STORMSHIELD

KLEINE UNTERNEHMEN UND FILIALEN

EINHEITLICHE SICHERHEITSLÖSUNG

Stormshield SN210

NETWORK SECURITY | ENDPOINT SECURITY | DATA SECURITY

Stormshield SN210

DIE SICHERHEITSLÖSUNG FÜR KLEINE UNTERNEHMEN, NIEDERLASSUNGEN UND REMOTE-STANDORTE

ENTSCHEIDEN SIE SICH FÜR EINE EINHEITLICHE SICHERHEITSLÖSUNG

Der SN200 bietet Ihnen die branchenweit umfassendsten Sicherheitsfunktionen für optimalen Schutz: Firewall, Intrusionsschutz, Anwendungskontrolle, VPN, Virenschutz, Spamschutz, Webfilter, Management von Sicherheitsrisiken …

VERTRAUENSZONEN IM NETZWERK SCHAFFEN

Dank der hohen Anzahl verfügbarer Ports können Sie Ihr Netzwerk in Segmente unterteilen, um so Ihre sensiblen Ressourcen zu verwalten bzw. Internetdienste bereitzustellen.

BETRIEBLICHE KONTINUITÄT SICHERN

Mit der Redundanz der Internetzugänge steht Ihnen für Ihre Geschäftsaktivitäten dauerhaft eine qualitativ hochwertige Verbindung zur Verfügung.

MOBILITÄT BEI HÖCHSTER SICHERHEIT

Das SSL-VPN der Stormshield Network Security-Lösungen ist mit allen Endgerättypen (Android, Apple, Windows...) kompatibel und bietet Ihren mobilen Nutzer eine sichere Anbindung an alle Ressourcen in Ihrem Unternehmen, als ob sie mit dem LAN verbunden wären.

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.

Sicherheitslücken kontrollieren

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

Internetaktivität überwachen

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

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
SYSTEM	
Max. Anzahl Filterregeln	4.096
Max. Anzahl statistisches Routing	512
Max. Anzahl dynamisches Routing	1.000
HOHE VERFÜGBARKEIT	
Aktiv/Passiv	-
HARDWARE	
Schnittstellen 10/100/1000	2+6
Speicher	Speicher auf SD Card**
MTBF bei 25° C (Jahre)	20,6
Abmessungen	1U (<1/2 19")
Höhe x Breite x Tiefe (mm)	46 x 210 x 195
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 11,1W 0,1A
Geräuschpegel	Ohne Lüfter
Wärmeableitung	45
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 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.

Management von Sicherheitsrisiken

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 Signaturensystem 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

Version 1.1 - Copyright Stormshield 2017