netzwerken
IPv6 VPN über IPv4 WAN	Nutzung von IPv6 VPN über IPv4 WAN-Verbindungen
RADIUS	RADIUS Authorization und Accounting, Auslagerung von VPN-Konfigurationen in externem RADIUS-Server bei IKEv2, RADIUS CoA (Change of Authorization)
High Scalability VPN (HSVPN)	Übertragung von mehreren, sicher getrennten Netzen innerhalb eines VPN-Tunnels
Advanced Mesh VPN	Dynamischer VPN-Tunnelaufbau zwischen beliebigen Filialen bei Bedarf
IKEv2-EAP*	VPN-Clients können mit IKEv2-EAP gegen eine zentrale Datenbank wie Microsoft Windows Server oder RADIUS-Server authentifiziert werden
Zwei-Faktor-Authentifizierung*	Zwei-Faktor Authentifizierung mit R&S®LANCOM Advanced VPN Client über IKEv2 EAP-OTP
***)**	Nur mit VPN-25 Option
Performance	
Routing-Performance	Daten zur Routing-Performance finden Sie im R&S®NC Techpaper "Routing-Performance" hier.
VoIP	
SIP ALG	SIP ALG (Application Layer Gateway) agiert als Proxy für SIP. Automatische Öffnung der notwendigen Ports für Sprachdaten. Automatische Adressumsetzung (STUN unnötig).
Schnittstellen	
WAN: Ethernet	10/100/1000 MBit/s Gigabit Ethernet
Ethernet Ports	4 individuelle Ports, 10/100/1000 MBit/s Gigabit Ethernet, im Auslieferungszustand als Switch geschaltet. Bis zu 3 Ports können als zusätzliche WAN-Ports geschaltet werden. Ethernet-Ports können in der LCOS-Konfiguration elektrisch deaktiviert werden. Unterstützung von Energiesparfunktionen nach IEEE 802.3az
SFP-Einschub	Steckplatz für Small Form-factor Pluggable Gigabit-Ethernet-Transceiver ("mini-GBIC"). Kompatibel mit optionalen R&S®LANCOM SFP-Modulen für Glasfaseranschlüsse über kurze Distanzen (SX) oder lange Distanzen (LX). Im Auslieferungszustand als weiterer LAN-Port geschaltet, kann als WAN-Port konfiguriert werden
Port-Konfiguration	Jeder Ethernet-Port kann frei konfiguriert werden (LAN, DMZ, WAN, Monitor-Port, Aus). LAN Ports können als Switch oder isoliert betrieben werden. Als WAN-Port können zusätzliche, externe DSL-Modems oder Netzabschlussrouter inkl. Load-Balancing und Policy-based Routing betrieben werden. DMZ-Ports können mit einem eigenen IP-Adresskreis ohne NAT versorgt werden
USB 2.0 Host-Port	USB 2.0 Hi-Speed Host-Port zum Anschluss von USB-Druckern (USB-Druck-Server), USB-Datenträgern (FAT Dateisystem); bidirektionaler Datenaustausch möglich
Serielle Schnittstelle	Serielle Konfigurationsschnittstelle / COM-Port (USB-C): 9.600-115.000 Bit/s.
Management und Monitoring	
Management	R&S®LANCOM Management Cloud, LANconfig, WEBconfig, R&S®LANCOM Layer 2 Management (Notfall-Management)

R&S®LANCOM 1800EFW

Management und Monitoring	
Management-Funktionen	Alternative Boot-Konfiguration, automatisches Software-Update über LANconfig, individuelle Zugriffs- und Funktionsrechte für bis zu 16 Administratoren, RADIUS- und RADSEC-Benutzerverwaltung, Fernwartung (über WAN oder (W)LAN, Zugangsrechte (lesen/schreiben) separat einstellbarüber) SSL, SSH, HTTPS, Telnet, TFTP, SNMP, HTTP, alternative Steuerung der Zugriffsrechte durch TACACS+, Scripting, zeitliche Steuerung aller Parameter und Aktionen durch CRON-Dienst
FirmSafe	Zwei speicherbare Firmware-Versionen im Gerät, inkl. Testmodus bei Firmware-Updates
Automatisches Firmware-Update	Konfigurierbare automatische Prüfung und Installation von Firmware-Updates
Monitoring	R&S®LANCOM Management Cloud, LANmonitor, WLANmonitor
Monitoring-Funktionen	Geräte-SYSLOG, SNMPv1,v2c,v3 inkl. SNMP-TRAPS, sehr umfangreiche LOG- und TRACE-Möglichkeiten, PING und TRACEROUTE zur Verbindungsüberprüfung, interne Loggingbuffer für SYSLOG und Firewall-Events
Monitoring-Statistiken	Umfangreiche Ethernet-, IP- und DNS-Statistiken, SYSLOG-Fehlerzähler, Accounting inkl. Export von Accounting-Informationen über LANmonitor und SYSLOG, Layer-7-Anwendungserkennung inkl. anwendungsbezogenes Erfassen des verursachten Traffics
IPerf	IPerf ermöglicht es den Datendurchsatz von IP-Netzwerken zu testen (integrierter Client und Server)
SLA-Monitor (ICMP)	Performance-Überwachung von Verbindungen
Netflow	Export von Informationen über eingehenden bzw. ausgehenden IP-Datenverkehr
SD-LAN	SD-LAN - Automatische LAN-Konfiguration über die R&S®LANCOM Management Cloud
SD-WAN	SD-WAN - Automatische WAN-Konfiguration über die R&S®LANCOM Management Cloud
Hardware	
Gewicht	450 g
Umgebung	Temperaturbereich 0–35° C; Luftfeuchtigkeit 0–95%; nicht kondensierend
Gehäuse	Robustes Kunststoffgehäuse, Anschlüsse auf der Rückseite, für Wandmontage vorbereitet, Kensington-Lock; Maße 210 x 45 x 140 mm (B x H x T)
Anzahl Lüfter	1 leiser Lüfter
Abwärme (max.)	120 BTU/h
Leistungsaufnahme (max./Idle)	30 Watt / 12 Watt
Konformitätserklärungen*	
Europa/EFTA	CE
Australien / Neuseeland	RCM
Herkunftsland	Made in Germany
***) Hinweis**	Der vollständige Text der jeweiligen Konformitätserklärung ist hier verfügbar.
Lieferumfang	
Handbuch	Quick Installation Guide (DE/EN)
Kabel	Zwei Ethernet-Kabel, 3m
Antennen	Zwei 3 dBi Dipol-WLAN-Antennen (Gewinn ist abhängig von der genutzten Frequenz.)
Netzteil	Externes Steckernetzteil (230 V), NEST 12 V/3,5 A DC, Hohlstecker 2,1/5,5 mm, Temperaturbereich 0 bis +40° C, R&S®LANCOM Art.-Nr. 112098
Support	
Gewährleistungsverlängerung	Kostenfreie Gewährleistungsverlängerung auf 3 Jahre (Austausch-Service bei Defekt) Details finden Sie hier: Link. Es finden die Service- und Supportbedingungen mit Stand vom 01.07.2026, abrufbar unter rs-nc.rohde-schwarz.com/fileadmin/pdf/LCS/ServiceSupportConditions/Rohde-Schwarz-Networks-and-Cybersecurity-GmbH-Service-und-Supportbedingungen-20260701.pdf, Anwendung.

R&S®LANCOM 1800EFW

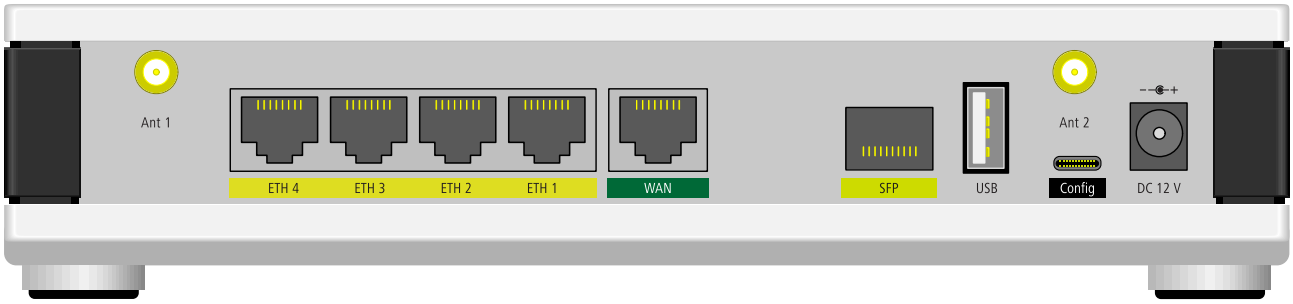
Support	
Security Updates	Bis 2 Jahre nach End of Sale des Gerätes (aber min. 3 Jahre, siehe Link), verlängerbar mit R&S®NC Support-Produkten
Software Updates	Regelmäßig kostenfreie Updates inkl. neuer Features im Rahmen des R&S®NC Lifecycle Managements (Link)
Angaben zum EU Data Act	Details zu Produktdaten und Daten verbundener Dienste finden Sie unter: Link
Hersteller-Support	Erhältlich mit R&S®NC-Produkten wie Support Access (nur für R&S®NC Community Partner), Direct oder Premium
R&S®NC Support Access	Exklusiv für R&S®NC Community Partner: Persönlicher Hersteller-Support (Best Effort) und Security Updates für das Gerät, gültig für alle Service-Kategorien, laufzeitbasiert jeweils zum Quartalsstart für 1, 3 oder 5 Jahre (Art.-Nr. 10804, 10805 oder 10806)
R&S®NC Replacement Basic S	Security Updates bis EOL (min. 5 Jahre) und 5 Jahre Austausch-Service mit Versand des Ersatzgerätes innerhalb von 5 Tagen nach Eintreffen des defekten Gerätes (8/5/5Days), Art.-Nr. 10720
R&S®NC Replacement Advanced S	Security Updates bis EOL (min. 5 Jahre) und 5 Jahre NBD-Vorabaustausch mit Lieferung des Ersatzgerätes innerhalb eines Werktages (8/5/NBD), Art.-Nr. 10730
R&S®NC Support Direct 24/7 S	Direkter, priorisierter 10/5-Hersteller-Support inkl. 24/7-Notfall-Hotline und Security Updates für das Gerät, zugesicherte Erstreaktionszeiten (SLA) von max. 30 Minuten bei telefonischer Meldung massiver Betriebsstörungen (Priorität 1) und max. 4 Stunden für alle weiteren Anliegen (Priorität 2), laufzeitbasiert für 1, 3 oder 5 Jahre(Art.-Nr. 10752, 10753 oder 10754)
R&S®NC Support Direct Advanced 24/7 S	Direkter, priorisierter 10/5-Hersteller-Support inkl. 24/7-Notfall-Hotline und Security Updates für das Gerät, NBD-Vorabaustausch mit Lieferung des Ersatzgerätes zum nächsten Werktag (24/7/NBD), zugesicherte Erstreaktionszeiten (SLA) von max. 30 Minuten bei telefonischer Meldung massiver Betriebsstörungen (Priorität 1) und max. 4 Stunden für alle weiteren Anliegen (Priorität 2), laufzeitbasiert für 1, 3 oder 5 Jahre (Art.-Nr. 10776, 10777 oder 10778)
R&S®NC Support Direct 10/5 S	Direkter, priorisierter 10/5-Hersteller-Support und Security Updates für das Gerät, zugesicherte Erstreaktionszeiten (SLA) von max. 2 Stunden bei telefonischer Meldung massiver Betriebsstörungen (Priorität 1) und max. 4 Stunden für alle weiteren Anliegen (Priorität 2), laufzeitbasiert für 1, 3 oder 5 Jahre.(Art.-Nr. 10740, 10741 oder 10742)
R&S®NC Support Direct Advanced 10/5 S	Direkter, priorisierter 10/5-Hersteller-Support und Security Updates für das Gerät, NBD-Vorabaustausch mit Lieferung des Ersatzgerätes zum nächsten Werktag (10/5/NBD), zugesicherte Erstreaktionszeiten (SLA) von max. 2 Stunden bei telefonischer Meldung massiver Betriebsstörungen (Priorität 1) und max. 4 Stunden für alle weiteren Anliegen (Priorität 2), laufzeitbasiert für 1, 3 oder 5 Jahre.(Art.-Nr. 10764, 10765 oder 10766)
Software	
Lifecycle Management	Das Gerät unterliegt nach der Abkündigung (End of Sale) dem R&S®NC Lifecycle Management. Details dazu finden Sie unter: Link
IT-Security made in Germany	Die Entwicklung und Qualitätssicherung erfolgen in Deutschland nach hohen Sicherheitsstandards. Das Vertrauenszeichen „IT-Security made in Germany" des Bundesverbands IT-Sicherheit belegt das erreichte Sicherheitsniveau.
Optionen	
VPN	R&S®LANCOM VPN-25 Option (25 Kanäle), Art.-Nr. 60083
R&S®LANCOM Security Essentials	R&S®LANCOM Security Essentials B Option 1 Jahr (für R&S®LANCOM SD-WAN Gateways der 700-, 800-, 1600-, 1700-, 1800-, IAP- und OAP-Serien sowie WLAN-Controller R&S®LANCOM WLC-60), Art.-Nr. 62168
R&S®LANCOM Security Essentials	R&S®LANCOM Security Essentials B Option 3 Jahre (für R&S®LANCOM SD-WAN Gateways der 700-, 800-, 1600-, 1700-, 1800-, IAP- und OAP-Serien sowie WLAN-Controller R&S®LANCOM WLC-60), Art.-Nr. 62169
R&S®LANCOM Security Essentials	R&S®LANCOM Security Essentials B Option 5 Jahre (für R&S®LANCOM SD-WAN Gateways der 700-, 800-, 1600-, 1700-, 1800-, IAP- und OAP-Serien sowie WLAN-Controller R&S®LANCOM WLC-60), Art.-Nr. 62170
R&S®LANCOM BPjM Filter	R&S®LANCOM BPjM Filter Option, 5 Jahre Laufzeit, Art.-Nr. 61418
R&S®LANCOM Public Spot	Hotspot-Option für R&S®LANCOM Produkte, flexible Zugangsmöglichkeiten (Voucher, E-Mail, SMS), inkl. komfortablem Einrichtungs-Assistent, sichere Trennung von Gast- und Hausnetz, Art.-Nr. 60642
R&S®LANCOM Public Spot (10er Bulk)	Hotspot-Option für R&S®LANCOM Produkte, flexible Zugangsmöglichkeiten (Voucher, E-Mail, SMS), inkl. komfortablem Einrichtungs-Assistent, sichere Trennung von Gast- und Hausnetz (10er Bulk), Art.-Nr. 61312
R&S®LANCOM All-IP Lizenz Option	Upgrade-Option zur Nutzung der R&S®LANCOM Router an All-IP-Anschlüssen, Unterstützung von TK-Anlagen und Telefoniegeräten sowie Sprach- & Faxdiensten, inkl. Voice Call Manager, Art.-Nr. 61419

R&S®LANCOM 1800EFW

Optionen	
R&S®LANCOM Public Spot PMS Accounting Plus	Erweiterung der R&S®LANCOM Public Spot (XL) Option für die Anbindung an Hotelabrechnungssysteme mit FIAS-Schnittstelle (wie Micros Fidelio) zur Authentifizierung und Abrechnung von Gastzugängen, für 178x-, 179x-, 19xx-Router, 2100EF, WLCs und aktuelle Central Site Gateways, Art.-Nr. 61638
R&S®LANCOM VoIP +10 Option	Upgrade von R&S®LANCOM VoIP-Routern für 10 zusätzliche interne VoIP-Teilnehmer (additiv bis zu 40) und 10 externe SIP-Leitungen (additiv bis zu 55), Art.-Nr. 61423
R&S®LANCOM Management Cloud	
R&S®LANCOM Management Cloud	R&S®LMC-B-1Y Lizenz (1 Jahr), ermöglicht für ein Jahr die Verwaltung eines Gerätes der Kategorie B mit der R&S®LANCOM Management Cloud, Art.-Nr. 50103
R&S®LANCOM Management Cloud	R&S®LMC-B-3Y Lizenz (3 Jahre), ermöglicht für drei Jahre die Verwaltung eines Gerätes der Kategorie B mit der R&S®LANCOM Management Cloud, Art.-Nr. 50104
R&S®LANCOM Management Cloud	R&S®LMC-B-5Y Lizenz (5 Jahre), ermöglicht für fünf Jahre die Verwaltung eines Gerätes der Kategorie B mit der R&S®LANCOM Management Cloud, Art.-Nr. 50105
Geeignetes Zubehör	
1000Base-BX20-U SFP-Modul	R&S®LANCOM SFP-AON-1, Art.-Nr.: 60200
GPON ONT SFP-Modul	R&S®LANCOM SFP-GPON-2, Kompatibel zum Betrieb an FTTH-Anschlüssen der Deutschen Telekom, Art.-Nr.: 60212
1000Base-BX20 SFP-Modul-Paar	R&S®LANCOM SFP-BiDi1550-SC1, Art.-Nr.: 60201
1000Base-SX SFP-Modul, 550 m	R&S®LANCOM SFP-SX-LC1, Art.-Nr.: 61556
1000Base-SX SFP-Modul, 550 m (10er Bulk)	R&S®LANCOM SFP-SX-LC1 (10er Bulk), Art.-Nr.: 60184
1000Base-SX SFP-Modul, 2 km	R&S®LANCOM SFP-SX2-LC1, Art.-Nr.: 60183
1000Base-LX SFP-Modul	R&S®LANCOM SFP-LX-LC1, Art.-Nr.: 61557
1000Base-LX SFP-Modul (10er Bulk)	R&S®LANCOM SFP-LX-LC1 (10er Bulk), Art.-Nr.: 60185
SFP-Kupfer-Modul 1G	R&S®LANCOM SFP-CO1, Art.-Nr.: 61494
SFP-Kupfer-Modul 1G (10er Bulk)	R&S®LANCOM SFP-CO1 (10er Bulk), Art.-Nr.: 60186
19"-Montage	19" Rackmount-Adapter, Art.-Nr. 61501
19"-Montage	19" Rack Mount Plus Adapter, Art.-Nr. 61644
R&S®LANCOM Wall Mount	Wandhalterung zur einfachen und diebstahlsicheren Befestigung von R&S®LANCOM Geräten im Kunststoffgehäuse, Art.-Nr. 61349
R&S®LANCOM Wall Mount (White)	Wandhalterung zur einfachen und diebstahlsicheren Befestigung von R&S®LANCOM Geräten im Kunststoffgehäuse, Art.-Nr. 61345
VPN-Client-Software	R&S®LANCOM Advanced VPN Client für Windows - 1er Lizenz Art.-Nr. 61600
VPN-Client-Software	R&S®LANCOM Advanced VPN Client für Windows - 10er Lizenz, Art.-Nr. 61601
VPN-Client-Software	R&S®LANCOM Advanced VPN Client für Windows - 25er Lizenz, Art.-Nr. 61602
VPN-Client-Software	R&S®LANCOM Advanced VPN Client für Mac OS X, 1er Lizenz, Art.-Nr. 61606
VPN-Client-Software	R&S®LANCOM Advanced VPN Client für Mac OS X, 10er Lizenz, Art.-Nr. 61607
***) Hinweis**	Support zu Fremdherstellerzubehör (SFP und DAC) ist ausgeschlossen und wird nicht gewährt
Artikelnummer(n)	
R&S®LANCOM 1800EFW (EU)	62139
R&S®LANCOM 1800EFW (WW)	62128

LCOS 10.94

R&S®LANCOM 1800EFW



Rohde & Schwarz Networks and Cybersecurity GmbH
Adenauerstr. 20/B2
52146 Würselen | Deutschland
info.rs-nc@rohde-schwarz.com | www.rohde-schwarz.com/networks-and-cybersecurity

R&S und Rohde & Schwarz sind Marken der Rohde & Schwarz GmbH & Co. KG, die u.a. in Deutschland, EU, USA, China und weiteren Ländern eingetragen oder benutzt werden. Andere verwendete Namen oder Bezeichnungen können (registrierte) Marken von unterschiedlichen Firmen oder Inhabern sein. Dieses Dokument enthält zukunftsbezogene Aussagen zu Produkten und Produkteigenschaft. Der Herausgeber behält sich vor, diese jederzeit ohne Angaben von Gründen zu ändern. Keine Gewähr für technische Ungenauigkeiten oder Auslassungen. 11/2026

ROHDE&SCHWARZ
Make ideas real