

Datenblatt:

Microwall IO



Sichere Kommunikation von Maschinen und Anlagen

Sichere Kommunikation = sicherer Betrieb - Die Microwall IO schützt als Firewall über geeignete Regeln Ihre kritischen Maschinen oder Anlagen vor unerwünschten/schädlichen Zugriffen. Sowohl von der Insel ausgehende wie auch auf die Insel zugreifende Kommunikation wird ausschließlich auf das für den Betrieb erforderliche Maß beschränkt und die Angriffsfläche somit deutlich reduziert. Schädliche Ereignisse wie z.B. Lastspitzen, Broadcaststürme etc. bleiben lokal begrenzt und haben keine Auswirkungen auf das jeweils andere Segment.

Digitale Ein-/Ausgänge integrieren fernwartungs- und firewallspezifischen Aktionen in Automatisierungs- und Prozess-Umgebungen. Über SPS-Ausgänge oder einfache Schalter können z.B. der VPN-Zugang, bestimmte Firewallregeln oder der Status der Netzwerkschnittstellen gesteuert werden. Die Ausgänge ermöglichen die externe Visualisierung von Meldungen und Ereignissen wie z.B. einen aktivierten VPN-Zugang.

Sichere Inbetriebnahme - Im Gegensatz zu vielen anderen Routern, die ausgehenden Datenverkehr häufig ungebremst freigeben, sperrt die Microwall VPN zunächst jeglichen netzwerkübergreifenden Datenverkehr. Im Discover-Mode werden ausgehende Kommunikationsversuche der inselseitig angeschlossenen Geräte aufgezeichnet und inklusive dem zugehörigen Hostnamen des Zielservers dokumentiert. Aus erlaubten Zielen wird per Mausklick eine Freigaberegeln erzeugt, unerwünschte Kommunikation bleibt blockiert.

Sicherer Fernzugriff per VPN - Für die Fernwartung bzw. den Fernzugriff auf das Inselnetzwerk stellt die Microwall VPN einen eine Wirguard(R)-VPN-Endpunkt zur Verfügung der aktiv als VPN-Client oder passiv als VPN-Server betrieben werden kann.

Mehr Infos: Mehr zur Funktionsweise der Microwalls erfahren Sie [hier](#).

Eigenschaften

Schnittstellen:

- **2x Ethernet 100/1000BaseT**
 - Autosensing/Auto-MDIX
 - Hoher Datendurchsatz
 - max. 900MBit/s im Router-Modus, max. 300MBit/s VPN
- **2 Schalteingänge + 2 Schaltausgänge**
 - Eingänge + Ausgänge in 24V Technik
 - Ausgänge stromtreibend bis 500mA

Konnektivität:

- **2 digitale Eingänge + 2 digitale Ausgänge in 24V-Technik**
 - Eingänge steuern VPN, Firewallregeln und Netzwerk-Interfaces
 - Ausgänge melden z.B. VPN-Verbindungen
- **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
- **Discover-Mode**
 - Assistierte und sichere Inbetriebnahme neuer/unbekannter Geräte

- Aufzeichnung ausgehender Verbindungsversuche inkl. DNS-Hostnamen
- Erzeugung von Freigaberegeln per Mausklick
- **WireGuard VPN-Server & VPN-Client**
 - Sichere VPN-Einwahl in die Insel für Windows-, Linux-, Android-, MacOS-, IOS-Clients, Microwalls
 - Zugriffsteuerung der VPN-Clients über eigene Firewall
 - Optionale Steuerung des Tunnels über digitale Eingänge
 - Signalisierung des VPN-Status über digitale Ausgänge
 - Im Client-Modus VPN-Verbindung zu Ihrem Hersteller-/Service-Netzwe
- **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, Hostnamen und TCP/UDP-Portnummern
 - Regelsätze über digitale Eingänge steuerbar
 - 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 gemäß EN 61000-6-2
 - geringe Störemission gemäß EN EN 55032:2015 + A1 Kl. B, EN 61000-3-2 & EN 61000-3-3
- **5 Jahre Garantie**

♥ Wünschen Sie sich was:
[Ihre Verbesserungsvorschläge und Ergänzungen](#)

Betriebsarten

Die Microwall IO 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. Für ausgehende Verbindungen kann als Ziel innerhalb der Regel auch mit Hostnamen gearbeitet werden. Kommunikation nicht dokumentierter und/oder unerwünschter Dienste wird unterbunden und schädliche Ereignisse wie z.B. Überlast von der Insel ferngehalten.

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.

Digitale Ein-/Ausgänge für Steuerung und Meldung

Die digitalen Eingänge ermöglichen z.B. die ereignisgesteuerte Aktivierung des VPN-Zugangs oder die Umschaltung von Regelgruppen der Firewall. Auf diesem Weg kann z.B. bei Anlagen-Störungen der Bediener oder auch die Anlagen-Steuerung selbst über einen Schaltkontakt die VPN-Verbindung zum Hersteller aufbauen.

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 im Insel-Netzwerk erfolgen. Diese Insel-Hosts werden hierdurch quasi zu geniessen aber trotzdem den Schutz durch geeignete Firewall-Regeln.

Discover-Mode

Verbindungsversuche inselseitig angeschlossener Hosts werden aufgezeichnet. Ziel-Hostnamen protokolliert. Für gewünschte Verbindungen wird per Ma Unbekannte, unerwünschte oder schädliche Verbindungen bleiben blockiert.

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
Digitale Ausgänge:	2 x Digital Out 6V-30V, 500mA kurzschlussfest
Digitale Eingänge:	2 x Digital In max. Eingangsspannung +/-30V verpolungssicher innerhalb dieses Bereichs Schaltschwelle 8V +/- 1,5V "Ein"-Strom = 2,2 mA
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.
Anschlüsse:	1 x 6-fach Schraubklemme, steckbar, E/As, RM 3,5mm 1 x 2-fach Schraubklemme, steckbar, ext. Versorgung, RM 5.08mm 2 x RJ45 für Netzwerk
Stromaufnahme:	PoE Class 2 (3,84W bis 6,49W) oder bei externer Versorgung: typ. 160mA @24V DC max. 200mA @24VDC
Anzeigen:	2x LED System und Service 4x LED E/A-Status

Gehäuse und sonstige Daten

Gehäuse:	Kunststoff-Kleingehäuse für Hutschienenmontage 105x45x75mm (lxbxh)
Schutzklasse:	IP20
Gewicht:	ca. 180g
Umgebungstemperatur:	Lagerung: -40..+85°C Betrieb 0..+50°C (in nicht angereicherter Montage)
Zulässige Luftfeuchtigkeit:	5..95% relative Feuchte, nicht kondensierend
Lieferumfang:	1x Microwall IO 1x Kurzanleitung
