



# STORMSHIELD



SMALL BUSINESSES & AGENCIES

UNIFIED SECURITY

# Stormshield SN300

NETWORK SECURITY | ENDPOINT SECURITY | DATA SECURITY

# Stormshield SN300

THE SECURITY SOLUTION IDEAL FOR SMALL BUSINESSES, AGENCIES & REMOTE OFFICES WITH BUSINESS CONTINUITY CHALLENGES.



## CREATE SAFE ZONES ON YOUR NETWORK

With the SN300, you have a choice between 8 physical ports for better flexibility and granularity when defining your filter policy.



## ENSURE BUSINESS CONTINUITY

With the high availability feature, services continue to run uninterrupted, even when your appliance breaks down. Redundant internet access links keep your business running by allowing you to stay in touch on high-quality connections.



## MAKE THE MOST OF YOUR SECURITY

Embedded web-based reporting and log analysis tools let you supervise the security of your network and adapt your level of protection accordingly in a single click.



## 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.

SMALL BUSINESSES,  
AGENCIES  
& REMOTE OFFICES

### **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.

.....

# 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), filtering per localisation (countries, continents), URL filtering (embedded database or 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: Dynamic Host Reputation, IP reputation.

## 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, high availability, WAN link redundancy, 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, external storage (option).

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

## PERFORMANCE\*

Firewall throughput (1518 byte UDP)	800 Mbps
IPS throughput (1518 byte UDP)	800 Mbps
IPS throughput (1 Mbyte HTTP files)	800 Mbps
Antivirus throughput	200 Mbps

## VPN\*

IPSec throughput - AES128/SHA1	400 Mbps
IPSec throughput - AES256/SHA2	350 Mbps
Max number of IPSec VPN tunnels	100
Number of SSL VPN clients (Portal mode)	50
Number of simultaneous SSL VPN clients	20

## NETWORK CONNECTIVITY

Concurrent connections	150,000
New connections per second	18,000
Number of main gateways (max)/backup (max)	64/64
Number of interfaces (Agg, Dialup, ethernet, loopback, VLAN, pptp, ...)	100

## CONNECTIVITY

10/100/1000 interfaces	8
------------------------	---

## SYSTEM

Max number of filtering rules	8,192
Max number of static routes	512
Max number of dynamic routes	10,000

## REDUNDANCY

High Availability (Active/Passive)	✓
------------------------------------	---

## HARDWARE

Local storage	SD Card storage**
MTBF (years)	9,2
Racking	0,5U - 19"
Height x Width x Depth (mm)	44.5 x 210 x 195
Weight	1.3 kg (2.9 lbs)
Packaged Height x Width x Depth (mm)	115 x 395 x 285
Packaged weight	2.4 kg (5.3 lbs)
Power supply (AC)	110-240V 60-50Hz 1.3-0.7A
Power consumption	230V 50Hz 30W 0.25A
Fan	1
Noise level	22 dbA
Thermal dissipation (max, BTU/h)	103
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
------------	--------

\* Performance is measured in a laboratory and under conditions ideal for version 3.0. Results may vary according to test conditions and the software version.

\*\* Option.

# 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 millions 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](http://WWW.STORMSHIELD.EU)