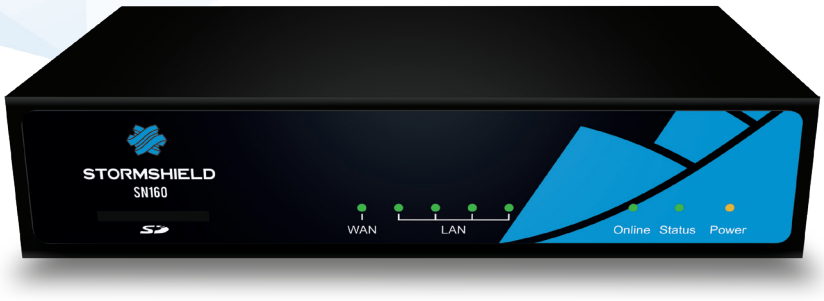
STORMSHIELD

SMALL BUSINESSES & AGENCIES



UNIFIED SECURITY

Stormshield SN160

NETWORK SECURITY | ENDPOINT SECURITY | DATA SECURITY

Stormshield SN160

THE SECURITY SOLUTION IDEAL FOR AGENCIES, REMOTE OFFICES & BRANCHES AND SMALL BUSINESSES.

AGENCIES, REMOTE OFFICES & BRANCHES SMALL BUSINESSES

GET THE BEST UNIFIED SECURITY AT UNBEATABLE VALUE

Without compromising on security in any way, the SN160 embeds all the security functions needed for ensuring the flawless protection of small IT structures. Pure technological prowess.

GRANT ACCESS TO THE RESOURCES ON YOUR CORPORATE NETWORK WITH TOTAL PEACE OF MIND

Sophisticated IPSec VPN features mean that your branches and remote offices are interconnected securely and seamlessly to the main resources of your corporation.

RUN IN UTM MODE OR REMOTE OFFICE MODE

The SN160 provides optimal end-to-end security adapted to your needs, thanks to two dedicated maintenance packs (*Remote Office Security Pack* for the protection of remote offices and *Premium UTM Security Pack* to ensure the security of sites connected directly to the internet).

CONFIGURE THE KIND OF HIGH-LEVEL SECURITY YOU WOULD EXPECT IN LARGE CORPORATIONS IN JUST 3 MINUTES

Intuitive wizards guide you through each step of the installation and configuration of your security device.

Ensure the continuity of your business

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

Save time

The administration interface on Stormshield Network Security products has been designed to be ergonomic and intuitive in order to assist you in securing your corporate network quickly and with zero errors.

Connect coworkers

With the virtual private network, (IPSec and SSL VPN), coworkers get secure access to corporate resources regardless of where they are and from any terminal.

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.

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), filtering per localisation (countries, continents), URL filtering (cloud mode), transparent authentication (Active Directory SSO Agent, SSL, SPNEGO), multi-user authentication in cookie mode (Citrix- TSE), guest mode authentication, time scheduling per rule.

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), 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, multi-domain authentication (including internal LDAP), explicit proxy, policy-based routing (PBR), QoS management, DHCP client/relay/server, NTP client, DNS proxy-cache, HTTP proxy-cache, IPFIX/NetFlow.

MANAGEMENT

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

Non-contractual document. The features mentioned are those in version 3.0.

** Performance is measured in a laboratory and under conditions ideal for version 3.1. Results may vary according to test conditions and the software version.*

*** Option*

Technical specifications

PERFORMANCE*	
Firewall throughput (1518 byte UDP)	1 Gbps
IPS throughput (1518 byte UDP)	800 Mbp
IPS throughput (1 Mbyte HTTP files)	400 Mbps
Antivirus throughput	100 Mbps
VPN*	
IPSec throughput - AES128/SHA1	200 Mbps
IPSec throughput - AES256/SHA2	200 Mbps
Max number of IPSec VPN tunnels	50
Number of SSL VPN clients (Portal mode)	20
Number of simultaneous SSL VPN clients	5
NETWORK CONNECTIVITY	
Concurrent connections	150,000
New connections per second	6,000
Number of main gateways (max)/backup (max)	64/64
CONNECTIVITY	
10/100/1000 interfaces	1+ 4 ports (Switch)
SYSTEM	
Max number of filtering rules	4,096
Max number of static routes	512
Max number of dynamic routes	1,000
REDUNDANCY	
High Availability (Active/Passive)	-
HARDWARE	
Local storage	SD Card storage**
MTBF (years)	24.9
Racking	1U (<1/2 19")
Height x Width x Depth (mm)	45 x 176 x 107
Weight	0.55 kg (1,25 lbs)
Packaged Height x Width x Depth (mm)	78 x 320 x 200
Packaged weight	1.2 kg (2,65 lbs)
Power supply (AC)	100-240V 60-50Hz 1.5-0.8A
Power consumption	230V 50Hz 8.4W 0.07A
Noise level	Fanless
Thermal dissipation (max, BTU/h)	35
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° to 149°F)
Relative humidity, storage (without condensation)	5% to 95% @ 60°C
CERTIFICATIONS	
Compliance	CE/FCC/CB

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

Contact your Regional Sales office today:

WWW.STORMSHIELD.COM/ABOUT-US/OUR-SALES-OFFICES/

Version 1.3 - Copyright Stormshield 2018