



STORMSHIELD

STORMSHIELD NETWORK VS5 & VS10

APPLIANCES VIRTUELLES POUR SERVEURS

VIRTUAL APPLIANCES FOR CLOUD

Les points clés

- ▶ Pas de coût initial pour un retour sur investissement rapide (ROI)
- ▶ Protection IPS éprouvée et détections de vulnérabilités
- ▶ Adaptée aux solutions des leaders du marché de la virtualisation
- ▶ Solution évolutive



Pour rivaliser sur le marché actuel, les sociétés développent de plus en plus de services web et d'applications supportant des opérations 24/7. Le niveau d'investissement atteint pour cette croissance incontrôlée n'étant plus acceptable, les responsables informatiques voient la virtualisation comme une solution intéressante pour réduire sensiblement les coûts de leur infrastructure serveur.

Pourtant, du point de vue de la sécurité, la virtualisation n'est pas synonyme d'avantages. En supprimant complètement la séparation physique traditionnelle en différentes zones de confiance pour les serveurs privés et publics, la virtualisation apparaît comme une arme à double tranchant. Dans leur effort pour rendre l'utilisation du matériel plus simple, plus cohérente et plus agile, les sociétés oublient souvent que les actifs virtuels sont tout aussi vulnérables que leurs équivalents physiques.

La solution la plus efficace pour surveiller la communication entre les serveurs virtuels fonctionnant sur le même matériel physique consiste à installer une appliance virtuelle qui regroupe les fonctionnalités firewall et IPS. L'appliance virtuelle Stormshield pour les serveurs est la solution pour protéger une DMZ virtuelle.

LA PROTECTION DE VOTRE DMZ VIRTUELLE

Comme les environnements physiques, les réseaux virtuels peuvent être victimes d'attaques sur la bande passante, de DoS, de virus et d'exploits. Ces menaces compromettent la disponibilité du réseau ainsi que la productivité des employés. Pour utiliser au mieux la virtualisation en réduisant les risques, les sociétés n'ont pas seulement besoin d'une protection en temps réel contre les menaces actuelles et futures, mais aussi de retrouver une visibilité et un contrôle complets des failles applicatives sur les différents serveurs virtuels.

Intégré au cœur du système d'exploitation, le moteur de prévention d'intrusion breveté de Stormshield fournit une analyse protocolaire et comportementale en temps réel du flux de données. Notre architecture unique intègre un IPS ainsi que toutes les fonctionnalités d'une solution tout-en-un (UTM); une valeur ajoutée supplémentaire dont les entreprises peuvent bénéficier en cas de besoin. De plus, les appliances VS5 et VS10 supportent la segmentation transparente des réseaux, une politique de sécurité intuitive basée sur l'utilisateur et protègent les données provenant des tunnels IPSec ou VPN SSL sécurisés en scannant en amont le trafic généré via des connexions distantes.

En plus des protections certifiées EAL 4+ testées et approuvées pour votre trafic données et voix, les appliances virtuelles Stormshield pour serveurs intègrent un

À PROPOS

Arkoon et Netasq, filiales à 100% d'Airbus Defence and Space CyberSecurity, opèrent sous la marque Stormshield et proposent tant en France qu'à l'international 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

Téléphone



Page de contact email



Document non contractuel. Afin d'améliorer la qualité de ses produits, Arkoon et Netasq se réserve le droit d'effectuer des modifications sans préavis.

Toutes marques sont la propriété de leurs sociétés respectives.

module de détection en temps réel des vulnérabilités sans coût supplémentaire. Cette solution offre une évaluation en temps réel des menaces qui affectent vos serveurs virtuels ainsi que les informations utiles sur l'emplacement des patches et des mises à jour afin de les corriger.

Les appliances virtuelles Stormshield pour serveurs sont compatibles avec VMware VSphere™ et Citrix XenServer™. Grâce au format de l'appliance virtuelle, le processus d'installation/restauration est extrêmement simple et permet une grande portabilité.

UN BUDGET CONTROLÉ

Parce que toutes les entreprises doivent prendre en compte le rapport qualité/prix de la sécurité informatique, Stormshield a souhaité contribuer à la protection des serveurs virtuels en donnant accès aux solutions VS5 et VS10 sans frais de mise en service.

Pour bénéficier de la gamme complète de fonctions de sécurité et de l'évaluation des vulnérabilités proposées par les appliances virtuelles Stormshield pour serveurs, il suffit aux entreprises de souscrire aux services de maintenance et aux mises à jour du système et des protections. Les avantages d'un abonnement annuel sont évidents : contrôle total des coûts, retour sur investissement rapide pour une protection de pointe.

Les appliances virtuelles Stormshield pour serveurs offrent une protection "future ready", en sécurisant votre réseau, votre productivité et votre budget.

SPÉCIFICATIONS TECHNIQUES

	VS5	VS10
Machines virtuelles protégées	5	10
Vulnerability Manager	Oui	Oui
Connexions simultanées	1 000 000	2 000 000
Nb max de Vlan	512	512
Nb max de tunnels VPN IPSec	10 000	10 000
Nb de clients VPN SSL simultanés	500	500

FIREWALL UTILISATEUR

Base de données interne (LDAP)
Authentification par un tiers - LDAP, Active Directory, Radius, NTLM
Authentification transparente - Microsoft SPNEGO - Certificat SSL - Agent SSO

FIREWALL MULTIFONCTION - UTM

Proxies SMTP, POP3, HTTP, FTP
Antivirus, antispyware intégrés
Antispam par réputation (DNS RBL)
Antispam avec analyses heuristiques
VPN IPSec
VPN SSL
Stormshield Extended Web Control 65 catégories (Option)

IPS - FIREWALL APPLICATIF

Vérification en temps réel de la politique de sécurité
Programmation horaire de politiques
Quarantaine automatique en cas d'attaques

Protection contre les attaques de type flooding
Protection contre l'évasion de données
Gestion avancée de la fragmentation
Protection contre les SQL injections
Protection contre les Cross Site Scripting (XSS)
Détection de chevaux de Troie
Protection contre l'hijacking de sessions
Analyses applicatives dédiées (plugins) : IP, TCP, UDP, HTTP, FTP, SIP, RTP/RTCP, H323, DNS, SMTP, POP3, IMAP4, NNTP, SSL, MGCP, Edonkey, SSH, Telnet ...

SERVICES RÉSEAU

Client et serveur DHCP
Client NTP
Proxy cache DNS

RÉSEAU - ROUTAGE - QUALITÉ DE SERVICE

Mode transparent, routé et hybride

Translation d'adresses (NAT, PAT, split)
Routage statique - Routage par politique
Routage dynamique
Garantie et limitation de bande passante
Gestion de bande passante par priorité

MANAGEMENT

Administration par rôles
Stormshield Unified Manager
Stormshield Real-Time Monitor
Stormshield Event Reporter ssh v2

MONITORING - REPORTING

Serveurs syslog (max 3)
Alertes e-mail
Génération automatique de rapports interactifs
Agent SNMP v1, v2, v3 (DES, AES)