STORMSHIELD

SNi20

Industrial security

Up to 4 Gbps
FIREWALL PERFORMANCE

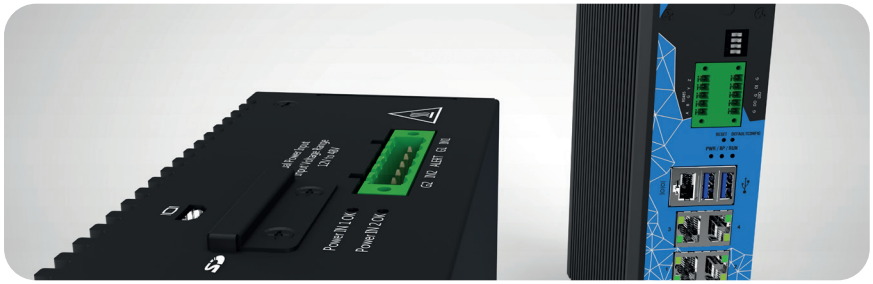
Up to 800 Mbps
VPN PERFORMANCE

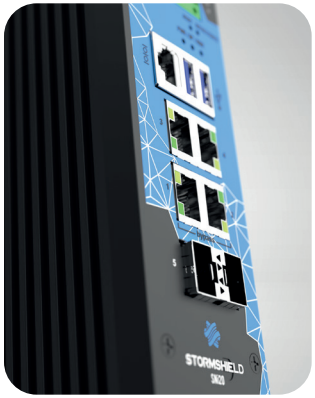
Ruggedized
INTEGRATION INTO YOUR CONSTRAINED ENVIRONMENTS



NETWORK SECURITY

AN INDUSTRIAL-GRADE FIREWALL







Transparent zone isolation

Network integration features ensure the segmentation of your operational system with minimal impact on your existing infrastructure. The SNi20 product thus guarantees optimal isolation between the different zones of your system.

Secure remote maintenance

Remote maintenance operators have direct and secure access to the systems to be maintained. By deploying SNi20 within your operational infrastructure, you control access by limiting exposed zones.

Securing operations

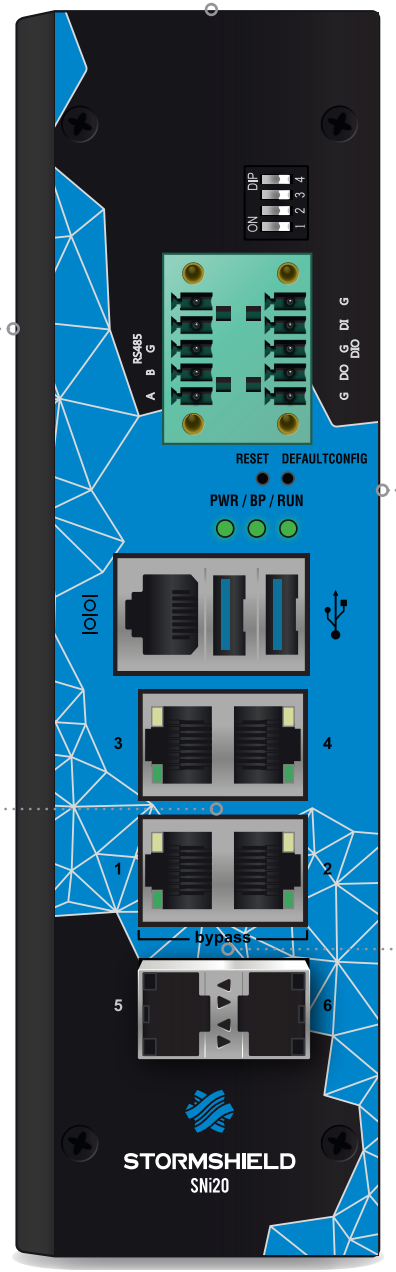
By combining access controls for different zones with deep packet inspection (DPI), you ensure comprehensive security for your infrastructure. The SNi20 product's safety mode guarantees the continuity of your operational processes.

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.

Redondant industrial power supply
2 x 12-48 VDC

Ruggedized appliance
for constrained operating environments



Operational warranty
High availability

TPM
Chip

-40° to +70°C
Extended operating temperature range

ESSENTIAL DATA

Industrial SNi20

Connectivity
2
SFP 1GbE Interfaces

Performance
4 Gbps
Firewall

Performance
2.5 Gbps
Firewall (IMIX)

Compact
ruggedized
Format

VPN
800 Mbps
IPsec throughput

VPN
200
IPsec tunnels



FEATURES

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

Network segmentation

The different 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) **provides maintenance operators with controlled and secure access** to the systems requiring maintenance. Compliant with deployment requirements in operational environments, you can deploy access boxes within your operational infrastructure.

Securing operations

The intrusion prevention engine enhances **access control to operational areas to secure process-related actions**. Deep packet inspection (DPI) verifies the proper use of commands, and safe mode ensures the continuity of your operational processes.

... and unique firmware

Stormshield offers a unique, ergonomic interface for managing its products range. This **reduces operating costs, facilitates the management** of IT teams and **saves time** for the company.

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]	SNi20
Firewall throughput (1518 byte UDP)	**4 Gbps**
Firewall throughput (IMIX)	**2.5 Gbps**
IPS throughput (1518 byte UDP)	**2.6 Gbps**
IPS throughput (IMIX)	**690 Mbps**
Threat protection*	**240 Mbps**

** 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	SNi20
IPsec throughput - AES-GCM256 (1408 bytes)	**800 Mbps**
IPSec - AES-GCM256 (IMIX)	**390 Mbps**
Max number of IPsec VPN tunnels (1024 kbps per tunnel)	**200**
Nb of SSL VPN clients	**200**

NETWORK CONNECTIVITY	SNi20
Max number of simultaneous sessions	**500,000**
Nb of new sessions/sec.	**20,000**

CONNECTIVITY	SNi20
Copper 10/100/1000 Interfaces	**2-4**
1Gbps SFP slots	**0-2**

REDUNDANCY	SNi20
High Availability	**Yes**
Bypass (safety mode)	**Optional**

PROTOCOLS - DEEP PACKET INSPECTION (DPI)	SNi20
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	SNi20
Storage	**SD card**
TPM chip	**Yes**
MTBF at 25°C (years)	**35.1**
Installation	**DIN rail UTA 159 (35mm, IEC/EN 60715:2017)**
Height x Width x Depth (mm)	**210 x 60 x 155**
Weight	**1.75 kg (3.86 lbs)**
Packaged Height x Width x Depth (mm)	**190 x 270 x 235**
Packaged weight	**2.46 kg (5.42 lbs)**
Double power supply (DC)	**2x12-48VDC 3-0.75A**
Power consumption 48VDC @25°C (idle/avg/max in Watt)	**6 / 8 / 9**
Thermal dissipation 48VDC (idle/avg/max in BTU/h)	**20 / 27 / 31**
Noise level	**Fanless**
Ingress Protection code (IP code)	**IP30**
Operational Environment	Temperature: **-40° to +70°C (-40° to +158°F)** Humidity: **0% to 95%**
Storage Environment	Temperature: **-40° to +85°C (-40° to +185°F)** Humidity: **0% to 95%**

CERTIFICATIONS	SNi20
CE/FCC/CB, EN 55032, EN 55035, EN 50121-1, EN 50121-4, EN 61000-3, EN 61000-6-2, EN 61000-6-4, IEC 60068-2, IEC 61850-3, IEC 61000-4-18, IEC 62443-4-1, IEEE 1613	

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

INDUSTRIAL 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	Option	✔
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.

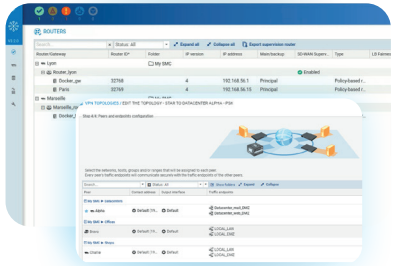
MANAGE YOUR SECURITY WITH EFFICIENT TOOLS



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