SIEMENS

Ingenuity for life

Digitale Schutzengel

Verstärken Sie Ihre Netzwerksicherheit mit Industrial Security Appliances SCALANCE S

siemens.de/scalance-s

… wissen, wie Ihr Netzwerk geschützt wird

Industrial Security mit Industrial Security Appliances SCALANCE S

Unternehmen müssen heute die Chancen der Digitalisierung nutzen, um auch in Zukunft erfolgreich zu sein. Die Digitalisierung verspricht niedrigere Kosten, höhere Produktionsqualität, Flexibilität und Effizienz sowie kürzere Reaktionszeiten auf Kundenwünsche und Marktanforderungen. Durch die zunehmende Digitalisierung werden immer mehr Maschinen und Anlagen miteinander vernetzt – somit sind industrielle Kommunikationsnetzwerke die Basis der Digitalisierung. Bis 2020 sollen laut Experten schon 15 Milliarden kommunikationsfähige Maschinen im industriellen Internet der Dinge vernetzt sein. Die Angriffsoberfläche wächst exponentiell und damit gehen neue Anforderungen an die Netzwerksicherheit einher, um Maschinen, Anlagen und Know-how weiterhin zu schützen. Industrial Security beruht auf einem vielschichtigen Konzept – „Defense in Depth" –, das Ihre Anlage sowohl rundum als auch in die Tiefe schützt.

- **Anlagensicherheit** beginnt mit dem klassischen Gebäudezutritt und reicht bis zur Sicherung sensibler Bereiche mittels Codekarten. Zusätzlich bietet Siemens mit den Industrial Security Services auch Risikoanalysen, die Implementierung geeigneter Maßnahmen und deren Überwachung sowie regelmäßige Updates.
- **Netzwerksicherheit** umfasst den Schutz von Automatisierungsnetzwerken gegen unbefugte Zugriffe durch Netzwerkzugangsschutz (beispielsweise mittels DMZ – demilitarisierter Zone), Netzwerksegmentierung und verschlüsselte Kommunikation. Für zuverlässigen Zellenschutz sorgen unter anderem die Industrial Security Appliances SCALANCE S.
- **Systemintegrität** schützt Ihre Automatisierungssysteme und Steuerungskomponenten vor unbefugten Zugriffen und erfüllt spezielle Anforderungen wie Know-how-Schutz. Zudem sorgt die Systemhärtung für Robustheit Ihrer Komponenten gegenüber Netzwerkangriffen.

Defense in Depth

Um Industrieanlagen umfassend vor Cyberangriffen von innen und außen zu schützen, muss auf allen Ebenen gleichzeitig angesetzt werden: von der Betriebs- bis zur Feldebene, von der Zutrittskontrolle bis zum Kopierschutz. Zu diesem Zweck nutzen wir eine tiefengestaffelte Verteidigung – „Defense in Depth" – als übergreifendes Schutzkonzept und orientieren uns dabei an den Empfehlungen der IEC 62443, dem führenden Standard für Security in der industriellen Automatisierung.

Erfahren Sie mehr: siemens.de/industrialsecurity

Industrial Security Appliances SCALANCE S

Schützen Sie Ihre industriellen Kommunikationsnetzwerke mit den Industrial Firewall und VPN Appliances

Zum Schutz vor gezielten Angriffen auf Soft- und Hardwarekomponenten von Unternehmen bietet Siemens auf industrieller Zellenebene umfangreiche Sicherheitsmaßnahmen im Cyber-Umfeld. Die Industrial Security Appliances SCALANCE S sichern Ihr Automatisierungsnetzwerk ab. Sie helfen bei der Einrichtung eines Zellenschutzkonzeptes und unterstützen das Security-Konzept „Defense in Depth". Die Security-Geräte schließen nahtlos an die Security-Strukturen der Office- und IT-Welt an. Dabei erfüllen sie die speziellen Anforderungen der Automatisierungstechnik, wie beispielsweise leichte Hochrüstbarkeit bestehender Anlagen, einfache Inbetriebnahme oder minimale Stillstandszeiten im Fehlerfall. Abhängig vom jeweiligen Sicherheitsbedürfnis können verschiedene Sicherheitsmaßnahmen miteinander kombiniert werden.

Die Entwicklung von SCALANCE S wird gemäß den Vorgaben des Industrial-Security-Standards IEC 62443-4-1 durchgeführt, was durch eine TÜV-Zertifizierung bestätigt wurde. Sie bieten ein flexibles Security-Zonenkonzept (beispielsweise Netzwerktrennung, DMZ, gesicherte Fernwartung), ermöglichen eine vielseitige Projektierung mit TIA Portal, WBM und CLI und können in die Netzwerkmanagement-Software SINEMA Server oder SINEC NMS eingebunden werden. Zudem sind sie in einem Temperaturbereich von –40 bis +70 °C einsetzbar.

Hochperformante Industrial Firewall Appliance

SCALANCE SC63x-2C

Diese hochperformante Industrial Firewall Appliance bietet Ihnen folgende Vorteile:

- **Zellenschutz via Firewall – auch benutzerspezifisch konfigurierbar – mit 600 Mbit/s und bis zu 1.000 Firewall-Regeln**
- **Bridge-Firewall zum Schutz flacher Netzwerke**
- **NAT/NAPT für die Kommunikation mit Serienmaschinen mit identischen IP-Adressen**
- **gesicherter Fernzugriff via SINEMA Remote Connect**
- **Fiber Optic für große Distanzen (bis zu 200 km)**
- **digitaler Eingang zur lokalen Aktivierung des gesicherten Fernzugriffs**
- **digitale Signalausgabe über Meldekontakt**
- **Konsolen-Port für direkten Zugriff über Programmiergerät**
- **redundante DC 24 V-Versorgung**
- **vielseitige Montagemöglichkeiten zur schnellen und zuverlässigen Befestigung**
- **kompakte Bauform mit Rückseite aus Metall**
- **einfacher Gerätetausch mittels Wechselmedium C-PLUG zur automatischen Sicherung von Konfigurations- oder Projektierungsdaten**
- **Integration in redundante Netzwerkstrukturen mittels VRRPv3 und bei SCALANCE SC636-2C zusätzlich mittels MRP**

Industrial VPN Appliance

SCALANCE S615

Diese Industrial VPN Appliance bietet Ihnen folgende Vorteile:

- Zellenschutz via Firewall – auch benutzerspezifisch konfigurierbar – mit 100 Mbit/s und bis zu 128 Firewall-Regeln
- Verwaltung von bis zu 20 VPN-Verbindungen mit einer Datenrate von bis zu 35 Mbit/s
- NAT/NAPT für die Kommunikation mit Serienmaschinen mit identischen IP-Adressen
- gesicherter Fernzugriff via SINEMA Remote Connect
- digitaler Eingang zur lokalen Aktivierung des gesicherten Fernzugriffs
- digitale Signalausgabe
- redundante DC 24 V-Versorgung
- vielseitige Montagemöglichkeiten zur schnellen und zuverlässigen Befestigung mit Montagerahmen, auch für den Einbau in 19”-Racks geeignet
- schmale Bauform, leichtes Kunststoffgehäuse
- einfacher Gerätetausch mittels Wechselmedium C-PLUG zur automatischen Sicherung von Konfigurations- oder Projektierungsdaten
- Integration in redundante Netzwerkstrukturen mittels VRRPv3

Hochperformante Industrial VPN Appliance

SCALANCE SC64x-2C

Mit dieser hochperformanten Industrial VPN Appliance profitieren Sie von folgenden Vorteilen:

- Zellenschutz via Firewall – auch benutzerspezifisch konfigurierbar – mit 600 Mbit/s und bis zu 1.000 Firewall-Regeln
- Bridge-Firewall zum Schutz flacher Netzwerke
- Verwaltung von bis zu 200 VPN-Verbindungen mit einer Datenrate von bis zu 120 Mbit/s
- NAT/NAPT für die Kommunikation mit Serienmaschinen mit identischen IP-Adressen
- gesicherter Fernzugriff via SINEMA Remote Connect
- Fiber Optic für große Distanzen (bis zu 200 km)
- digitaler Eingang zur lokalen Aktivierung des gesicherten Fernzugriffs
- digitale Signalausgabe über Meldekontakt
- Konsolen-Port für direkten Zugriff über Programmiergerät
- redundante DC 24 V-Versorgung
- vielseitige Montagemöglichkeiten zur schnellen und zuverlässigen Befestigung
- kompakte Bauform mit Rückseite aus Metall
- einfacher Gerätetausch mittels Wechselmedium C-PLUG zur automatischen Sicherung von Konfigurations- oder Projektierungsdaten
- Integration in redundante Netzwerkstrukturen mittels VRRPv3 und bei SCALANCE SC646-2C zusätzlich mittels MRP

Suchen Sie Ihren persönlichen digitalen Schutzengel aus – egal ob Industrial Firewall oder Industrial VPN Appliance: Sie gehen dabei stets auf Nummer sicher.

SCALANCE S auf einen Blick

SCALANCE	SC632-2C/SC636-2C	S615	SC642-2C/SC646-2C
Anzahl Firewall-Regeln	1.000	128	1.000
Anzahl VPN-Verbindungen	–	20	200
Firewall-Datendurchsatz	600 Mbit/s	100 Mbit/s	600 Mbit/s
IPsec-VPN-Datendurchsatz	–	35 Mbit/s	120 Mbit/s
Portausprägung elektrisch	2x RJ45/6x RJ45	5x RJ45	2x RJ45/6x RJ45
Portausprägung optisch über Combo-Ports	2x SFP	–	2x SFP
Konsolen-Port	Ja	–	Ja
SINEMA Remote Connect Lizenzfreischaltung	Integriert	Via KEY-PLUG SINEMA RC	Integriert
MRP-Client / HRP-Client	Ja – nur mit SC636-2C	Nein	Ja – nur mit SC646-2C
Bridge Firewall	Ja	Nein	Ja
VRRPv3-Kopplung	6	2	6
Benutzerspezifische Firewall	Ja	Ja	Ja

Herausgeber
Siemens AG 2019

Process Industries and Drives
Postfach 48 48
90026 Nürnberg
Deutschland

Artikel-Nr.: PDPA-B10336-01
Dispo 21507
WS 01190.0
Gedruckt in Deutschland

Securityhinweise

Siemens bietet Produkte und Lösungen mit Industrial Security-Funktionen an, die den sicheren Betrieb von Anlagen, Systemen, Maschinen und Netzwerken unterstützen.

Um Anlagen, Systeme, Maschinen und Netzwerke gegen Cyber-Bedrohungen zu sichern, ist es erforderlich, ein ganzheitliches Industrial Security-Konzept zu implementieren (und kontinuierlich aufrechtzuerhalten), das dem aktuellen Stand der Technik entspricht. Die Produkte und Lösungen von Siemens formen einen Bestandteil eines solchen Konzepts.

Die Kunden sind dafür verantwortlich, unbefugten Zugriff auf ihre Anlagen, Systeme, Maschinen und Netzwerke zu verhindern. Diese Systeme, Maschinen und Komponenten sollten nur mit dem Unternehmensnetzwerk oder dem Internet verbunden werden, wenn und soweit dies notwendig ist und nur wenn entsprechende Schutzmaßnahmen (z.B. Firewalls und/oder Netzwerksegmentierung) ergriffen wurden.

Weiterführende Informationen zu möglichen Schutzmaßnahmen im Bereich Industrial Security finden Sie unter

https://www.siemens.com/industrialsecurity

Die Produkte und Lösungen von Siemens werden ständig weiterentwickelt, um sie noch sicherer zu machen. Siemens empfiehlt ausdrücklich, Produkt-Updates anzuwenden, sobald sie zur Verfügung stehen und immer nur die aktuellen Produktversionen zu verwenden. Die Verwendung veralteter oder nicht mehr unterstützter Versionen kann das Risiko von Cyber-Bedrohungen erhöhen.

Um stets über Produkt-Updates informiert zu sein, abonnieren Sie den Siemens Industrial Security RSS Feed unter

https://www.siemens.com/industrialsecurity