LCOS 10.94

R&S®LANCOM ISG-5000

Zentrale Performance für mittelgroße SD-WAN-Szenarien

Multi-Service-IP-Netzwerke benötigen auf der Zentralseite absolute Hochleistung und Zuverlässigkeit. Das Multi-Gigabit-Gateway R&S®LANCOM ISG-5000 bildet den sicheren und zukunftsfähigen Kern Ihrer VPN-Vernetzungsstrategie dank leistungsstarker Plattform mit modernsten Verschlüsselungstechnologien, High Scalability VPN und Redundanz-Funktionen. Vernetzen Sie über SD-WAN mühelos Standorte, Filialen und externe Mitarbeiter. Und bei Bedarf erweitern Sie das Gerät um weitere Funktionen wie Hotspot, Clustering oder bis zu 1.000 VPN-Kanäle.

- SD-WAN Central Site Gateway
- 100 simultanen VPN-Verbindungen (1.000 optional)
- Unterstützung von bis zu 4096 VLANs / 256 ARF-Kontexten
- SD-WAN-Unterstützung mit High Scalability VPN (HSVPN)
- 2x 10G SFP+-Ports, 6x GE-ETH-Ports, RJ45-Config-Port
- Leistungsstarkes SD-WAN für mittelgroße, standortverteilte Netzwerk-Infrastrukturen in Verbindung mit der R&S®LANCOM Management Cloud
- Optional erweiterbar um Hotspot-, Content Filter- oder Clustering-Funktionen
- Erweiterter Schutz mit dem Content Filter der R&S®LANCOM Security Essentials Option

R&S®LANCOM ISG-5000

Sichere Standortvernetzung für mittelgroße SD-WAN-Szenarien

Das R&S®LANCOM ISG-5000 ist die zentrale Instanz für Ihr leistungsstarkes SD-WAN in mittelgroßen Infrastrukturen. 100 integrierte VPN-Kanäle auf Basis modernster Verschlüsselungstechnologien und bedarfsorientierte Ports (2x 10 Gigabit SFP+, 6x Gigabit Ethernet und 2x USB) liefern Ihnen die besten Bedingungen, mobile Mitarbeiter zu vernetzen, unternehmensinterne Daten zu schützen und sensible Teilbereiche oder Filialen mit hoher IPSec-Performance sicher anzubinden. Mit der R&S®LANCOM VPN Option kann das Gateway auf bis zu 1.000 VPN-Kanäle aufgerüstet werden: Ihr Netzwerk ist so optimal skalierbar und die Infrastruktur wächst bei Bedarf mit – ohne zusätzliche Hardwarekomponenten.

Leistungsstarkes SD-WAN für ein deutlich einfacheres Management von Enterprise-Strukturen

Das R&S®LANCOM ISG-5000 bietet in Verbindung mit der R&S®LANCOM Management Cloud die perfekte Grundlage für den Aufbau eines leistungsstarken SD-WANs. Dies ermöglicht unter anderem die hochgradig automatisierte Konfiguration eines Wide Area Networks und einen automatischen Rollout der Gerätekonfigurationen auf Ihre einzelnen Standorte. Sie profitieren von höchster Skalierbarkeit, sparen Personalkosten und haben den Status Ihres Netzwerks 24/7 im Blick – ideal für mittelgroße Enterprise-Szenarien mit einer Vielzahl an Standorten.

Next-Generation SD-WAN: High Scalability VPN (HSVPN)

Das R&S®LANCOM ISG-5000 unterstützt High Scalability VPN (HSVPN). Stetig wachsende Digitalisierung, mehr Anwendungsvielfalt und höhere Datenmengen erfordern leistungsstarke und moderne Netzwerke. High Scalability VPN verbessert hierfür deutlich die Skalierbarkeit und Effizienz Ihrer Architektur. Wo zuvor für jede Anwendung ein einzelner VPN-Tunnel benötigt wurde, bündelt HSVPN beliebig viele Netze in einem einzigen VPN-Tunnel und transportiert diese gesammelt an die Gegenstelle – dabei bleibt jedes Netz sicher und strikt voneinander getrennt. Der Vorteil für Ihr Business: deutlich weniger benötigte VPN-Tunnel sowie schnellere Wiederherstellungszeiten bei Failover.

Maximale Port-Flexibilität

Von Glasfaser- über Ethernet- bis zum USB-Port: Als Kern des Netzwerkes bietet dieses Integrated Services Gateway 6 Gigabit Ethernet Ports sowie 2x USB. Darüber hinaus steigern Sie dank 2 SFP+-Ports mit 10 Gigabit die Kapazität Ihrer Datentransfers zu Servern, Netzspeichern oder Switches.

R&S®LANCOM ISG-5000

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)
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
Router-Virtualisierung	ARF (Advanced Routing und Forwarding) mit bis zu 256 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

R&S®LANCOM ISG-5000

Sicherheit	
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).
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	100 Tunnel gleichzeitig aktiv (200 in Verbindung mit der VPN-200 Option, 500 in Verbindung mit der VPN-500 Option bzw. 1000 in Verbindung mit der VPN-1000 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
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

R&S®LANCOM ISG-5000

VPN	
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
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
VoIP	
Anzahl interner VoIP-Rufnummern	10 (bis zu 40 mit VoIP +10 Option)
Anzahl gleichzeitiger VoIP-Verbindungen	bis zu 100 externe VoIP-Sprachkanäle, je nach Umkodierung, Echo-Unterdrückung und Last
Funktionen	Halten/Rückfrage, Makeln, Verbinden, Automatische Anrufweiterschaltung (CFU, CFB, CFNR), Rufnummernanzeige/-unterdrückung (CLIP, CLIR), Zweitanruf unterdrücken (Busy on Busy), spontane Amtsholung, Gruppenrufe, Rufverteilung, Overlap Dialing
Rufgruppen	Kaskadierbare Rufgruppen, Rufverteilung, gleichzeitig oder nacheinander. Abwurf nach Zeitablauf oder bei besetzt/nicht erreichbar.

R&S®LANCOM ISG-5000

VoIP	
Call-Router	Zentrale Vermittlung für ankommende und abgehenden Rufe. Rufnummernumsetzung, Ziffernersetzung und Nummernergänzung. Konfiguration der Leitungs- und Wegewahl inkl. Leitungs-Backup. Wegewahl abhängig von rufender und gewählter Rufnummer, SIP-Domäne und Leitung. Sperre von Rufnummern oder Rufnummernblöcken, Einbindung lokaler Teilnehmer in die Rufnummernkreise einer übergeordneten TK-Anlage, Ergänzung/Entfernung leitungsbezogener Präfixe und Stammnummern.
SIP-Proxy	Bis zu 25 SIP-Provider (bis zu 55 mit VoIP +10 Option), bis zu 4 übergeordnete SIP-TK-Anlagen inkl. Leitungsbackup. SIP-Verbindungen von/zu internen Teilnehmern, SIP-Providern und SIP-TK-Anlagen. Automatisches Bandbreitenmanagement und automatische Konfiguration der Firewall für SIP-Verbindungen.
SIP-Trunk	Vermittlung von Rufen auf Basis von Durchwahlen an/von VoIP-TK-Anlagen/VoIP-Provider (Unterstützung der SIP-DDI-Funktionalität gemäß ITU-T Q.1912.5). Einzige Registrierung der Stammnummer. Mapping ganzer VoIP-Rufnummernblöcke
Session Border Controller (SBC)	Trennung von unsicheren und sicheren Netzen, QoS, Management von Signalisierungs- und Sprachdaten, Transcoding
Media-Protokolle	RTP, SIPS und SRTP
SIP-Codec Unterstützung	Bei reinen SIP-Verbindungen: G.711 µ-law/A-law (64 kbit/s), G.722, G.723, G.726, G.729, iLBC, PCM (16, 20 und 24 Bit, Mono und Stereo), OPUS, AAC (LC, HE HEv2), MPEG Layer II, ADPCM 4SB. DTMF Unterstützung (Inband, RFC2833, SIP-INFO)
Autoprovisionierung	Automatische Netzwerk- und VoIP-Integration der R&S®LANCOM DECT N510/610 IP Basisstation
SIP ALG	SIP ALG (Application Layer Gateway) agiert als Proxy für SIP. Automatische Öffnung der notwendigen Ports für Sprachdaten. Automatische Adressumsetzung (STUN unnötig).
Schnittstellen	
Ethernet Ports	6 ETH-Ports (10/100/1000 MBit/s Ethernet) und zwei SFP+-Ports (10 GBit/s); bis zu 5 Ports können als zusätzliche WAN-Ports inkl. Load-Balancing geschaltet werden. Ethernet-Ports können in der LCOS-Konfiguration elektrisch deaktiviert werden. Das R&S®LANCOM GPON-SFP-1 wird im SFP+ Port bis max. 1Gbit/s unterstützt.
Port-Konfiguration	Jeder Ethernet-Port kann frei konfiguriert werden (LAN, DMZ, WAN, Monitor-Port, Aus). Als WAN-Port können zusätzliche, externe DSL-Modems oder Netzabschlussrouter inkl. Load-Balancing und Policy-based Routing betrieben werden.
USB 3.0 Host-Port	2x USB 3.0 Host-Port zum Anschluss von USB-Druckern (USB-Druck-Server), seriellen Geräten (COM-Port-Server), USB-Datenträgern (FAT Dateisystem); bidirektionaler Datenaustausch möglich
Serielle Schnittstelle	Serielle Konfigurationsschnittstelle / COM-Port (RJ-45): 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)
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

R&S®LANCOM ISG-5000

Hardware	
Gewicht	3,5 kg
Spannungsversorgung	Internes Netzteil (100–240 V, 50-60 Hz)
Umgebung	Temperaturbereich 0–40° C; Luftfeuchtigkeit 0–85%; nicht kondensierend
Gehäuse	Robustes Metallgehäuse, 19" 1 HE (440 x 44 x 269,2 mm, B x H x T) mit abschraubbaren Montagewinkeln, Netzwerkanschlüsse auf der Frontseite
Anzahl Lüfter	2
Abwärme (max.)	204 BTU/h
Leistungsaufnahme (max.)	60 Watt
Konformitätserklärungen*	
Europa/EFTA	CE
Nordamerika	FCC/IC
***) Hinweis**	Der vollständige Text der jeweiligen Konformitätserklärung ist hier verfügbar.
Lieferumfang	
Handbuch	Hardware-Schnellübersicht (DE/EN), Installation Guide (DE/EN)
Kabel	Ethernet-Kabel, 3 m
Kabel	EU-Variante: Kaltgeräte-Netzkabel
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.
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	Technischer Hersteller-Support im Rahmen eines Support-Vertrages (R&S®NC Community Partner, R&S®NC Support Direct oder R&S®NC Support 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 L	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. 10722
R&S®NC Replacement Advanced L	Security Updates bis EOL (min. 5 Jahre) und 5 Jahre NBD-Vorabaustausch mit Lieferung des Ersatzgerätes innerhalb eines Werktages (8/5/NBD), Art.-Nr. 10732
R&S®NC Support Direct 24/7 L	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. 10758, 10759 oder 10760)
R&S®NC Support Direct Advanced 24/7 L	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. 10782, 10783 oder 10784)
R&S®NC Support Direct 10/5 L	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. 10746, 10747 oder 10748)

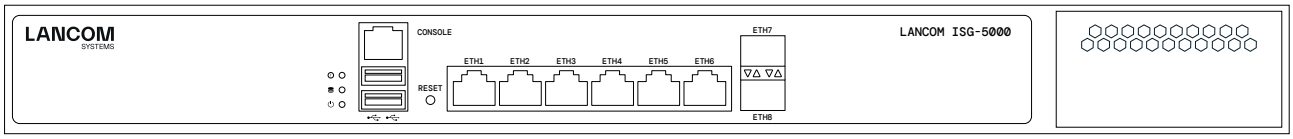
R&S®LANCOM ISG-5000

Support	
R&S®NC Support Direct Advanced 10/5 L	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. 10770, 10771 oder 10772)
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-200 Option (200 Kanäle), Art.-Nr. 61404
VPN	R&S®LANCOM VPN-500 Option (500 Kanäle), Art.-Nr. 61402
VPN	R&S®LANCOM VPN-1000 Option (1000 Kanäle), Art.-Nr. 61403
R&S®LANCOM Security Essentials	R&S®LANCOM Security Essentials D Option 1 Jahr (für R&S®LANCOM SD-WAN Central Site Gateways ISG-5000 und ISG-8000 sowie WLAN-Controller R&S®LANCOM WLC-2000), Art.-Nr. 62174
R&S®LANCOM Security Essentials	R&S®LANCOM Security Essentials D Option 3 Jahre (für R&S®LANCOM SD-WAN Central Site Gateways ISG-5000 und ISG-8000 sowie WLAN-Controller R&S®LANCOM WLC-2000), Art.-Nr. 62174
R&S®LANCOM Security Essentials	R&S®LANCOM Security Essentials D Option 5 Jahre (für R&S®LANCOM SD-WAN Central Site Gateways ISG-5000 und ISG-8000 sowie WLAN-Controller R&S®LANCOM WLC-2000), Art.-Nr. 62175
R&S®LANCOM BPjM Filter	R&S®LANCOM BPjM Filter Option, 5 Jahre Laufzeit, Art.-Nr. 61418
R&S®LANCOM Public Spot XL	Hotspot-Option für R&S®LANCOM WLC-4100, WLC-4025(+) sowie R&S®LANCOM 9100(+) VPN, R&S®LANCOM 7100(+), LANCOM ISG-1000, R&S®LANCOM ISG-4000 und R&S®LANCOM ISG-8000 zur User-Authentifizierung (empfohlen bis zu 2.500), flexible Zugangsmöglichkeiten (Voucher, E-Mail, SMS), inkl. komfortablem Einrichtungs-Assistent, Art.-Nr. 61624
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 VPN High Availability Clustering XL Option	Komfortable Verwaltung von hochverfügbaren Geräte-Clustern wie ein einzelnes Gerät – auch bei standortübergreifenden Netzwerken, Art.-Nr. 61637
***) Hinweis**	Weitere Details zu R&S®LANCOM Service Packs sind unter der folgenden Internetadresse verfügbar: Link
R&S®LANCOM Management Cloud	
R&S®LANCOM Management Cloud	R&S®LMC-D-1Y Lizenz (1 Jahr), ermöglicht für ein Jahr die Verwaltung eines Gerätes der Kategorie D mit der R&S®LANCOM Management Cloud, Art.-Nr. 50109
R&S®LANCOM Management Cloud	R&S®LMC-D-3Y Lizenz (3 Jahre), ermöglicht für drei Jahre die Verwaltung eines Gerätes der Kategorie D mit der R&S®LANCOM Management Cloud, Art.-Nr. 50110
R&S®LANCOM Management Cloud	R&S®LMC-D-5Y Lizenz (5 Jahre), ermöglicht für fünf Jahre die Verwaltung eines Gerätes der Kategorie D mit der R&S®LANCOM Management Cloud, Art.-Nr. 50111
Geeignetes Zubehör	
1000Base-BX20-U SFP-Modul	R&S®LANCOM SFP-AON-1, Art.-Nr.: 60200
10GBASE-BX20-U SFP-Modul	R&S®LANCOM SFP-AON-10, Art.-Nr.: 60211
GPON ONT SFP-Modul	R&S®LANCOM SFP-GPON-2, Kompatibel zum Betrieb an FTTH-Anschlüssen der Deutschen Telekom, Art.-Nr.: 60212

LCOS 10.94

R&S®LANCOM ISG-5000

Geeignetes Zubehör	
XGS-PON ONT SFP-Modul	R&S®LANCOM SFP-XGSPON-1, Kompatibel zum Betrieb an FTTH-Anschlüssen der Deutschen Telekom, Art.-Nr.: 60207
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
10GBASE-SR/SW SFP-Modul	R&S®LANCOM SFP-SX-LC10, Art.-Nr.: 61485
10GBASE-LR/LW SFP-Modul	R&S®LANCOM SFP-LX-LC10, Art.-Nr.: 61497
10GBASE-ER SFP-Modul	R&S®LANCOM SFP-LR40-LC10, Art.-Nr.: 60182
Direct Attach Kabel	R&S®LANCOM SFP-DAC10-1m, Art.-Nr.: 61495
Direct Attach Kabel	R&S®LANCOM SFP-DAC10-3m, Art.-Nr.: 60175
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
RJ45/USB Serial Adapter	R&S®LANCOM RJ45/USB Serial Adapter, Art.-Nr.: 61659
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 ISG-5000 (EU)	61079



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