



# STORMSHIELD



KLEINE UNTERNEHMEN  
UND FILIALEN

EINHEITLICHE SICHERHEITSLÖSUNG

# Stormshield SN300

NETWORK SECURITY | ENDPOINT SECURITY | DATA SECURITY

# Stormshield SN300

DIE SICHERHEITSLÖSUNG FÜR KLEINE UNTERNEHMEN,  
NIEDERLASSUNGEN UND REMOTE-STANDORTE MIT  
HOHEN GESCHÄFTSANFORDERUNGEN



## VERTRAUENSZONEN IM NETZWERK SCHAFFEN

Der SN300 bietet Ihnen mit seinen 8 Ports die Möglichkeit, Ihre Filterstrategie detailliert und flexibel zu definieren.



## BETRIEBLICHE KONTINUITÄT SICHERN

Dank der Hochverfügbarkeitsfunktion werden die Dienste im Falle einer Fehlfunktion Ihres Gerätes unterbrechungsfrei fortgeführt. Mit der Redundanz der Internetzugänge steht Ihnen für Ihre Geschäftsaktivitäten dauerhaft eine qualitativ hochwertige Verbindung zur Verfügung.



## NUTZEN SIE IHRE SICHERHEIT

Mithilfe der integrierten Webreporting- und Protokollanalysetools können Sie die Sicherheit Ihres Netzwerkes überwachen und jederzeit per Mausklick Ihre Schutzeinstellungen anpassen.



## RICHTEN SIE SICH IN NUR 3 MINUTEN SO SICHER EIN WIE DIE GRÖSSTEN UNTERNEHMEN

Intuitive Assistenten leiten Sie Schritt für Schritt durch die Installation und Konfiguration Ihrer Sicherheitslösung.

KLEINE UNTERNEHMEN,  
NIEDERLASSUNGEN UND  
REMOTE-STANDORTE

### **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.

### **Zeit gewinnen**

Die Verwaltungsoberfläche der Produkte von Stormshield Network Security ist ergonomisch und intuitiv gestaltet und ermöglicht Ihnen das schnelle und fehlerfreie Sichern Ihrer IT-Umgebung.

### **Mitarbeiter vernetzen**

Das virtuelle private Netz (VPN IPSec und SSL) bietet Ihren Mitarbeitern sicheren Zugriff auf Unternehmensressourcen an jedem Ort und mit jedem mobilen Endgerät.

### **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

Intrusion Detection, Protokollanalyse, Anwendungsüberwachung, DoS-Schutz (Denial of Service), SYN Proxy, Schutz vor SQL-Injections, 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 Quarantänenmanagement im Angriffsfall, Antispam und Antiphishing: Reputationsanalyse – heuristischer Scanner, Integrierter Virenschutz (HTTP, SMTP, POP3, FTP), SSL-Entschlüsselung und -Inspektion, VoIP-Schutz (SIP), Kollaborative Sicherheit: Dynamische Host Reputation, IP Reputation.

## VERTRAULICHKEIT BEIM DATENAUSTAUSCH

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, transparent (bridge)/routed/hybrid modes, 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 (DiffServ, Priorisierung, Reservierung, Begrenzung), DHCP Client Relay-Server, Client-NTP, DNS-Proxy-Cache, HTTP-Proxy-Cache, Redundante WAN-Verbindungen, 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*

# Technische Daten

## LEISTUNGSDATEN\*

Datendurchsatz Firewall (UDP 1518 Byte)	800 Mbit/s
Datendurchsatz Firewall + IPS (UDP 1518 Byte)	700 Mbit/s
Datendurchsatz Firewall + IPS (1 MB HTTP)	800 Mbit/s
Datendurchsatz Firewall + IPS + Antivirus	160 Mbit/s
Datendurchsatz Firewall + Antivirus	200 Mbit/s

## NETZWERKKONNEKTIVITÄT

Max. Anzahl simultaner Sitzungen	150.000
Anzahl neue Sitzungen/Sek.	18.000
Max. Anzahl Dialups	4
Max. Anzahl Vlan 802.1Q	64

## SYSTEM

Max. Anzahl Filterregeln	8.192
Max. Anzahl statistisches Routing	512
Max. Anzahl dynamisches Routing	10.000

## VPN

Datendurchsatz IPsec – AES128/SHA1	400 Mbit/s
Max. Anzahl VPN-/IPsec-Tunnel	200
Anzahl simultaner VPN SSL-Clients	20

## HOHE VERFÜGBARKEIT

Aktiv/Passiv	✓
--------------	---

## HARDWARE

Schnittstellen 10/100/1000	8
Lagerung	Speicher auf SD-Karte**
MTBF bei 25° C (Jahre)	9,2
Abmessungen	1U (1/2 Breite)
Höhe x Breite x Tiefe (mm)	44.5 x 210 x 195
Gewicht	1,3 kg
Höhe x Breite x Tiefe verpacktes Produkt (mm)	115 x 395 x 285
Gewicht (verpackt)	2,4 kg
Versorgung (AC)	110–240 V 60–50 Hz 1.3-0.7A
Verbrauch	230 V 50 Hz 30W 0.25A
Lüfter	1
Geräuschpegel	22 dbA
Wärmeableitung	103
Betriebstemperatur	5° bis 40° C (41° bis 104° F)
Relative Luftfeuchtigkeit bei Betrieb (keine Kondensation)	20 % bis 90 % bei 40° C
Lagertemperatur	-30 bis 65 °C (-22 bis 149 °F)
Relative Luftfeuchtigkeit bei Lagerung (keine Kondensation)	5 % bis 95 % bei 60° C

## ZERTIFIZIERUNGEN

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

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

\*\*Optional

# 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)