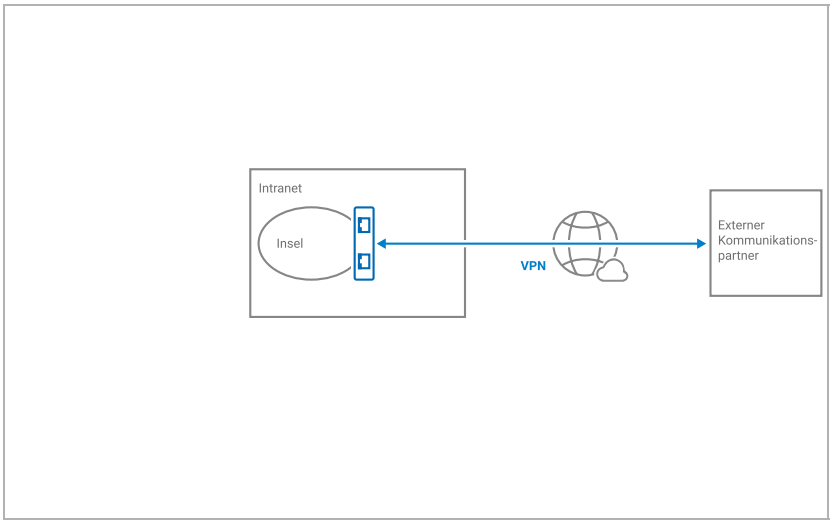
Datenblatt:

Microwall VPN



Artikel-Nr.: 55211

EUR 448,00

*Nettopreis für
gewerbliche Anwender

In den Warenkorb
Musterbestellung
Angebot anfordern
Kontakt

Firmware
Tools
Anleitung
Applikationen

Für größere Ansicht auf das Bild klicken

Sichere Kommunikation von Maschinen und Anlagen

Um eine Maschine und das umliegende Netzwerk gleichermaßen zu schützen, wird die Einheit zunächst in einem eigenen Netzwerksegment isoliert. Dieses kann einen einzelnen Computer, eine einzelne Maschine oder auch eine ganze Anlage umfassen. Die Microwall VPN routet diese Geräte-Insel sicher und einfach in das Unternehmensintranet. Einfach und intuitiv erstellbare Filterregeln schützen die sensible Insel-Kommunikation vor schädlichen Ereignissen im Intranet sowie vor unerwünschten Zugriffen. Fernwartung und Fernzugriff auf die Teilnehmer des Inselnetzes und das Management der Microwall VPN können über einen WireGuard-VPN-Tunnel sowohl als VPN-Server wie auch als VPN-Client erfolgen.

Mehr Infos: Mehr zur Funktionsweise der Microwall VPN erfahren Sie hier.

Eigenschaften | Betriebsarten | Technische Daten | Zubehör

Eigenschaften:

Schnittstellen:

- **2x Ethernet 100/1000BaseT**
  - Autosensing & Auto-MDIX
- **Hoher Datendurchsatz**
  - Gigabit-Ethernet
  - max. 900MBit/s im Router-Modus, max. 300MBit/s VPN
  - Geringe Latenzen durch leistungsfähige Hardware-Plattform

Konnektivität:

- **Betriebsart: Standard-Router**
  - Integration in das Routing-Konzept des Intranets
  - Static NAT für 1:1-Mapping von Intranet-IPs auf Insel-Hosts
- **Betriebsart: NAT-Router**
  - Integration der Insel über eine einzige Intranet-IP
- **WireGuard VPN-Server**
  - Sichere VPN-Einwahl in die Insel für Windows-, Linux-, Android-, MacOS-, IOS-Clients, Microwalls
  - Zugriffsteuerung der VPN-Clients über eigene Firewall
- **WireGuard VPN-Client**
  - VPN-Verbindung zu Ihrem Hersteller-/Service-Netzwerk
- **WireGuard VPN Box-to-Box**
  - VPN-Tunnel zwischen zwei Microwalls
  - Sichere Verbindung von Inselnetzen durch das Intra-/Internet

Management & Security:

- **Sicheres Firmware-Konzept mit Secure-Boot**
  - Kein Upload manipulierter Firmware oder Fremd-Firmware
- **Konfiguration per HTTPS-only**
  - Unterstützung individueller Zertifikate
  - Schnellinbetriebnahme per WuTility oder DHCP
  - Zwangspasswort ohne Default-Login

- **Port-Management für alle lokalen Dienste**
  - Alle Service-/Management-Dienste konfigurierbar/deaktivierbar
- **Konsequent Whitelist-basiertes Firewall-Konzept**
  - Filterregeln auf Basis von IPv4-Adressen und TCP/UDP-Portnummern
  - Eigene Firewall für eingehende VPN-Verbindungen
- **Logging**
  - Identifizierung unerwünschter Kommunikationsversuche
- **Netzwerkmanagement-Systeme**
  - Optionale Unterstützung SNMPv2c/3 (lesend)

Spannungsversorgung

- **Externe Versorgung**
  - Schraubklemmanschluss 24V-48V DC
- **Power-over-Ethernet (PoE)**

Normen & Co.:

- **Normenkonform sowohl in Büro- als auch in Industrieumgebungen:**
  - hohe Störfestigkeit für industrielles Umfeld
  - geringe Störemission für Wohn- und Geschäftsbereiche
- **5 Jahre Garantie**

Wünschen Sie sich was:
Ihre Verbesserungsvorschläge und Ergänzungen

Betriebsarten:

Die Microwall VPN lagert sensible Komponenten oder Teilnetze in ein separates Insel-Netzwerk aus und trennt dieses somit vom übergeordneten Unternehmens-Intranet. Für Fernwartungen, Remote-Support etc. steht ein WireGuard VPN-Server zur Verfügung, der ausgewählten VPN-Clients einen sicheren und über eine eigene Firewall geschützten Zugriff auf die Insel-Teilnehmer erlaubt.

Alle Verbindungen zwischen den Netzwerken müssen über Regeln auf Basis von Quell-/Ziel-IP und den verwendeten TCP/UDP-Portnummern eine ausdrückliche Freigabe erhalten. Kommunikation nicht dokumentierter und/oder unerwünschter Dienste wird unterbunden und schädliche Ereignisse wie z.B. Überlast von der Insel ferngehalten.

Filterregeln und VPN-Management

Die Firewall-Regeln und das VPN-Management werden einfach und übersichtlich über die Webseiten der Microwall VPN verwaltet und sind durchgängig Whitelist-basiert. So wird jegliche Kommunikation, die nicht ausdrücklich in Form einer Regel freigegeben ist, blockiert.

Modus NAT-Router

Ähnlich zu einem klassischen DSL-Internet-Anschluss wird das gesamte Insel-Netzwerk über nur eine IP-Adresse der Intranet-Seite in das dortige Netz eingebunden. Ein Eingriff in das Routing-Konzept des Intranets ist nicht erforderlich. Auch der Betrieb mehrerer Insel-Netzwerke mit gleichen IP-Bereichen ist in dieser Betriebsart möglich. Maschinen und Anlagen-Hersteller bietet sich hierdurch die Möglichkeit, interne Netzwerke mit einer einheitlichen Serien-IP-Konfiguration zu betreiben - aufwändige Anpassungen an die Kunden-Infrastruktur entfallen.

Modus Standard-Router

Die Microwall VPN arbeitet als klassischer Router und das Insel-Netzwerk wird z.B. in Form statischer Routen im Intranet bekannt gemacht. Per Static-NAT kann zusätzlich ein 1:1-Mapping von Intranet-Adressen auf feste IPs im Insel-Netzwerk erfolgen. Diese Insel-Hosts werden hierduch quasi zu lokalen Teilnehmern des Intranets, geniessen aber trotzdem den Schutz durch geeignete Firewall-Regeln.

WireGuard-VPN

Als VPN-Lösung für den Remote-Zugriff in das Insel-Netzwerk nutzt die Microwall VPN die WireGuard-Plattform. Gegenüber anderen VPN-Lösungen bietet diese u.a. hohen Datendurchsatz und ein einfaches Management bei einem gleichzeitig hohen Niveau an Sicherheit und Stabilität. Details und aktuelle Informationen zu WireGuard finden Sie unter https://www.wireguard.com. Die Microwall VPN kann auf ihrem Intranet-Anschluss einen VPN-Client oder VPN-Server Endpunkt zur Verfügung stellen. Je nach Anwendung können sich somit externe WireGuard-Clients in die Insel einwählen oder die Microwall verbindet sich als VPN-Client - zum Beispiel - in Ihr Service-Netzwerk.

Technische Daten:

Anschlüsse und Anzeigen

Netzwerk:	2x 100/1000BaseT Autosensing/Auto-MDIX RJ45 IPv6 auf Anfrage
Datendurchsatz:	Router-Modus (unidirektional TCP): max. 900MBit/s VPN-Tunnel (unidirektional TCP): max. 300MBit/s
Galvanische Trennung:	Netzwerkanschlüsse min. 1500 Volt
Versorgungsspannung:	Power-over-Ethernet (PoE) oder DC 24V .. 48V (+/-10%) bzw.

Versorgungsanschluss:	Steckbare Schraubklemme, 5.08mm Raster Beschriftung "L+" und "M"
Stromaufnahme:	PoE Class 2 (3,84W bis 6,49W) oder bei externer Versorgung: typ. 150mA @24V DC max. 200mA @24VDC
Anzeigen:	2x LEDs Netzwerkstatus 1x LED Error

Gehäuse und sonstige Daten

Gehäuse:	Kunststoff-Kleingehäuse für Hutschienenmontage 105x22x75mm (lxbxh)
Schutzklasse:	IP20
Gewicht:	ca. 120g
Umgebungstemperatur:	Lagerung: -40..+85°C Betrieb 0..+50°C (in nicht angereihter Montage)
Zulässige Luftfeuchtigkeit:	5..95% relative Feuchte, nicht kondensierend
Lieferumfang:	1x Microwall VPN 1x Kurzanleitung

Zubehör

*Netto Einzelpreis für gewerbliche Anwender

Netzteile

Steckernetzteil, 24V / 500mA DC mit Euro-Stecker	11021	21,00€
Steckernetzteil, 24V / 750mA DC mit Euro-, US- & UK-Stecker	11026	38,00€
Netzteil für Hutschiene, 24V / 630mA DC (Handelsware, 2 Jahre Hersteller-Garantie)	11080	33,00€

Mechanik-Zubehör

Wandgehäuse, Schutzklasse IP66 / IP67	11120	54,00€
Montagewinkel zur Wandbefestigung	58812	11,20€
19" Hutschiene	58813	21,00€

Ergänzende Netzwerk-Produkte

Ethernet Switch Industry, 4 Port	55604	218,00€

Software

WuTility	00104	kostenlos

* Unser Angebot richtet sich ausschließlich an gewerbliche Anwender. Privaten Endabnehmern nennen wir gerne Handelspartner, über die unsere Geräte bezogen werden können.

W&T
www.WuT.de

Wir sind gerne persönlich für Sie da:

Wiesemann & Theis
GmbH
Porschestr. 12
42279 Wuppertal
Tel.: 0202/2680-110 (Mo-Fr. 8-17 Uhr)
Fax: 0202/2680-265
info@wut.de

© Wiesemann & Theis GmbH, Irrtum und Änderungen vorbehalten: Da wir Fehler machen können, darf keine unserer Aussagen ungeprüft verwendet werden. Bitte melden Sie uns alle Ihnen bekannt gewordenen Irrtümer oder Missverständnisse, damit wir diese so schnell wie möglich erkennen und beseitigen können.

Datenschutz