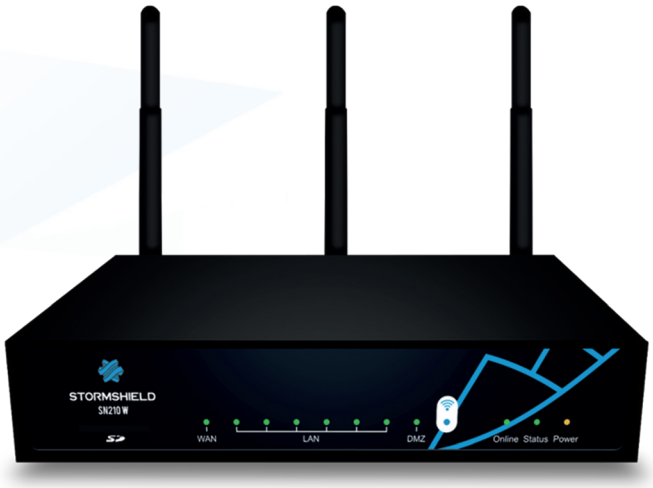
STORMSHIELD

KLEINE UNTERNEHMEN UND AUSSENSTELLEN



SICHERHEIT FÜR IHR WLAN – EINFACH UND MÜHELOS

Stormshield SN210W

NETWORK SECURITY | ENDPOINT SECURITY | DATA SECURITY

Stormshield SN210W

DIE SICHERHEITSLÖSUNG FÜR KLEINUNTERNEHMEN, FILIALEN, AUSSENSTELLEN UND KLEINGEWERBE

SICHERES WLAN

Mit seinen getrennten WLAN-Bereichen ermöglicht das SN210W die Segmentierung des drahtlosen Netzwerks und vereinfacht damit die Verwaltung der Zugriffsrechte und der damit verbundenen Ressourcen. Alle mobilen Geräte und verbundenen Objekte werden dabei über eine einzige Sicherheitslösung geschützt.

ENTSCHEIDEN SIE SICH FÜR DIE BESTE, VEREINHEITLICHTE SICHERHEITSLÖSUNG

Die SN210W-Lösung bietet die umfassendsten Funktionen, die derzeit auf dem Markt für einen optimalen Schutz verfügbar sind: Firewall, Schutz gegen Eindringlinge, Anwendungskontrolle, VPN, Antivirus, Antispam, Webfilterung, Schwachstellenverwaltung.

SICHERN SIE DEN UNTERBRECHUNGSFREIEN BETRIEB IHRES UNTERNEHMENS

Dank der Redundanz der Internetverbindungen können Sie sich auf eine hochwertige, unterbrechungsfreie Verbindung verlassen und damit Betriebsausfälle verhindern.

DER SICHERE WEG IN DIE MOBILE ARBEITSWELT

Die VPN SSL der Stormshield Network Security-Lösung ist mit allen Endgeräten (Android, Apple, Windows...) kompatibel und bietet Ihren mobilen Anwendern eine abgesicherte Verbindung über alle Ressourcen Ihres Unternehmens als wären sie mit dem lokalen Netzwerk verbunden.

KLEINE UNTERNEHMEN, FILIALEN, AUSSENSTELLEN UND KLEINE GEWERBEUNTERNEHMEN

Sichern Sie den unterbrechungsfreien Betrieb Ihres Unternehmens

Die Angebotspalette von Stormshield Network Security enthält alle Schutztechnologien, um auch komplexe und ausgeklügelte Angriffe zu bekämpfen, die die Aktivitäten Ihres Unternehmens gefährden können.

Geben Sie Ihr WLAN beruhigt für Ihre Gäste frei

Der Gastmodus ist speziell für WLAN-Netze vorgesehen und ermöglicht Ihren Kunden und Partnern eine darahtlose Verbindung, ohne dass Sie die Kontrolle über die Benutzer aufgeben müssten.

Verwalten Sie Schwachstellen

Veraltete Anwendungen oder Programme mit bekannten Schwachstellen auf Ihren Workstations und Servern werden in Echtzeit erkannt.

Behalten Sie die Kontrolle über die Internetnutzung

Dank der erweiterten Filterfunktionen und der Steuerung der Servicequalität können Sie die Internetnutzung nach Bedarf kontrollieren.

KONTROLLE DER NUTZUNG

Firewall/IPS/IDS-Modus, Firewall basierend auf der Identität der Benutzer, Firewall für Anwendungen, Microsoft Services Firewall, Erkennung und Kontrolle der Nutzung mobiler Endgeräte, Bestandsverwaltung von Anwendungen (Option), Schwachstellenerkennung (Option), Filterung nach Standort (Land, Kontinent), Filtern von URLs im Cloud-Modus, transparente Authentifizierung (Agent SSO Active Directory, SSL, SPNEGO), Mehrfachbenutzer-Authentifizierung im Cookie-Modus (Citrix-TSE), Gastmodus-Authentifizierung, durch Regeln gesteuerte Zeitprogrammierung.

SCHUTZ GEGEN BEDROHUNGEN

Vorbeugung gegen Eindringversuche, Protokollanalyse, Inspektion von Anwendungen, Schutz gegen Denial-of-Service (DoS), Schutz gegen SQL-Einschleusung, Schutz gegen Cross Site Scripting (XSS), Schutz gegen bösartigen Code und Web2.0-Skripte, Erkennung von Trojanern, Erkennung von interaktiven Verbindungen (Botnet, Command&Control), Schutz gegen Datendiebstahl, erweiterte Verwaltung der Fragmentierung, automatische Quarantäne bei Angriffen, Antispam und Antiphishing: Analyse nach Reputation – heuristische Engine, integriertes Antivirus (HTTP, SMTP, POP3, FTP), Erkennung unbekannter Malware durch Sandboxing, Dechiffrierung und Inspektion von SSL, Schutz von VoIP (SIP), Sicherung der Zusammenarbeit: Anpassung der Richtlinien für die Filterung je nach Sicherheitsereignissen oder erkannten Schwachstellen.

VERTRAULICHKEIT DES DATENVERKEHRS

VPN IPSec von Site zu Site oder Nomadenmodus, Fernzugriff über VPN SSL im Tunnelmodus für mehrere Betriebssysteme (Windows, Android, iOS, …), zentralisiert verwalteter, konfigurierbarer VPN SSL-Agent (Windows), Unterstützung von VPN IPSec Android/iPhone.

NETZWERK UND INTEGRATION

IPv6, NAT, PAT, transparenter Modus (Bridge)/geroutet/hybrid, dynamisches Routen (RIP, OSPF, BGP), Verwaltung von internen oder externen PKI auf mehreren Ebenen, Verzeichnisse für mehrere Domänen (einschließlich interne LDAP-Verzeichnisse), expliziter Proxy, Routen nach Richtlinien (PBR), Verwaltung der Servicequalität, Client/Relais/Server DHCP, NTP-Client, Proxy-Cache DNS, Proxy-Cache HTTP, IPFIX/NetFlow.

VERWALTUNG

Webschnittstelle für die Verwaltung, objektorientierte Sicherheitsrichtlinie, Hilfe bei der Konfiguration in Echtzeit, Zähler der Nutzung von Firewall-Regeln, mehr als 15 Installationsassistenten, globale/lokale Sicherheitsrichtlinien, Tools für Berichte und die Analyse von integrierten Protokollen, interaktive und anpassbare Berichte, Versenden von Trace-Logs im Syslog UDP/TCP/TLS, SNMP-Agent v1, v2, v3, automatisches Speichern der Konfigurationen.

Dokument ohne Vertragskraft. Die angegebenen Funktionen beziehen sich auf die Version 3.0.

* Die Leistungsdaten gelten für Version 3.1 und wurden unter idealen Laborbedingungen ermittelt. Die Werte können je nach Testbedingungen und Programmversion davon abweichen.

*** Option*

Technische Daten

LEISTUNGSDATEN*	
Datendurchsatz Firewall (UDP 1518 Byte)	2 Gbit/s
Datendurchsatz IPS (UDP 1518 Byte)	1,6 Gbit/s
Datendurchsatz IPS (1 MB HTTP)	800 Mbit/s
Datendurchsatz Antivirus (Proxy)	300 Mbit/s
NETZWERKKONNEKTIVITÄT VPN	
Datendurchsatz IPsec – AES128/SHA1	350 Mbit/s
Datendurchsatz IPsec – AES256/SHA2	350 Mbit/s
Max. Anzahl VPN-/IPsec-Tunnel	50
Max. Anzahl VPN-/SSL-Client (portal mode)	20
Anzahl simultaner VPN SSL-Clients	20
NETZWERKKONNEKTIVITÄT	
Max. Anzahl simultaner Sitzungen	200.000
Anzahl neue Sitzungen/Sek.	15.000
Anzahl der Hauptgateways (max.)/Backup-Gateways (max.)	64/64
Max. Schnittstellenanzhal (Agg, Dialup, Ethernet, loopback, VLAN, PPTP,...)	100
KONNEKTIVITÄT	
Schnittstellen 10/100/1000	2+6
Anz. SSID	2
Protokolle	802.11 a/b/g/n
Authentifizierung	WPA/WPA2
SYSTEM	
Max. Anzahl Filterregeln	4.096
Max. Anzahl statistisches Routing	512
Max. Anzahl dynamisches Routing	1.000
HOHE VERFÜGBARKEIT	
Aktiv/Passiv	-
HARDWARE	
Speicher	Speicher auf SD Card**
MTBF bei 25° C (Jahre)	20,1
Abmessungen	1U (<1/2 19")
Höhe x Breite x Tiefe (mm)	46 x 210 x 240
Gewicht	1 kg
Höhe x Breite x Tiefe verpacktes Produkt (mm)	90 x 360 x 290
Gewicht (verpackt)	2 kg
Versorgung (AC)	100–240 V 60–50 Hz 1,3–0,75A
Verbrauch	230 V 50 Hz 13,3W 0,17A
Geräuschpegel	0hne Lüfter
Wärmeableitung	55
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/CB

Für Sicherheit mit hoher Wertschöpfung

STORMSHIELD NETWORK VULNERABILITY MANAGER*

Rüsten Sie Ihre Organisation mit einem einfachen und leistungsstarken Tool für die Erkennung von Schwachstellen ohne Beeinträchtigung Ihres IT-Systems aus.

Schwachstellenverwaltung
Ausgehend von den Datenströmen, die durch die Appliance geleitet werden, erfasst der Stormshield Network Vulnerability Manager den Bestand der Betriebssysteme, der benutzten Anwendungen und ihrer Schwachstellen auf Arbeitsplätzen und Servern. Sobald eine Schwachstelle in Ihrem Netzwerk erkannt wird, werden Sie informiert.

Problembehebung (Maßnahmen)
Stormshield Network Vulnerability Manager verfügt über eine Reihe von spezifischen und interaktiven Berichten zur Anwendung einer Schutzfunktion mit einem Klick.

STORMSHIELD NETWORK EXTENDED WEB CONTROL*

Kontrollieren Sie die Internetnavigation Ihres Unternehmens und optimieren Sie die Nutzung Ihrer Bandbreite, indem Sie eine wirksame und leistungsfähige Lösung für die URL-Filterung bereitstellen.

Profunde Analyse
Milliarden Anfragen werden von der Extended Web Control analysiert, um das Risiko von Websites laufend zu bewerten und die Blokkierung von Abfragen zu ermöglichen, wenn eine infizierte oder bösartige Site erkannt wird.

Erweiterte Filter für alle
Die Lösung Extended Web Control kann für die komplette Stormshield Network Security-Produktserie aktiviert werden. Sie nutzen damit eine moderne Filterlösung unabhängig von der Größe Ihres Unternehmens.

ANTIVIRUS KASPERSKY*

Schützen Sie sich mit der besten Antiviruslösung.

Abwehren von Bedrohungen
Die Kaspersky-Antiviruslösung für die Stormshield Network Security-Appliances beruht nicht nur auf einem Basissystem mit Virussignaturen, sondern enthält Emulationsmechanismen, mit denen bösartiger Programmcode proaktiv erkannt werden kann.

Schutz des Perimeters
Die Kaspersky-Antivirustechnologie für die Stormshield Network Security-Appliances ermöglicht eine Antivirusprüfung der Datenströme aller mit dem Netzwerk verbundenen Geräte sowie den lokalen Schutz der Workstations und Server.

** Option*

STORMSHIELD

WWW.STORMSHIELD.EU

dach@stormshield.eu