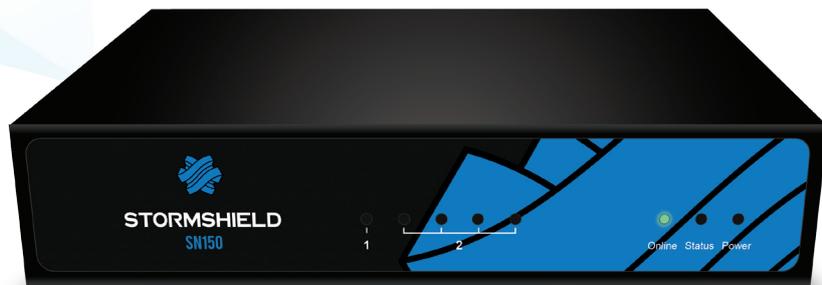




STORMSHIELD



PETITES ENTREPRISES & FILIALES

LA SÉCURITÉ UNIFIÉE

Stormshield SN150

NETWORK SECURITY | ENDPOINT SECURITY | DATA SECURITY

Stormshield SN150

LA SOLUTION DE SÉCURITÉ DÉDIÉE AUX PETITES STRUCTURES (AGENCES, SITES DISTANTS & PETITES ENTREPRISES).



BÉNÉFICIEZ DE LA MEILLEURE SÉCURITÉ UNIFIÉE POUR UN RAPPORT QUALITÉ/PRIX IMBATTABLE

Sans aucun compromis sur la sécurité, le SN150 embarque toutes les fonctions de sécurité nécessaires pour assurer une protection optimale des petites structures informatiques. Une véritable prouesse technologique.



OFFREZ UN ACCÈS EN TOUTE SÉRÉNITÉ AUX RESSOURCES DE VOTRE ENTREPRISE

Avec les fonctionnalités VPN IPsec évoluées, vos filiales et sites distants sont connectés de manière sécurisée et transparente aux ressources informatiques de votre entreprise.



UTILISATION EN MODE UTM OU EN MODE SITE DISTANT

Le SN150 vous apporte une sécurité de bout-en-bout, adaptée à vos usages, grâce à deux packs de maintenance dédiés (*Remote Office Security Pack* pour la protection de sites distants et *Premium UTM Security Pack* pour assurer la sécurité d'un site directement connecté à Internet).



CONFIGUREZ EN 3 MINUTES UNE SÉCURITÉ HAUT NIVEAU, DIGNE DES PLUS GRANDES ORGANISATIONS

Avec des assistants intuitifs, vous êtes guidés étape par étape dans l'installation et la configuration de votre équipement de sécurité.

PETITES STRUCTURES (FILIALES, AGENCES & SITES DISTANTS)

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.

Gagnez du temps

L'interface d'administration des produits Stormshield Network Security a été pensée de façon ergonomique et intuitive afin de vous aider à sécuriser votre entreprise plus rapidement et sans erreur.

Connectez vos collaborateurs

Grâce au réseau privé virtuel (vpn IPsec et SSL), vos collaborateurs disposent d'un accès sécurisé aux ressources de l'entreprise où qu'ils se trouvent et depuis n'importe quels terminaux mobiles.

Maîtrisez votre usage d'internet

Vous pouvez programmer, avec les fonctions de filtrage avancé et à la gestion de la qualité de service, l'utilisation d'internet selon vos besoins.

.....

Spécifications techniques

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), 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, Redondance de liens WAN (jusqu'à 12 liens).

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, External Storage (option).

PERFORMANCES (en Mbps)*

Débit Firewall	400
Débit Firewall + IPS (Paquets de 1518 octets)	200
Débit Firewall + IPS (Fichiers de 1 Mo HTTP)	150

CONNECTIVITÉ RÉSEAU

Nb max de sessions simultanées	30 000
Nb max de dialups	4
VLAN 802.1Q (Max)	64

VPN (en Mbps)

Débit IPsec	80
-------------	----

HAUTE DISPONIBILITÉ

Actif/Passif	-
--------------	---

ANTIVIRUS (en Mbps)

Débit HTTP	30
------------	----

HARDWARE

Interfaces 10/100/1000	1 + 4 ports
MTBF (en années)	12,5
Taille	<0,5U - 19"
Hauteur x Largeur x Profondeur (mm)	37 x 176 x 107
Poids	0.55 kg (1,25 lbs)
Hauteur x Largeur x Profondeur emballé (mm)	78 x 320 x 180
Poids emballé	1.15 kg (2,6 lbs)
Alimentation (AC)	110-240V 60-50Hz 0.6-0.4A
Consommation	230V 50Hz 9W 0.08A
Ventilateur	-
Niveau de bruit	Sans ventilateur
Dissipation thermique (max, BTU/h)	31
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)

CERTIFICATIONS

Conforme aux directives européennes	CE/CEM/ECC
-------------------------------------	------------

Document non contractuel. Les fonctionnalités citées sont celles de la version 1

* Les performances sont mesurées en laboratoire et en conditions idéales pour la version 1. Les résultats peuvent varier en fonction des conditions de test et de la version logicielle.

**En option

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'apppliance, 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.

Remediation (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 quel 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 antivirus 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 antivirus Kaspersky pour les appliances Stormshield Network Security assure une inspection antivirus 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

Netasq

Parc Scientifique Haute Borne - Parc Horizon, Bat 6, Avenue de l'Horizon 59650 Villeneuve d'Ascq

Arkoon-Netasq © Copyright 2014