

# STORMSHIELD



LEISTUNGSFÄHIGE NEXT-GENERATION-FIREWALL MIT HOHER PORTDICHTHE

## Stormshield SN6000

NETWORK SECURITY | ENDPOINT SECURITY | DATA SECURITY

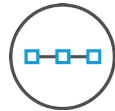
# Stormshield SN6000

DIE SICHERHEITSLÖSUNG FÜR ANSPURCHSVOLLE  
UNTERNEHMEN UND ORGANISATIONEN



## HOCHLEISTUNGSZUGANG

Mit einem Datendurchsatz der Firewall von 130 Gbit/s entspricht der SN6000 schon heute den hohen Anforderungen kritischer Infrastrukturen. Die Multicore-Architektur ist für die modernsten Softwaretechnologien konzipiert und garantiert auch in Zukunft eine hohe Leistungsfähigkeit.



## BRANCHENWEIT HÖCHSTE PORTDICHTHE!

Der SN6000 bietet eine hohe Portdichte (bis zu 58 Ethernetports) und einen Glasfaseranschluss mit sehr hoher Bandbreite. Durch die erstklassige Modularität dieses Produkts können Sie allen Weiterentwicklungen Ihrer Infrastruktur mit Gelassenheit entgegen sehen.



## BLEIBEN SIE GELASSEN

Der SN6000 verfügt über redundante Hardwarekomponenten die RAID-Festplatten und eine Doppelstromversorgung und garantiert somit einen unterbrechungsfreien Betrieb Ihrer Sicherheitslösung.



## ÜBERWACHEN SIE DIE KORREKTE FUNKTION IHRER HARDWARE

Mit der Intelligent Platform Management Interface (IPMI) können Sie Ihr SN6000-Produkt gezielt steuern und überwachen. Im Falle einer Fehlfunktion der Hardware erhalten Sie umgehend eine Warnmeldung.

GROSSE UNTERNEHMEN  
UND RECHENZENTREN

### **Betriebliche Kontinuität sichern**

Die Produkte von Stormshield Network Security vereinen alle verfügbaren Sicherheitstechnologien und bieten einen zuverlässigen Schutz vor komplexen Angriffen, die Ihre betrieblichen Aktivitäten gefährden könnten.

### **Sicherheitslücken kontrollieren**

Veraltete oder gefährdete Anwendungen auf Arbeitsplatzrechnern und Servern werden in Echtzeit erkannt.

### **Konformitätsverpflichtungen einhalten**

Sie kommen Ihren Verpflichtungen in Bezug auf Standards, Regelungen und Normen nach, die eine Zugriffskontrolle erforderlich machen (PCI-DSS, ISO 27001 oder Datenschutzgesetz usw.).

### **Internetaktivität überwachen**

Dank der zuverlässigen Filterfunktionen sowie der Funktionen zur Verwaltung der Dienstqualität haben Sie die Möglichkeit, die Internetaktivitäten entsprechend Ihren Anforderungen zu steuern.

.....

## NUTZUNGSKONTROLLE

Firewall/IPS/IDS-Modus, Benutzer-Firewall, Anwendungsfirewall, Microsoft Services Firewall, Erkennung und Nutzungsüberwachung für mobile Endgeräte, Anwendungsinventar (Option), Erkennung von Sicherheitslücken (Option), Filterung nach Land / Kontinent, URL-Filter (Cloud-Modus), transparente Authentifizierung (Agent SSO Active Directory, SSL, SPNEGO), Multi-User-Authentifizierung im Cookie-Modus (Citrix/TSE), Authentifizierung: Gast-Modus, regelbasierte Zeitsteuerung.

## SCHUTZ VOR SICHERHEITSRISIKEN

Intrusionsschutz, Protokollanalyse, Anwendungsüberwachung, DoS-Schutz (Denial of Service), Schutz vor Einschleusung von SQL-Code, Schutz vor Cross Site Scripting (XSS), Schutz vor schädlichen Programmcodes und Web 2.0-Malware, Trojanererkennung, Erkennung interaktiver Dienste (Botnet, Command&Control), Schutz vor Sitzungsübernahme, Schutz vor Datenverlust, Management von Fragmenten, Automatisches Quarantänemanagement im Angriffsfall, Antispam und Antiphishing: Reputationsanalyse – heuristischer Scanner, Integrierter Virenschutz (HTTP, SMTP, POP3, FTP), Sandbox für Malware-Erkennung, SSL-Entschlüsselung und -Inspektion, VoIP-Schutz (SIP), Kollaborative Sicherheit: Dynamische Host Reputation, IP Reputation.

## VERTRAULICHKEIT BEIM AUSTAUSCH VON DATEN

VPN IPSec Site-to-Site oder Nomade, Remotezugriff per VPN SSL im Tunnelmodus für Multi-OS (Windows, Android, IOS, ...), zentral konfigurierbare Agent-VPN SSL (Windows), VPN IPSec-Unterstützung Android/ iPhone.

## NETZWERK – INTEGRATION

IPv6, NAT, PAT, Transparentmodus (Bridge)/geroutet/hybrid, Dynamisches Routing (RIP, OSPF, BGP), Verwaltung einer internen/externen PKI auf verschiedenen Ebenen, Multi-Domänen-Authentifizierung (Inklusive internem LDAP), expliziter Proxy, Policy-basiertes Routing (PBR), Management der Dienstqualität, DHCP-Client/Relai/Server, NTP-Client, DNS-Proxy-Cache, http-Proxy-Cache, hohe Verfügbarkeit, Redundante WAN-Verbindungen, LACP-Management, Spanning-Tree-Management (RSTP/MSTP), IPFIX/NetFlow.

## VERWALTUNG

Web-Managementschnittstelle, Richtlinien für objektorientierte Sicherheit, Konfigurationsunterstützung in Echtzeit, Nutzungszähler für Firewall-Regeln, mehr als 15 Installationsassistenten, globale/lokale Sicherheitsrichtlinien, Reporting- und Analysetools für eingebettete Protokolle, interaktive und personalisierbare Berichte, Versand per Syslog-Server (UDP/TCP/TLS), SNMP-Agent V1, V2, V3 (AES, DES), automatische Speicherung von Konfigurationen.

*Unverbindliches Dokument Die genannten Funktionen entsprechen denen von Version 3.0*

\* Die Leistungsdaten gelten für Version 3.0 und wurden unter idealen Laborbedingungen ermittelt. Die Werte können je nach Testbedingungen und Programmversion davon abweichen.

\*\* IP-Datenfeld: 60 % (48 Byte) – 25 % (494 Byte) – 15 % (1500 Byte).

<sup>1</sup> Bei Austausch des 1. Netzmoduls mit 8 Ports 10/100/1000 durch ein Modul mit 4 Glasfaser

# Technische Daten

## LEISTUNGSDATEN\*

|   |            |
|---|------------|
| Datendurchsatz Firewall (UDP 1518 Byte)       | 130 Gbit/s |
| Datendurchsatz Firewall IMIX                  | 45 Gbit/s  |
| Datendurchsatz Firewall + IPS (UDP 1518 Byte) | 55 Gbit/s  |
| Datendurchsatz Firewall + IPS (1 MB HTTP)     | 17 Gbit/s  |
| Datendurchsatz Firewall + IPS + Antivirus     | 3,8 Gbit/s |
| Datendurchsatz Firewall + Antivirus           | 4,7 Gbit/s |

## NETZWERKKONNEKTIVITÄT

|                                  |            |
|----------------------------------|------------|
| Max. Anzahl simultaner Sitzungen | 10.000.000 |
| Anzahl neue Sitzungen/Sek.       | 180.000    |
| Max. Anzahl Dialups              | 12         |
| Max. Anzahl Vlan 802.1Q          | 1.024      |

## SYSTEM

|                                   |         |
|-----------------------------------|---------|
| Max. Anzahl Filterregeln          | 32.768  |
| Max. Anzahl statistisches Routing | 5.575   |
| Max. NB für dynamisches Routing   | 500.000 |

## VPN

|                                    |           |
|------------------------------------|-----------|
| Datendurchsatz IPsec – AES128/SHA1 | 12 Gbit/s |
| Max. Anzahl VPN-/IPsec-Tunnel      | 10.000    |
| Anzahl simultaner VPN SSL-Clients  | 500       |

## HOHE VERFÜGBARKEIT

|              |   |
|--------------|---|
| Aktiv/Passiv | ✓ |
|--------------|---|

## HARDWARE

|  |                                  |
|--|----------------------------------|
| Schnittstellen 10/100/1000   | 10-58                            |
| 1 Gb SFP Schnittstelle   | 0-56 <sup>1</sup>                |
| 10 Gb SFP+ Schnittstelle   | 0-28 <sup>1</sup>                |
| Optionale Netzerweiterungsmodule<br>(8 Ports 10/100/1000; 4 oder 8 Ports 1Gb SFP; 4 Ports 10Gb SFP+) | 6                                |
| Lagerung   | 256 GB SSD                       |
| Big-Data-Option für lokale Speicherung   | > 900 GB SSD                     |
| redundante SSD   | RAID1                            |
| Abmessungen  | 2U - 19"                         |
| Höhe x Breite x Tiefe (mm)   | 89 x 445 x 645                   |
| Versorgung (AC)  | 110-230V 60–50 Hz 10-5A          |
| Verbrauch  | 230 V 50 Hz 505W 2,31A           |
| Redundante Stromversorgung (hot swappable)   | ✓                                |
| Lüftung  | 3                                |
| Betriebstemperatur   | 10 bis 35 °C (50 bis 95 °F)      |
| Relative Luftfeuchtigkeit bei Betrieb (keine Kondensation)   | 8 bis 90 bei 35 °C               |
| Lagertemperatur  | -30° bis 65° C [-22° bis 149° F] |
| Relative Luftfeuchtigkeit bei Lagerung (keine Kondensation)  | 5 bis 95 %                       |

## ZERTIFIZIERUNGEN

|             |        |
|-------------|--------|
| Konformität | CE/FCC |
|-------------|--------|

# Für höchste Sicherheit



## STORMSHIELD NETWORK VULNERABILITY MANAGER\*

Entscheiden Sie sich für ein einfaches und dabei leistungsfähiges Tool zur Erkennung von Sicherheitslücken, das sich nahtlos in Ihre vorhandene IT-Umgebung einfügt.

### Sicherheitsrisiken minimieren

Basierend auf dem Anwendungszugriff inventarisiert der Stormshield Network Vulnerability Manager die Betriebssysteme, die verwendeten Anwendungen sowie deren Sicherheitsrisiken auf dem Server. Bei Erkennen einer Sicherheitsgefährdung in Ihrem Netzwerk wird umgehend eine Warnmeldung ausgegeben.

### Weiteres Vorgehen

Der Stormshield Network Vulnerability Manager schlägt konkrete und interaktive Maßnahmen vor, die den sofortigen Schutz per Mausklick ermöglichen.



## STORMSHIELD NETWORK EXTENDED WEB CONTROL\*

Kontrollieren Sie mithilfe einer effizienten und leistungsstarken URL-Filterlösung den Internetverkehr in Ihrem Unternehmen, und sorgen Sie für eine optimierte Bandbreitennutzung.

### Umfassende Analyse

Extended Web Control analysiert Milliarden von Anfragen und ist dadurch in der Lage, das Gefährdungsniveau von Websites zu bewerten und die Blockierung von infizierten oder schädlichen Webseiten einzuleiten.

### Umfassende Filterfunktionen für alle

Die Lösung Extended Web Control kann für sämtliche Produkten von Stormshield Network Security aktiviert werden. Damit steht eine komplexe Filterlösung für jede Unternehmensgröße zur Verfügung.



## ANTIVIRUS KASPERSKY\*

Vertrauen Sie in puncto IT-Sicherheit auf die umfassendste Virenschutzlösung.

### Bedrohungen blockieren

Die Kaspersky-Antivirenlösung für die Stormshield Network Security-Anwendungen beruht nicht nur auf einem Signaturesystem zum Schutz vor Malware, sondern integriert darüber hinaus Emulationsmechanismen zur proaktiven Erkennung von schädlichen Programmcodes.

### Perimeterschutz

Die Kaspersky-Antivirentechnologie für die Stormshield Network Security-Anwendungen überprüft die im Netzwerk verwendeten Geräte auf Schadsoftware und garantiert dadurch den lokalen Schutz von Einzelplatzgeräten und Servern.

*\* Option*



**STORMSHIELD**

[WWW.STORMSHIELD.EU](http://WWW.STORMSHIELD.EU)