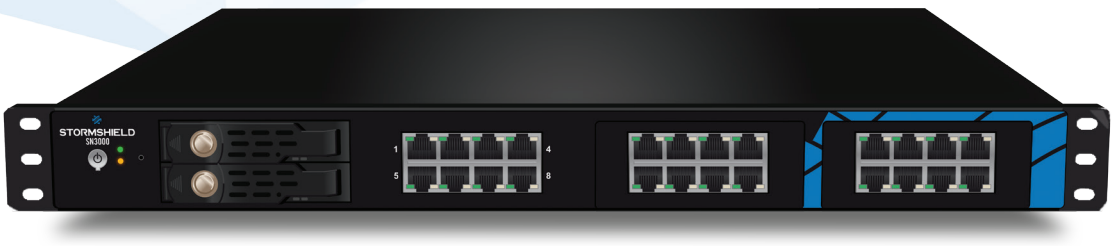
STORMSHIELD

LARGE CORPORATIONS & DATACENTERS



RELIABLE AND SCALABLE HIGH-GRADE UTM & NEXT-GENERATION FIREWALL

Stormshield SN3000

NETWORK SECURITY | ENDPOINT SECURITY | DATA SECURITY

Stormshield SN3000

THE SECURITY SOLUTION IDEAL FOR BUSINESSES & LARGE CORPORATIONS WITH CRITICAL INFRASTRUCTURES.

YOUR INVESTMENT IS FUTURE-READY

Eagerly awaited but only in the process of being deployed in corporate networks, the IPv6 protocol is supported on the whole Stormshield Network Security range. Take on the future and the challenges it brings.

PEACE OF MIND

The SN3000 holds redundant hardware components such as RAID disks and a dual power supply to guarantee that your security solution runs uninterrupted.

OPTIMIZE YOUR INFRASTRUCTURE OVERHEADS

Occupying a compact space (1U) hosted in a datacenter, the SN3000 offers unrivalled network modularity with up to 28 ports (1GE, 10GE, 10/100/1000).

IMPROVE THE SECURITY POLICY ACCORDING TO CONTEXT

Adapt the level of protection for a workstation or server according to the level of risk identified (security alarms generated or vulnerabilities detected). In security reports, select your risk mitigation strategy in just one click.

LARGE CORPORATIONS & DATACENTERS

Ensure the continuity of your business

All protection technologies needed for responding to the most sophisticated attacks are embedded in the entire range.

Manage vulnerabilities

Obsolete or vulnerable applications on workstations and servers are detected in real time.

Keep your commitments to compliance

Stormshield Network Security products are a key component in ensuring compliance with standards, regulations and norms that require access control (PCI-DSS, ISO 27001 or the Data Protection Act, etc.).

Stay in control of your internet usage

Thanks to advanced filtering and the management of quality of service, you can define the way you want the internet to be used.

Technical specifications

USAGE CONTROL

Firewall/IPS/IDS mode, identity-based firewall, application firewall, Microsoft Services Firewall, detection and control of the use of mobile terminals, application inventory (option), vulnerability detection (option), URL filtering (embedded database or cloud mode), transparent authentication (Active Directory SSO Agent, SSL, SPNEGO), multi-user authentication in cookie mode (Citrix- TSE), global/local security policy.

PROTECTION FROM THREATS

Intrusion prevention, protocol scan, 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, Trojan detection, detection of interactive connections (botnets, Command&Control), protection from data evasion, Advanced management of fragmentation, automatic quarantining in the event of an attack, Antispam and antiphishing: reputation-based analysis —heuristic engine, embedded antivirus (HTTP, SMTP, POP3, FTP), detection of unknown malware via sandboxing, SSL decryption and inspection, VoIP protection (SIP), collaborative security: adaptation of the filter policy according to security events or detected vulnerabilities.

CONFIDENTIALITY

Site-to-site or nomad IPSec VPN, remote SSL VPN access in multi-OS tunnel mode (Windows, Android, iOS, etc), SSL VPN agent configurable centrally (Windows), Support for Android/iPhone IPSec VPN.

NETWORK - INTEGRATION

IPv6, NAT, PAT, transparent (bridge)/routed/hybrid modes, dynamic routing (RIP, OSPF, BGP), multi-level internal or external PKI management, internal LDAP directory, explicit proxy, policy-based routing (PBR), QoS management, DHCP client/relay/server, NTP client, DNS proxy-cache, http proxy-cache, high availability, WAN link redundancy, LACP management, Spanning-tree management(RSTP/MSTP).

MANAGEMENT

Web-based management interface, object-oriented security policy, real-time configuration help, firewall rule counter, more than 15 installation wizards, embedded log reporting and analysis tools, interactive and customizable reports, sending to syslog, SNMP v1, v2, v3 agent, automated configuration backup.

Non-contractual document. The features mentioned are those in version 2.1.

** Performance is measured in a laboratory and under conditions ideal for version 2.1. Results may vary according to test conditions and the software version.*

*** IP size: 60% (48 bytes) – 25% (494 bytes) – 15% (1500 bytes).*

PERFORMANCE*	
Firewall throughput (1518 byte UDP)	50 Gbps
Firewall (IMIX**)	15 Gbps
IPS throughput (1518 byte UDP)	30 Gbps
IPS throughput (1 Mbyte HTTP files)	14 Gbps
Antivirus throughput	4 Gbps
VPN*	
IPSec throughput - AES128/SHA1	6.5 Gbps
IPSec throughput - AES256/SHA2	5 Gbps
Max number of IPSec VPN tunnels	5,000
Number of SSL VPN clients (Portal mode)	1,024
Number of simultaneous SSL VPN clients	500
NETWORK CONNECTIVITY	
Concurrent connections	2,500,000
New sessions per second	120,000
Number of main gateways (max)/backup (max)	64/64
Number of interfaces (Agg, Dialup, ethernet, loopback, VLAN, pptp, ...)	1,300
HARDWARE	
10/100/1000 interfaces	10-26
1Gb fiber interfaces	0-16
10Gb fiber interfaces	0-8
Optional interfaces (8 ports 10/100/1000 - 4 ports 1Gb Fiber - 4 ports 10Gb Fiber)	2
SYSTEM	
Max number of filtering rules	32,768
Max number of static routes	10,240
Max number of dynamic routes	500,000
REDUNDANCY	
High Availability (Active/Passive)	✔
Redundant disks	RAID1
Redundant Power supply (hot swappable)	✔
HARDWARE	
Local storage	128 GB SSD
Big Data Option (local storage)	> 900 GB SSD
Racking	1U - 19"
Height x Width x Depth (mm)	44.5 x 443 x 560
Weight	9.6 kg (21.2 lbs)
Packaged Height x Width x Depth (mm)	184 x 710 x 573
Packaged weight	16.6 kg (36.6 lbs)
Power supply (AC)	110-230V 60-50Hz 5A-3A
Power consumption	230V 50Hz 182W 0.99A
Fan	3
Operational temperature	5° to 40°C (41° to 104°F)
Relative humidity, operating (without condensation)	20% to 90% @ 40°C
Storage temperature	-30° to 65°C (-22° to149°F)
Relative humidity, storage (without condensation)	5% to 95% @60°C
CERTIFICATIONS	
Compliance	CE/FCC

For security with high added value

STORMSHIELD NETWORK VULNERABILITY MANAGER*

Arm yourself with a simple and powerful vulnerability detection tool that leaves no impact on your information system.

Vulnerability Management
Based on data passing through the appliance, Stormshield Network Vulnerability Manager makes an inventory of operating systems, applications used and their vulnerabilities. As soon as a vulnerability appears on your network, you will be kept informed.

Remediation
Stormshield Network Vulnerability Manager offers a set of dedicated reports as well as a real-time dashboard that allow you to stay in control of your deployment.

STORMSHIELD NETWORK EXTENDED WEB CONTROL*

Monitor how users surf the internet on your corporate network and optimize your bandwidth consumption by deploying an effective and high-performance URL filtering solution.

Prevention of web-based threats

Extended Web Control analyzes illions of requests in order to continuously evaluate the risk level of various websites and to block infected or malicious sites from being visited as soon as they are detected.

Advanced filtering for all

The Extended Web Control solution can be enabled on the entire range of Stormshield Network Security products. You can therefore benefit from an advanced filter solution regardless of the size of your company.

KASPERSKY ANTIVIRUS*

Protect yourself by getting equipped with the best antivirus protection solution.

Protection from threats

The Kaspersky antivirus solution on Stormshield Network Security appliances is not based merely on a system of malware signatures, but also integrates emulation mechanisms to identify malicious code proactively.

Peripheral protection

Applying an antivirus inspection on the traffic of all devices connected to the network and relying on a behavioral analysis technology similar to sandboxing, it allows the detection of even unknown attacks.

** Option*

STORMSHIELD

Phone
+33 9 69 32 96 29

WWW.STORMSHIELD.EU