STORMSHIELD

SOLUTIONS UNIFIED THREAT MANAGEMENT ET NEXT-GENERATION FIREWALLS

SÉCURITÉ RÉSEAU

NETWORK SECURITY | ENDPOINT SECURITY | DATA SECURITY

VISION

FUTURE-READY SECURITY[1]

Parce qu'une solution de sécurité représente un investissement de plusieurs années, les produits Stormshield Network Security vous offrent la modularité et les fonctionnalités nécessaires pour **accompagner les futures évolutions** du système d'information.

SEAMLESS SECURITY[2]

Dans un monde du « Bring-Your-Own-Everything », il est de plus en plus difficile de contraindre les utilisateurs si l'on veut **développer une entreprise agile et en phase avec son temps**. Pour que la sécurité soit efficace, elle se doit d'être transparente pour les utilisateurs et les administrateurs.

COLLABORATIVE SECURITY[3]

Devant les menaces modernes qui contournent de façon triviale les systèmes de protection traditionnels, une nouvelle approche de la sécurité est nécessaire.

Les solutions Stormshield Network Security reposent sur le concept de « Multi-layer Collaborative Security ». Ce modèle holistique, basé sur **une collaboration active entre les moteurs de sécurité de nos différentes solutions** constitue le futur de la défense en profondeur des systèmes d'information.

TRUSTED SECURITY[4]

En tant qu'acteurs de confiance, Arkoon et Netasq délivrent **des technologies certifiées au plus haut niveau européen** (EU RESTRICTED, OTAN RESTRICTED, EAL4+, QUALIFICATION ANSSI). Les certifications et qualifications obtenues garantissent un niveau de protection adapté pour les informations stratégiques des sociétés et organisations les plus sensibles.

[1] Sécurité prête pour le futur / [2] Sécurité transparente / [3] Sécurité collaborative / [4] Sécurité de confiance

UNE GAMME COMPLÈTE

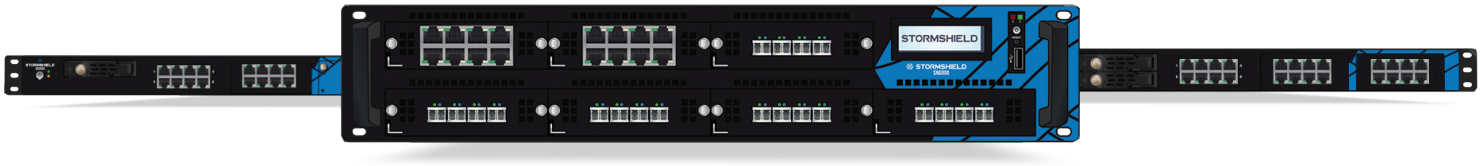
SN300 SN150 SN200

SÉCURITÉ UNIFIÉE

SN510 SN910 SN710

CONTINUITÉ BUSINESS DANS DES ARCHITECTURES COMPLEXES

SN2000 SN6000 SN3000



FLEXIBILITÉ & PERFORMANCE POUR INFRASTRUCTURES CRITIQUES

ÉGALEMENT

SÉCURITÉ RENFORCÉE POUR LES ENVIRONNEMENTS VIRTUALISÉS

Beaucoup d'organisations ont choisi la virtualisation à la fois pour rationaliser leur infrastructure IT et pour bénéficier d'une technologie qui offre une importante réduction du coût total de possession (TCO), une exploitation plus simple, une capacité d'évolution plus importante et une restauration plus rapide en cas de sinistre.

Pour accompagner ce choix, les appliances virtuelles Stormshield Network Security offrent le même niveau de protection et la même richesse fonctionnelle que les produits physiques de la gamme.

SOLUTIONS CLOUD-BASED

Pour permettre aux entreprises de déployer une infrastructure virtuelle dans le Cloud de façon maîtrisée et sécurisée, toute la richesse fonctionnelle des solutions Stormshield Network Security est disponible dans l'application Stormshield Network Cloud UTM, dédiée aux environnements Amazon Web Services.

- Protection efficace des serveurs, web services et applications virtualisés au sein d'un Cloud Amazon Web Services
- Mise en œuvre simplifiée via le Marketplace Amazon Web Services

ASSUREZ LA CONTINUITÉ DE VOTRE ACTIVITÉ

Les nouvelles appliances Stormshield Network Security sont le résultat de la combinaison des technologies Arkoon et Netasq. Nos expériences et références acquises dans les environnements sensibles et à fortes contraintes technologiques sont un gage de sérénité pour les organisations de toutes tailles.

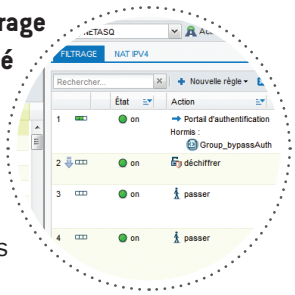
L'ensemble de la gamme **intègre toutes les technologies de protection pour répondre aux attaques les plus sophistiquées**.

Le moteur de prévention d'intrusion (IPS) de Stormshield Network Security combine des bases ciblées réactives et des analyses proactives pour détecter les attaques connues et inconnues.

MAÎTRISEZ VOTRE USAGE D'INTERNET

Internet est une source d'information et d'applications incontournable dont l'accès doit être maîtrisé.

Grâce aux fonctions de filtrage avancé et à la gestion de qualité de service, il est possible de définir l'utilisation d'Internet souhaitée et d'analyser les sites Web consultés, y compris les sites chiffrés ou basés sur des technologies Web2.0.



CONNECTEZ VOS COLLABORATEURS

L'évolution des comportements, la complexification des organisations ou la pression concurrentielle obligent les entreprises et leurs collaborateurs à développer leur agilité. La mobilité, le télétravail, l'utilisation professionnelle de terminaux mobiles personnels sont autant de nouveaux enjeux qu'il faut pouvoir traiter avec sérénité.

Grâce au réseau privé virtuel (VPN IPSec et SSL), les collaborateurs disposent d'**un accès sécurisé aux ressources de l'entreprise où qu'ils se trouvent et depuis n'importe quel terminal.** La fonction VPN SSL est particulièrement adaptée au BYOD.

GAGNEZ DU TEMPS

La configuration d'un équipement de sécurité est une opération cruciale qui doit être à la fois simple et complète. 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 rapidement et sans erreur**.

GÉREZ LES VULNÉRABILITÉS

Les vulnérabilités des postes et serveurs sont une porte ouverte pour les menaces avancées qui tentent de s'introduire sur le système d'information. Stormshield possède la seule technologie efficace de détection des vulnérabilités réseaux et applicatives intégrée à une solution firewall/UTM : Stormshield Network Vulnerability Manager.

Grâce à une analyse du trafic réseau, Les **applications obsolètes ou vulnérables sur les postes et serveurs sont détectées en temps réel** et une protection adaptée peut être appliquée en un clic.

RESPECTEZ VOS ENGAGEMENTS DE CONFORMITÉ

Les produits Stormshield Network Security sont un composant clé **pour assurer la conformité aux standards, réglementations et normes** qui imposent un contrôle des accès (PCI-DSS, ISO 27001 ou loi Informatique et Libertés, etc.).

QUE DIT LA LOI ?

Le chef d'entreprise est responsable de la sécurisation des données personnelles (article 34 de la loi informatique et liberté) et risque jusqu'à 300 000 euros d'amende et 5 ans d'emprisonnement (art. 226-17 du Code Pénal) en cas de non-respect de la législation.

Il a également obligation d'empêcher toute utilisation illicite de son réseau par ses employés ou par des personnes externes (art 323 CP).

La gamme de solutions Stormshield Network Security vous aide à respecter ces obligations vis-à-vis de la loi française.

Spécifications des solutions matérielles

	Petites entreprises, Agences, Filiales			Moyennes organisations, Agences			Grandes organisations, Datacenters		
	SN150	SN200	SN300	SN510	SN710	SN910	SN2000	SN3000	SN6000
PERFORMANCES*									
Débit Firewall (UDP 1518 octets)	400 Mbps	600 Mbps	800 Mbps	5 Gbps	10 Gbps	20 Gbps	30 Gbps	50 Gbps	130 Gbps
Débit IPS (UDP 1518 octets)	200 Mbps	600 Mbps	800 Mbps	3 Gbps	7 Gbps	12,5 Gbps	20 Gbps	30 Gbps	55 Gbps
Débit IPS (1 Mo HTTP)	150 Mbps	600 Mbps	800 Mbps	1,7 Gbps	2,6 Gbps	7 Gbps	12 Gbps	14 Gbps	17 Gbps
Débit Antivirus	55 Mbps	165 Mbps	200 Mbps	850 Mbps	1,6 Gbps	2,2 Gbps	3,2 Gbps	4 Gbps	4,7 Gbps
CONNECTIVITÉ RÉSEAU									
Nb max. de sessions simultanées	30 000	75 000	150 000	500 000	1 000 000	1 500 000	2 000 000	2 500 000	10 000 000
Nb de nouvelles sessions par sec.	2 500	15 000	18 000	20 000	40 000	60 000	90 000	120 000	180 000
VPN*									
Débit IPSec (AES128 – SHA1)	100 Mbps	250 Mbps	400 Mbps	1 Gbps	2,4 Gbps	4 Gbps	5 Gbps	6,5 Gbps	12 Gbps
Nb max. de tunnels VPN IPSec	25	50	100	500	1 000	1 000	5 000	5 000	10 000
Nb de clients VPN SSL simultanés	5	20	20	100	150	150	200	500	500
HAUTE DISPONIBILITÉ									
Actif/Passif	-	-	✔	✔	✔	✔	✔	✔	✔
CONNECTIVITÉ									
Interfaces 10/100/1000	1 + 4 ports (switch)	1 + 2x2 ports	8	12	8-16	8-16	10-26	10-26	10-58
Interfaces fibre 1Gb	-	-	-	-	0-4	0-6	0-16	0-16	0-56
Interfaces fibre 10Gb	-	-	-	-	0-2	0-2	0-8	0-8	0-28
HARDWARE									
Redondance (SSD, Alimentation)	-	-	-	-	-	-	-	✔	✔
Stockage local	-	SD Card**	SD Card**	320 GB	320 GB	128 GB SSD	128 GB SSD	128 GB SSD	256 GB SSD
Taille	<0,5U - 19"	0,5U - 19"	0,5U - 19"	1U - 19"	1U - 19"	1U - 19"	1U - 19"	1U - 19"	2U - 19"

Contrôle des usages
Mode Firewall/IPS/IDS, Firewall basé sur l'identité des utilisateurs, Firewall applicatif, Microsoft Services Firewall, Détection et contrôle de l'usage des terminaux mobiles, Inventaire des applications, Détection des vulnérabilités, Filtrage d'URLs (base embarquée ou mode Cloud), Authentification transparente (Agent SSO Active Directory, SSL, SPNEGO), Authentification multi-user en mode cookie (Citrix- TSE), Politique de sécurité globale/locale.

Protection contre les menaces
Prévention d'intrusion, Analyse protocolaire, Inspection applicative, Protection contre les dénis de service (DoS), 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'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, 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, Routage dynamique (RIP, OSPF, BGP), Gestion de PKI interne ou externe multi-niveau, Annuaire LDAP interne, Proxy explicite, Routage par politique (PBR), Gestion de la qualité de service, Client/relai/serveur DHCP, Client NTP, Proxy-cache DNS, Proxy-cache HTTP, Haute Disponibilité, 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, compteurs d'utilisation des règles firewall, plus de 15 assistants d'installation, outils de reporting et d'analyse de logs embarqués, Rapports interactifs et personnalisables, envoi des traces en syslog, Agent SNMP v1, v2, v3, Sauvegarde automatisée des configurations, stockage externe (option).

Spécifications des solutions virtualisées

	For Network[1]					For Cloud[2]	
CARACTÉRISTIQUES	V50	V100	V200	V500	VU	VS5	VS10
Adresses IP protégées	50	100	200	500	Illimité	-	-
Machines virtuelles protégées	-	-	-	-	Illimité	5	10
Vulnerability Manager	-	-	-	-	-	Oui	Oui
Connexions simultanées	100 000	200 000	400 000	600 000	3 000 000	1 000 000	2 000 000
Nb max de Vlan	128	128	128	128	512	512	512
Nb max de tunnels VPN IPSec	100	500	1 000	1 000	10 000	10 000	10 000
Nb de clients VPN SSL simultanés	20	35	70	175	500	500	500

* 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.
** En option
[1] Pour réseau / [2] Pour Cloud

CLOUD SERVICES

CLOUD REPORTING

Service clé en main de génération de rapports automatisés

Sans aucun investissement matériel ou humain, vous disposez de rapports périodiques complets avec des indicateurs détaillés sur l'activité de votre réseau et des utilisateurs. Disposant ainsi d'une vue synthétique des événements, vous pilotez et améliorez votre sécurité sans contraintes.

CLOUD BACKUP

Service de sauvegarde automatique de configurations

Ce service gratuit vous permet de sauvegarder automatiquement, dans l'infrastructure Cloud Stormshield ou sur un de vos serveurs, les dernières configurations de vos appliances Stormshield Network Security. Ainsi vous pourrez facilement récupérer et restaurer une configuration précédente en cas de réinitialisation, d'échange matériel ou d'erreur.

CLOUD UPDATE

Mises à jour automatiques

Le service Cloud Update met à jour automatiquement :

- les signatures contextuelles pour le moteur de prévention d'intrusion
- les applications
- la base de vulnérabilités
- les bases de filtrage URL
- les signatures antivirus
- les serveurs RBL et les whitelists antispam
- les versions mineures et majeures

SERVICES

PACKS DE SERVICES

Une indisponibilité prolongée de votre équipement de sécurité pourrait avoir des conséquences catastrophiques sur l'activité de votre entreprise. Stormshield propose une offre simple et claire avec 4 packs de services de sécurité intégrant la maintenance matérielle de votre produit.

SUPPORT TECHNIQUE

Vous bénéficiez, par le biais de votre partenaire, de l'aide de nos équipes de support technique multi-langues. Ces équipes sont basées dans nos locaux, au plus proche des équipes R&D, pour une collaboration étroite et directe. C'est pour vous la garantie de l'expertise Constructeur.

FORMATIONS

Proposées par Stormshield ou par un de ses partenaires certifiés et agréés, nos formations Administrateur et Expert vous permettent d'acquérir une maîtrise complète de nos produits. Enrichies sur de nombreux travaux pratiques, elles sont valorisées par une certification reconnue sur le marché.

STORMSHIELD

Arkoon et Netasq, filiales à 100% d'Airbus Defence and Space CyberSecurity, opèrent la marque Stormshield et proposent des solutions de sécurité de bout-en-bout innovantes pour protéger les réseaux (Stormshield Network Security), les postes de travail (Stormshield Endpoint Security) et les données (Stormshield Data Security).

WWW.STORMSHIELD.EU