Lancom R&S Unified Firewall UF-160 4 Anschlüsse 1GbE

Artikelnummer	999931114
Gewicht	1kg
Länge	1mm
Breite	1mm
Höhe	1mm

Produktbeschreibung

Die LANCOM R&S Unified Firewalls bieten hohe Netzwerksicherheit durch Unified Threat Management (UTM). Mit einem intuitiven grafischen Web-Interface überzeugen sie durch disruptive Usability und minimieren so mögliche Fehlerquellen bei der Firewall-Konfiguration. Zudem werden mit dem \"One-Click Security\"-Konzept der LANCOM Management Cloud passgenaue Sicherheitsarchitekturen mit Firewalls an verteilten Standorten automatisiert umgesetzt. Die in Deutschland entwickelten Next-Generation UTM-Firewalls stehen für vertrauenswürdige Unternehmensnetzwerke und garantierte Backdoor-Freiheit.

- **Top Usability durch intuitives Web-Interface und praktischen Setup-Wizards**
  Das Web-Interface der LANCOM R&S Unified Firewalls besticht durch disruptive Usability. Menschliche Fehler bei der Konfiguration der Firewall werden stark reduziert, 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. Umfangreiche Audit- und Compliance-Berichte sorgen zudem für höchste Transparenz.
- **Cloud-managed Security & SD-Branch**
  Maximieren Sie Ihren Schutz und minimieren Sie gleichzeitig Ihre Aufwände mit LANCOM Cloud-managed Security: Die LANCOM Management Cloud (LMC) übernimmt die manuelle Firewall-Konfiguration sowie die automatische Einrichtung von VPN-Verbindungen zwischen allen Standorten (Auto-VPN). Konfigurationen des Content Filters, der Anti-Virus-Funktion, der SSL Inspection und des Application Managements werden zentral und mit wenigen Klicks vorgenommen und automatisiert auf alle gewünschten Standorte angewendet. Auch die Integration der Firewalls erfolgt mit wenigen Klicks: Ein einfacher und zugleich sicherer Pairing-Prozess via PIN oder Aktivierungscode verbindet die Geräte mit der LANCOM Management Cloud.
- **Sandboxing und Machine Learning: zuverlässiger Schutz vor unbekannter Malware**
  Für die effektive Abwehr von Malware und Viren bieten die Firewalls 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 (Machine Learning), beruhend auf Milliarden von Stichproben, ermöglicht das Scannen und proaktive Blockieren auf Basis des Verhaltens. Die verwendete Cloud ist in Deutschland gehostet und entspricht den europäischen Datenschutzrichtlinien.
- **IDS / IPS: zuverlässiger Schutz vor bekannten Bedrohungen**
  Das in die UTM-Firewalls integrierte Intrusion Detection / Prevention System (\"IDS/IPS\") pflegt eine Datenbank bekannter Bedrohungen. Damit schützt sie die Endgeräte im Netzwerk vor einem breiten Spektrum von feindlichen Angriffen, gibt Warnmeldungen aus und beendet die Kommunikationsverbindung zu feindlichen Quellen. In der Bedrohungsdatenbank sind eine Blacklist mit IP-Adressen sowie Muster zur Erkennung von Malware in Kommunikationsverbindungen, für Netzwerk-Scans, für Brute-Force-Angriffe und mehr enthalten. Das IDS-/IPS-System generiert im IDS-Modus lediglich Warnmeldungen bei Zutreffen einer Regel auf den Datenverkehr. Zusätzlich dazu blockiert das System im IPS-Modus bösartigen Datenverkehr und verhindert durch \"Virtual Patching\" das Ausnutzen bekannter Lücken und Schwachstellen. Bei einem \"falschen Alarm\" kann der Admin den entsprechenden Datenverkehr erlauben.
- **Secure Web Gateway mittels HTTP(S)-Proxy: Filterung des Netzwerkverkehrs**
  Als Secure Web Gateways (SWG) wehren die Firewalls effektiv Angriffe aus dem Internet ab. Dabei dient ihr HTTP(S)-Proxy als Mittelsmann zur Filterung und Analyse von Netzwerkverkehr bis auf Anwendungsebene. Bei Websitezugriffen stellt der Proxy eine Verbindung zum Webserver her, generiert mithilfe seiner eigenen HTTP(S)-Proxy-CA ein Pseudo-Zertifikat für die Website und verwendet dieses, um eine Verbindung zum Browser herzustellen. So kann die UTM-Firewall als \"Secure Web Gateway\" mittels Proxy den Datenverkehr analysieren, URL- und Content Filter anwenden und nach Viren suchen.
- **Application Management und Content Filter: DPI-basierte Kontrolle über zugelassene Anwendungen und Inhalte**
  Die branchenführende R&S PACE2 DPI Engine ermöglicht den UTM-Firewalls über Deep Packet Inspection (DPI) eine präzise Klassifizierung des Netzwerkverkehrs auf Anwendungsebene. Dies ermöglicht Ihnen mithilfe des Application Managements selbst zu entscheiden, welche Anwendungen in Ihrem Netzwerk erlaubt oder blockiert werden sollen. Zur Steigerung der Netzwerk-Performance können vertrauenswürdige Anwendungen ebenfalls durch sogenannte Local Breakouts direkt ins Internet oder zu einer externen Gegenstelle umgeleitet werden. Über den Content Filter haben Sie außerdem die Möglichkeit, kategorienbasierte Filterregeln für z. B. kriminelle, pornografische oder gewalttätige Inhalte festzulegen. Damit wird Ihre Geschäftsintegrität zuverlässig geschützt.
- **SSL Inspection: Sicherheit auch bei verschlüsselten Kanälen**
  Mit der zunehmenden Verschlüsselung des Datenverkehrs nimmt auch das Risiko für eindringende Schadsoftware in die Systeme zu. Abhilfe schafft hier eine SSL Inspection mit Scans, Filterung und Anwendungserkennung auch bei verschlüsselten Datenpaketen sowie der erfolgreichen Umsetzung von Sicherheitsvorgaben.

Produkteigenschaften

Netzwerk - Typ	Firewall
Kapazität - Kapazität	Gleichzeitige Sitzungen: 1000000
Bereitgestellte Schnittstelle - Schnittstellen	4 x 1000Base-T - RJ-45
Farbkategorie	Weiß
Leistungsaufnahme im Betrieb	40 Watt
Anz. Anschlüsse	4
Netzwerk - Anschlusstechnik	Kabelgebunden

Weitere Bilder