SIEMENS

Ingenuity for life

Digital Guardian Angels

Strengthen your network security with Industrial Security Appliances SCALANCE S

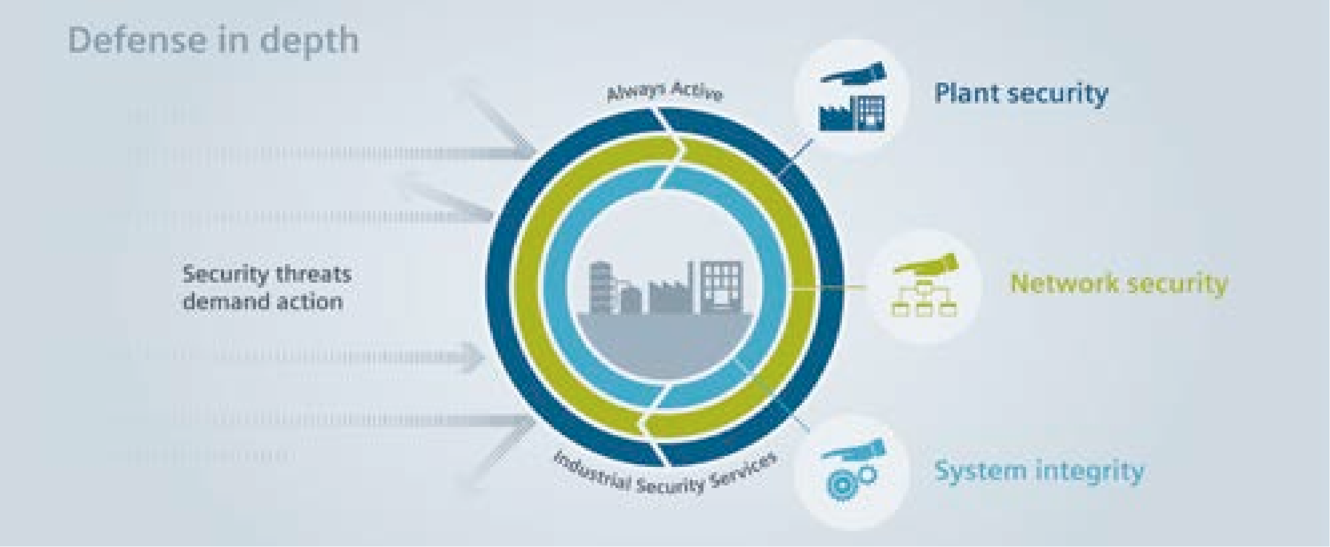
siemens.com/scalance-s

… know how your network is protected

Industrial Security with Industrial Security Appliances SCALANCE S

To remain successful into the future, companies need to seize the opportunities provided by digitalization today. Digitalization promises lower costs, improved production quality, flexibility, and efficiency. It brings a shorter response time to customer requests and market demands. Thanks to increasing digitalization, more and more machines and plants are being networked, making industrial communication networks the basis for digitalization. According to experts, 15 billion communication-capable machines will be networked in the industrial Internet of Things by 2020. This exponentially increases the attack surface and is accompanied by new network security requirements that ensure the continued protection of machines, plants, and expertise. Industrial Security is based on a multilayered concept – “defense in depth” – that gives your plant both all-round, in-depth protection.

- **Plant security** starts with conventional building access and extends to the securing of sensitive areas by means of key cards. With Industrial Security Services, Siemens also offers risk analyses, the implementation of suitable measures and their monitoring, as well as regular updates.
- **Network security** includes the protection of automation networks against unauthorized accesses with network access protection (for example, by means of a DMZ – demilitarized zone), segmentation, and encrypted communication. Reliable cell protection is ensured, for example, by SCALANCE S Industrial Security Appliances.
- **System integrity** protects your automation systems and control components against unauthorized accesses and meets special requirements such as know-how protection. It also provides system hardening to make your components robust against network attacks.



Defense in depth
To ensure comprehensive protection of industrial plants against internal and external cyber attacks, all levels must be protected simultaneously – from the plant management level to the field level and from access control to copy protection. This is why our approach to comprehensive protection offers defense throughout all levels – “defense in depth.” This concept complies with the recommendations of IEC 62443, the leading standard for security in industrial automation.

Learn more: siemens.com/industrialsecurity

SCALANCE S
Industrial Security Appliances

Protect your industrial communication networks with the industrial firewall and VPN appliances

Siemens offers comprehensive security measures in the cyber environment for protecting a company's software and hardware components against targeted attacks on the industrial cell level. The SCALANCE S Industrial Security Appliances safeguard your automation network. They help you to set up a cell protection concept and support the "defense in depth" security concept. The security appliances connect seamlessly to the security structures of the office and IT world. They meet the special automation technology requirements, such as easy upgrading of existing plants, simple commissioning, and minimal downtimes in the event of a fault. Various security measures can be combined, depending on the security requirements.

SCALANCE S development is performed according to the specifications of the IEC 62443-4-1 industrial security standard, as confirmed by TÜV (German technical inspectorate) certification. They offer a flexible security zone concept (for example network separation, DMZ, secure remote maintenance), enable versatile project planning with TIA Portal, WBM, and CLI, and can be integrated into the SINEMA Server or SINEC NMS network management software. They also can be operated in a temperature range from −40 to +70 °C.

High-performance industrial firewall appliance

SCALANCE SC63x-2C

This high-performance industrial firewall appliance offers the following benefits:

- Cell protection via firewall – also configurable on a user-specific basis – with 600 Mbit/s and up to 1,000 firewall rules
- Bridge firewall for the protection of flat networks
- NAT/NAPT for communicating with serial machines with identical IP addresses
- Secured remote access via SINEMA Remote Connect
- Fiber optics for long distances (up to 200 km)
- Digital input for local activation of secured remote access
- Digital signal output via signal contact
- Console port for direct access via programming device
- Redundant 24 V DC power supply
- Versatile installation options for fast and reliable mounting
- Compact design with metal rear panel
- Simple device replacement using C-PLUG replacement medium for automatically saving configuration and engineering data
- Integration in redundant network structures by means of VRRPv3 and, with SCALANCE SC636-2C, additionally by means of MRP

Industrial VPN appliance

SCALANCE S615

This industrial VPN appliance offers the following benefits:

- Cell protection via firewall – also configurable on a user-specific basis – with 100 Mbit/s and up to 128 firewall rules
- Administration of up to 20 VPN connections with a data rate of up to 35 Mbit/s
- NAT/NAPT for communicating with serial machines with identical IP addresses
- Secured remote access via SINEMA Remote Connect
- Digital input for local activation of secured remote access
- Digital signal output
- Redundant 24 V DC power supply
- Versatile installation options for fast and reliable mounting with mounting frame, also for installation in 19” racks
- Narrow design, light plastic housing
- Simple device replacement using C-PLUG replacement medium for automatically saving configuration and engineering data
- Integration into redundant network structures by means of VRRPv3

SCALANCE SC64x-2C

With this high-performance industrial VPN appliance, you enjoy the following benefits:

- Cell protection via firewall – also configurable on a user-specific basis – with 600 Mbit/s and up to 1,000 firewall rules
- Bridge firewall for the protection of flat networks
- Administration of up to 200 VPN connections with a data rate of up to 120 Mbit/s
- NAT/NAPT for communicating with serial machines with identical IP addresses
- Secured remote access via SINEMA Remote Connect
- Fiber optics for long distances (up to 200 km)
- Digital input for local activation of secured remote access
- Digital signal output via signal contact
- Console port for direct access via programming device
- Redundant 24 V DC power supply
- Versatile installation options for fast and reliable mounting
- Compact design with metal rear panel
- Simple device replacement using C-PLUG replacement medium for automatically saving configuration and engineering data
- Integration in redundant network structures by means of VRRPv3 and, with SCALANCE SC646-2C, additionally by means of MRP

High-performance industrial VPN appliance

You can select your personal digital guardian angel. Whether it is an industrial firewall or an industrial VPN appliance: you will always be on the safe side.

SCALANCE S at a glance

SCALANCE	SC632-2C/SC636-2C	S615	SC642-2C/SC646-2C
Number of firewall rules	1,000	128	1,000
Number of VPN connections	–	20	200
Firewall data throughput	600 Mbit/s	100 Mbit/s	600 Mbit/s
IPsec VPN data throughput	–	35 Mbit/s	120 Mbit/s
Port version, electrical	2x RJ45/6x RJ45	5x RJ45	2x RJ45/6x RJ45
Port version, optical via combo ports	2x SFP	–	2x SFP
Console port	Yes	–	Yes
SINEMA Remote Connect license key	Integrated	Via KEY-PLUG SINEMA RC	Integrated
MRP client / HRP client	Yes – only with SC636-2C	No	Yes – only with SC646-2C
Bridge firewall	Yes	No	Yes
VRRPv3 coupling	6	2	6
User-specific firewall	Yes	Yes	Yes

Published by
Siemens AG 2019

Process Industries and Drives
P.O. Box 48 48
90026 Nuremberg
Germany

Article No.: PDPA-B10336-01-7600
Dispo 21507
WS 01190.0
Printed in Germany

Subject to changes and errors. The information provided in this brochure contains descriptions or performance characteristics which, in case of actual use, do not always apply as described or which may change as a result of further development of the products. The desired performance characteristics are only binding if expressly agreed in the contract. Availability and technical specifications are subject to change without notice.

All product designations may be trademarks or product names of Siemens AG or supplier companies, the use of which by third parties for their own purposes may violate the rights of the owners.

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit

https://www.siemens.com/industrialsecurity

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under

https://www.siemens.com/industrialsecurity