STORMSHIELD

GRANDES ORGANISATIONS & DATACENTERS

SOLUTION UTM & NEXT-GENERATION FIREWALL ROBUSTE ET ÉVOLUTIVE

Stormshield SN3000

NETWORK SECURITY | ENDPOINT SECURITY | DATA SECURITY

Stormshield SN3000

LA SOLUTION DE SÉCURITÉ DÉDIÉE AUX INFRASTRUCTURES CRITIQUES, PRÉSENTANT UN ENCOMBREMENT MINIMUM.

GRANDES ORGANISATIONS & DATACENTERS

VOTRE INVESTISSEMENT EST FUTURE-READY[1]

Longtemps attendu et seulement en cours de déploiement dans les réseaux d'entreprise, le protocole IPv6 est supporté par l'ensemble de la gamme Stormshield Network Security. Vous êtes ainsi prêt à relever vos challenges du futur.

RESTEZ SEREIN

Le SN3000 possède des composants matériels redondants comme des disques RAID ou une double alimentation pour garantir un fonctionnement sans interruption de votre solution de sécurité.

OPTIMISEZ VOS COÛTS D'INFRASTRUCTURE

Avec un encombrement minimum (1U) pour un logement dans un datacenter, le SN3000 vous offre une modularité réseau inégalée jusqu'à 28 ports (1GE, 10GE, 10/100/1000).

AMÉLIOREZ LA POLITIQUE DE SÉCURITÉ EN FONCTION DU CONTEXTE

Vous adaptez le niveau de protection pour un poste de travail ou un serveur en fonction du niveau de risque identifié (alarmes de sécurité générées ou vulnérabilités détectées). En 1 clic sur les rapports de sécurité, vous choisissez votre stratégie de mitigation du risque.

Assurez la continuité des activités de votre entreprise

L'ensemble de la gamme Stormshield Network Security intègre toutes les technologies de protection pour répondre aux attaques les plus sophistiquées qui peuvent mettre en péril les activités de votre entreprise.

Gérez les vulnérabilités

Les applications obsolètes ou vulnérables sur vos postes et serveurs sont détectées en temps réel.

Respectez vos engagements de conformité

Vous respectez vos obligations vis-à-vis des standards, réglementations et normes qui imposent un contrôle des accès (PCI-DSS, ISO 27001 ou loi Informatique et Libertés, etc.).

Maîtrisez votre usage d'internet

Grâce aux fonctions de filtrage avancé et de gestion de la qualité de service, vous pouvez contrôler l'utilisation d'internet selon vos besoins.

[1] Sécurité prête pour le futur

CONTRÔLE DES USAGES

Mode Firewall/IPS/IDS, Firewall utilisateur, Firewall applicatif, Microsoft Services Firewall, Détection et contrôle de l'usage des terminaux mobiles, Inventaire des applications (option), Détection des vulnérabilités (option), Filtrage d'URLs (base embarquée ou mode Cloud), Programmation horaire par règle, Accès au réseau en mode guest.

PROTECTION CONTRE LES MENACES

Prévention d'intrusion, Analyse protocolaire, Inspection applicative, Protection contre les dénis de service (DoS), Proxy SYN, Protection contre les injections SQL, Protection contre le Cross Site Scripting (XSS), Protection contre les codes et scripts Web2.0 malveillants, Détection des chevaux de Troie, Détection des connexions interactives (Botnet, Command&Control), Protection contre l'usurpation de sessions, Protection contre l'évasion de données, Gestion avancée de la fragmentation, Mise en quarantaine automatique en cas d'attaque, Antispam et antiphishing : analyse par réputation — moteur heuristique, Antivirus intégré (HTTP, SMTP, POP3, FTP), détection de malwares inconnus par sandboxing, Déchiffrement et inspection SSL, Protection VoIP (SIP), Sécurité collaborative : adaptation de la politique de filtrage en fonction des événements de sécurité ou des vulnérabilités détectées.

CONFIDENTIALITÉ DES ÉCHANGES

VPN IPSec site à site ou nomade, IPSec NAT Transversal, Dead Peer Detection, Accès distant PPTP, Accès distant VPN SSL en mode tunnel multi-OS (Windows, Android, IOS,…), Agent VPN SSL configurable de manière centralisée (Windows), Support VPN IPSec Android/IPhone.

RÉSEAU - INTÉGRATION

IPv6, NAT, PAT, mode transparent (bridge)/routé/hybride (bridges sur plusieurs interfaces+routage), Routage dynamique (RIP, OSPF, BGP), Authentification transparente (Agent SSO Active Directory, SSL, SPNEGO), Authentification multi-user en mode cookie (Citrix- TSE), ICAP mode requête, Gestion de PKI interne ou externe multi-niveau, Annuaire LDAP interne, Proxy transparent ou explicite, Routage par politique (PBR), Gestion de la qualité de service (DiffServ, priorité, réservation, limitation), Client-relai-serveur DHCP, Client NTP, Proxy-cache DNS, Proxy-cache http, Haute-disponibilité avec synchronisation des sessions, Redondance de liens WAN, Gestion du LACP, Gestion du spanning-tree (RSTP/MSTP).

MANAGEMENT

Interface de management Web, politique de sécurité orientée objets, aide à la configuration en temps réel, plus de 15 assistants d'installation, politique de sécurité globale/locale, Outils de reporting et d'analyse de logs embarqués, Rapports interactifs et personnalisables, Envoi des traces vers des serveurs syslog (3 max), Compteurs d'utilisation des règles firewall, Agent SNMP v1, v2, v3 (AES, DES), Administration par rôle, Alertes e-mails, Sauvegarde automatisée des configurations.

Document non contractuel. Les fonctionnalités citées sont celles de la version 2.1.

** Les performances sont mesurées en laboratoire et en conditions idéales pour la version 2.1. Les résultats peuvent varier en fonction des conditions de test et de la version logicielle.*

*** Taille de la trame IP: 60% (48 octets) – 25% (494 octets) – 15% (1 500 octets).*

Spécifications techniques

PERFORMANCES*	
Débit Firewall (UDP 1518 octets)	50 Gbps
Débit Firewall (IMIX**)	15 Gbps
Débit IPS (UDP 1518 octets)	30 Gbps
Débit IPS (1 Mb HTTP)	14 Gbps
Débit Antivirus	4 Gbps
VPN*	
Débit IPSec - AES128/SHA1	6,5 Gbps
Débit IPSec - AES256/SHA2	5 Gbps
Nb max de tunnels VPN IPSec	5 000
Nb de clients VPN SSL en mode portail	1 024
Nb de clients VPN SSL simultanés	500
CONNECTIVITÉ RÉSEAU	
Nb max de sessions simultanées	2 500 000
Nb de nouvelles sessions/sec.	120 000
Nb de passerelles principales (max)/backup (max)	64/64
Nb max d'interfaces (Agg, Dialup, ethernet, loopback, VLAN, pptp, ...)	1 300
CONNECTIVITÉ	
Interfaces 10/100/1000	10-26
Interfaces 1Gb fibre	0-16
Interfaces 10Gb fibre	0-8
Modules d'extension réseau optionnels (8 ports 10/100/1000 / 4 ports 1G Fibre / 4 ports 10G Fibre)	2
SYSTÈME	
Nb max de règles de filtrage	32 768
Nb max de routes statiques	10 240
Nb max de routes dynamiques	500 000
REDONDANCE	
Haute disponibilité (Actif/Passif)	✔
SSD redondants	RAID1
Alimentation redondante (hot swappable)	✔
HARDWARE	
Stockage	128 Go SSD
Option Big Data pour stockage local	> 900 Go SSD
Taille	1U - 19"
Hauteur x Largeur x Profondeur (mm)	44.5 x 443 x 560
Poids	9.6 kg (21.2 lbs)
Hauteur x Largeur x Profondeur emballé (mm)	184 x 710 x 573
Poids emballé	16.6 kg (36.6 lbs)
Alimentation (AC)	110-230V 60-50Hz 5A-3A
Consommation	230V 50Hz 182W 0.99A
Ventilateurs	3
Température de fonctionnement	5° à 40°C (41° à 104°F)
Humidité relative en fonctionnement (sans condensation)	20% à 90% à 40°C
Température de stockage	-30° à 65°C (-22° à 149°F)
Humidité relative de stockage (sans condensation)	5% à 95% à 60°C
CERTIFICATIONS	
Conformité	CE/FCC

Pour une sécurité à haute valeur ajoutée

STORMSHIELD NETWORK VULNERABILITY MANAGER*

Dotez-vous d'un outil de détection de vulnérabilités simple et performant sans impact sur votre système d'information.

Gestion des vulnérabilités
A partir des flux transitant par l'appliance, Stormshield Network Vulnerability Manager inventorie les systèmes d'exploitation, les applications utilisées et leurs vulnérabilités, sur les postes et serveurs. Aussitôt qu'une vulnérabilité est détectée sur votre réseau, vous en êtes averti.

Remédiation (passez à l'action)
Stormshield Network Vulnerability Manager propose un ensemble de rapports dédiés et interactifs, permettant d'appliquer une protection en 1 clic.

STORMSHIELD NETWORK EXTENDED WEB CONTROL*

Contrôlez la navigation Internet de votre entreprise et optimisez la consommation de votre bande passante en déployant une solution de filtrage URL efficace et performante.

Analyse approfondie

Des milliards de requêtes sont analysées par Extended Web Control pour évaluer en permanence le niveau de risque des sites web et permettre le blocage des consultations dès qu'un site infecté ou malveillant est détecté.

Filtrage avancé pour tous

La solution Extended Web Control est activable sur l'ensemble de la gamme Stormshield Network Security. Vous bénéficiez d'une solution de filtrage avancée quelle que soit la taille de votre entreprise.

ANTIVIRUS KASPERSKY*

Protégez-vous en vous dotant de la meilleure solution de protection antivirus.

Bloquer les menaces

La solution antivirale Kaspersky pour les appliances Stormshield Network Security ne repose pas uniquement sur un système à base de signatures de malwares, elle intègre des mécanismes d'émulation pour identifier les codes malveillants de manière proactive.

Protection périmétrique

La technologie antivirale Kaspersky pour les appliances Stormshield Network Security assure une inspection antivirale des flux de tous les équipements connectés au réseau et complète ainsi la protection locale des postes et serveurs.

** Option*

STORMSHIELD

N°Cristal 09 69 32 96 29
APPEL NON SURTAXE

WWW.STORMSHIELD.EU