STORMSHIELD

SNi50

Industrial security

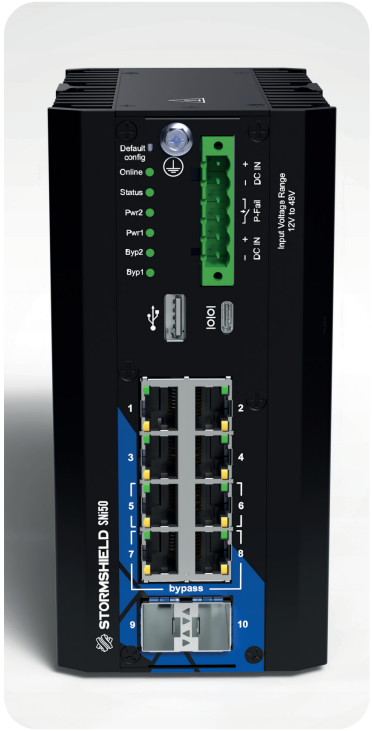
Up to 20 Gbps
FIREWALL PERFORMANCE

MTBF of 108 years
HIGH RELIABILITY

IEC 62443
FACILITATES YOUR COMPLIANCE

NETWORK SECURITY

AN INDUSTRIAL-GRADE FIREWALL



Transparent isolation of zones

Network integration capabilities provide optimal isolation between different operational zones with minimal impact on your existing infrastructure. With its IEC 62443* certification, SNi50 makes it easy to bring your operational system into compliance.

High reliability

The SNi50 product is designed to meet the high availability requirements of your industrial network. The extremely high reliability of the equipment (MTBF of 108 years) and the integrated enhanced safety mode guarantee optimal availability and security of your protection system.

Protection of extended operational networks

Combining access control for different zones with comprehensive analysis of industrial communication flows (Deep Packet Inspection) ensures you enjoy in-depth security for your extensive infrastructures. The SNi50 product safety mode ensures the continuity of your operational processes.

FOR **EUROPEAN CYBERSECURITY**

When you choose Stormshield, you gain true strategic independence and peace of mind in a highly charged geopolitical context. Completely developed in France, our firmware has received certification from leading European cybersecurity agencies such as ANSSI (France) and CCN (Spain), as well as Standard Qualification.

** Development processes are IEC62443-4-1 certified*

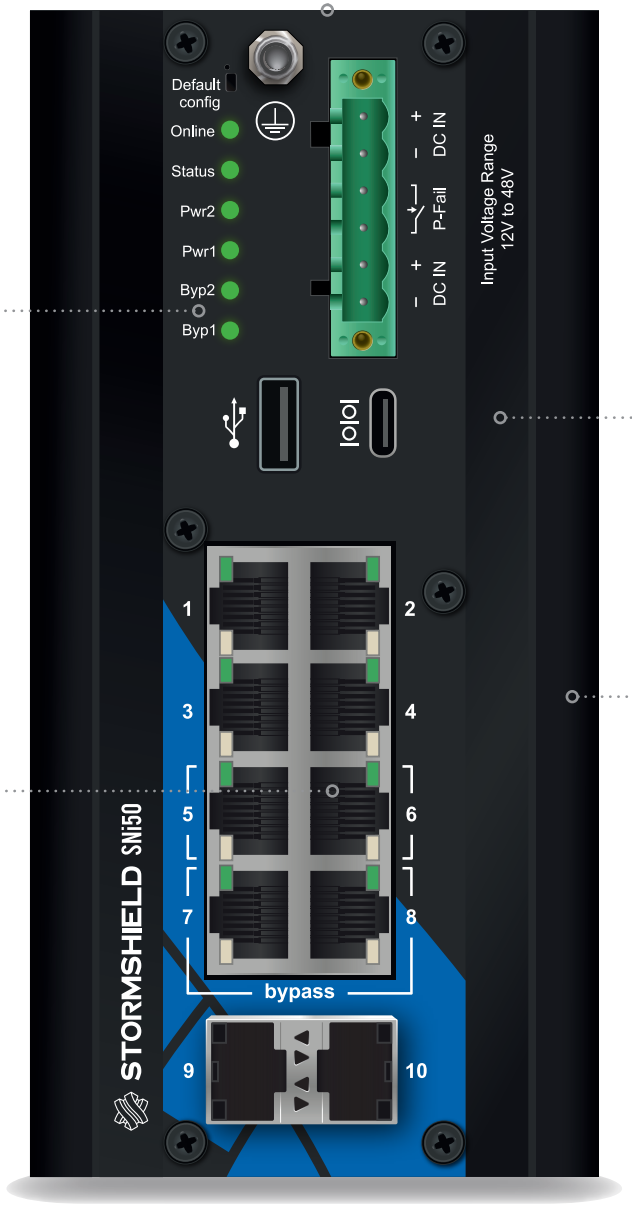
Redundant
industrial power supply

Safety mode
(bypass pairs)

Over 10 secured
industrial protocols

Rail-DIN
Easy to install in industrial cabinets

Ruggedized appliance
for constrained operating environments



ESSENTIAL DATA

Industrial SNi50

Connectivity
10
interfaces (8 copper 2.5G + 2 SFP+)

Performance
20 Gbps
Firewall

Performance
15 Gbps
IPS

2
Bypass
pairs

VPN
5.7 Gbps
IPsec throughput

VPN
750
IPsec tunnels

FEATURES

Non-contractual document. The features mentioned are for version 5.x.

Network segmentation

The various deployment modes for partitioning your operational system (router, transparent and hybrid) are among the most flexible on the market. They ensure **seamless integration of the firewall into your existing network architecture**.

Secure remote maintenance

The remote connection tool (VPN client) assists maintenance operators in obtaining **controlled, secure access to the systems to be maintained**. In accordance with deployment requirements for operational environments, you have the option of deploying access units within your infrastructure.

Delivering operational security

The intrusion prevention engine enhances access control to areas of the network infrastructure **for more secure actions linked to operational processes**. The in-depth analysis of operational protocols (Deep Packet Inspection) checks the correct use of commands, and the safety mode ensures the continuity of your processes.

... and unique firmware

Stormshield offers one single, user-friendly interface for managing its product range. This will r**educe operating costs, simplify team management and facilitate IT/OT convergence**, saving the company a great deal of time.

And more features

Usage control

Firewall/IPS/IDS mode • Identity-based firewall • Microsoft Services Firewall • Industrial firewall/IPS/IDS • Industrial application control • Detection and control of the use of mobile terminals • Geolocation (countries, continents) • Dynamic Host Reputation • Transparent authentication (Active Directory, SSO Agent, SSL) • Agent-based multi-user VDI authentication (Citrix, TSE) • Guest and sponsorship mode authentication, webservices • Host Checker • Zero Trust Network Access (ZTNA)

Protection from threats

Intrusion detection and prevention • Protocols autodetection and compliancy check • Application inspection • Protection from denial of service attacks (DoS) • Protection from SQL injections • Protection from Cross-Site Scripting (XSS) • Protection from malicious Web2.0 code and scripts (Clean & Pass) • Trojan detection • Detection of interactive connections (botnets, Command & Control) • Protection from data evasion • Advanced management of fragmentation • Automatic reaction to attack (notification, quarantine, block, QOS, dump) • Antispam and antiphishing: reputation-based analysis, heuristic engine • Embedded antivirus (HTTP, SMTP, POP3, FTP) • SSL decryption and inspection • VoIP protection (SIP) • Collaborative security: IP reputation, Cloud based Sandbox on the European territory (option)

Confidentiality

Site-to-site or nomad IPsec VPN • Post Quantum Resistant • Remote SSL VPN access in multi-OS tunnel mode (Windows, Android, iOS, etc.) • SSL VPN agent with automatic configuration (Windows) • Support for Android/iPhone IPsec VPN

Network - Integration

IPv6 • NAT, PAT, transparent (bridge)/routed/hybrid modes • Dynamic routing (RIP - OSPF - BGP) • Multicast • Multiple link management (balancing, failover) • Multi-level internal or external PKI management • Multi-domain authentication (including internal LDAP) • Policy-based routing (PBR) • QoS management • DHCP client/relay/server • NTP client • DNS proxy-cache • HTTP proxy • Aggregate links (LACP, Broadcast Mode and Redundancy) • Spanning-tree management (RSTP/MSTP) • SD-WAN, Multifactor Authentication (MFA)

Management

Web-based management • Interface with privacy mode (GDPR compliancy) • Object-oriented security policy • Contextual security policy • Real-time configuration helper • Rule counter • Connected or disconnected security updates • Global/local security policy • Embedded log reporting and analysis tools • Interactive and customizable reports • Support for multiple syslog server UDP/TCP/TLS • SNMP v2, v3 agent • IPFIX • Automated configuration backup • External storage (option) • Open API • Script recording • High availability.

TECHNICAL SPECIFICATIONS

PERFORMANCE[1]	SNi50
Firewall throughput (1518 byte UDP)	**20 Gbps**
Firewall throughput (IMIX)	**9.1 Gbps**
IPS throughput (1518 byte UDP)	**15 Gbps**
IPS throughput (IMIX)	**4 Gbps**
Threat protection*	**1.3 Gbps**
Latency (avg, µs, at 80% load)	**83 µs**

** Threat protection is measured with firewall, IPS, antivirus, IP reputation, and web application security enabled, using a realistic traffic mix, and with logging enabled.*

VPN	SNi50
IPsec throughput - AES-GCM256 (1408 bytes)	**5.7 Gbps**
IPSec - AES-GCM (IMIX)	**2.7 Gbps**
Max number of IPsec VPN tunnels	**750**
Nb of SSL VPN clients	**500**

NETWORK CONNECTIVITY	SNi50
Max number of simultaneous sessions	**600,000**
Nb of new sessions/sec.	**80,000**
Nb of main gateways (max) / backup (max)	**64/64**

CONNECTIVITY	SNi50
2.5GBASE-T copper interfaces	**8**
10Gb SFP+ interfaces	**2**
Bypass pairs (on copper ports)	**2**

REDUNDANCY	SNi50
High Availability / Bypass (safety mode)	**Yes**

PROTOCOLS - DEEP PACKET INSPECTION (DPI)	SNi50
Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP, PROFINET, SOFBUS/LACBUS, IEC 60870-5-104, IEC 61850 (MMS, Goose & SV), S7+ & IT	

HARDWARE	SNi50
Storage	**85 GB**
TPM chip	**Yes**
MTBF at 25°C (years)	**108.5**
Installation	**DIN rail UTA 159 (35mm, IEC/EN 60715:2017)**
Height x Width x Depth (mm)	**160 x 78 x 127**
Weight	**2.23 kg (4.92 lbs)**
Double power supply (DC)	**2x 12-48VDC 6A-1.5A**
Power consumption (idle / avg / max en W)	**20 / 29 / 31**
Fans	**-**
Thermal dissipation (max, BTU/h)	**68 / 99 / 106**
Operational temperature	**-40° to +70°C (-40° to +167°F)**
Relative humidity, operating (without condensation)	**0% to 95%**
Level of protection provided by the appliance (IP Code)	**IP40**
Storage temperature	**-40° to +85°C (-40° to +185°F)**
Relative humidity, storage (without condensation)	**5% to 95%**

CERTIFICATIONS	SNi50
CE/UKCA/FCC/ICES-003/RCM/CB, EN 61000-6-2, EN 61000-6-4, IEC 61000-4-18, IEC 60068-2, IEC 61850-3, IEEE 1613, EN 50121-1, EN 50121-4, IEC 60529	

1 Performance is measured in a laboratory environment under ideal conditions for version 5.x. Results may vary depending on test conditions and software version.

SERVICE PACKS

ESSENTIAL SECURITY PACK

Companies looking for protection for their industrial infrastructures can subscribe to this package. It is tailored **to carefully finely filter and manage access to the operational network while ensuring in-depth inspection of industrial protocols**. The VPN connection feature in particular (both IPsec and SSL) provides a secure access point for remote maintenance operations.

PREMIUM SECURITY PACK

This pack focuses on corporations with stringent security requirements, by **providing the best technology for countering even the most sophisticated attacks. Advanced antimalware system with emulation technology and URL filtering in cloud mode based on more than 70 categories (Extended Web Control)** will raise your protection to a level that is unrivalled on the market.

	Industrial Security Pack	Premium Security Pack
Next-Generation Firewall		
Layer 7 Firewall	✔	✔
Geolocation	✔	✔
Web applications	✔	✔
User authentication, MFA & SSO	✔	✔
Secure SD-WAN & ZTNA		
IPsec VPN gateway	✔	✔
Postquantum encryption	✔	✔
SSL VPN gateway & client	✔	✔
Device posture assessment	✔	✔
Threat Protection		
IPS/IDS	✔	✔
Trusted public certificates	✔	✔
Antispam	✔	✔
Threat intelligence (IP & domains)	✔	✔
Industrial protocols DPI	✔	✔
Antimalware	Option	✔
Breach Fighter AI-powered sandboxing	Option	✔
Extended Web Control (URL filtering)	Option	✔
Services		
Software maintenance	✔	✔
Hardware maintenance	✔	✔
Standard support access	✔	✔
Automated configuration backup	✔	✔
24x7 technical support access	Option	Option
Express exchange	Option	Option
Secure return	Option	Option

HARDWARE EXCHANGE

All security packs include hardware maintenance in order to ensure business continuity in the event of a hardware failure. Your appliance will simply be exchanged for a similar replacement product. Three levels of service are available.

Standard exchange
Your appliance will be exchanged once our customer service center receives the defective appliance.

Express exchange
Your appliance will be exchanged in advance. As soon as our support centers diagnose a hardware failure, the replacement product will be sent, which you would receive the next working day[1].

Serenity4all
With this service, you replace the product yourself once our support centers have diagnosed the malfunction fault[2].

[1] Please check with us regarding the eligible countries and cities. Applies to diagnoses made before 1 p.m.

[2] Replacement products must be acquired in advance for this service.

FOR OPTIMAL PROTECTION

Stormshield offers options to cover your additional cybersecurity needs.

Neutralize the most sophisticated threats with Stormshield Network Advanced Antivirus.

Benefit from an advanced and reliable filtering solution with Stormshield Extended Web Control.

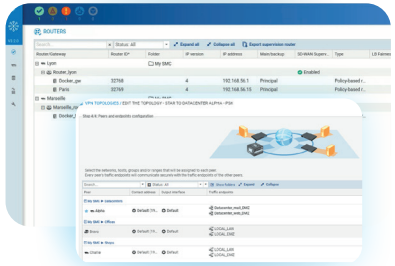
Expand your home office with highly secure remote access with Stormshield VPN Client.

MANAGE YOUR SECURITY WITH EFFICIENT TOOLS

A decision-making tool

with Stormshield Log Supervisor

Optimize your research tasks and incident response. And thanks to its quick overview of system effectiveness, you willl have peace of mind knowing your security investments are worthwhile.



Management of large infrastructures

with Stormshield Management Center

Stormshield Management Center exchanges SNS firewalls configuration and monitoring data in real time, while ensuring their confidentiality and integrity. Its intuitive graphical interface minimizes configuration errors and its global management of security and filtering policies eliminates repetitive tasks.

THE **EUROPEAN CHOICE** IN **CYBERSECURITY**

www.**stormshield**.com