STORMSHIELD

STORMSHIELD NETWORK VU (Illimité)

APPLIANCE VIRTUELLE POUR LES GRANDES ENTREPRISES

VIRTUAL APPLIANCES FOR NETWORK

Les avantages clés

- Solution éprouvée, certifiée EAL4+
- Licence IP et utilisateurs illimités
- Sécurité à la demande : pas de coût initial
- Adaptée aux solutions des leaders du marché de la virtualisation
- Prévention d'intrusion proactive Zero-day
- En phase avec les valeurs écologiques (Green IT)

De nombreuses entreprises choisissent la virtualisation comme un moyen de consolider leurs principaux centres de données. Il est essentiel pour ces entreprises de s'assurer que les nouvelles architectures virtuelles ne souffrent d'aucune dégradation au niveau de la protection dont elles disposent.

Les entreprises choisissent la virtualisation à la fois pour apporter une cohérence à leur infrastructure IT et pour bénéficier d'une technologie qui offre une importante réduction du coût total de possession (TCO), une exploitation plus simple, la répartition de charge, la portabilité du serveur et une récupération immédiate en cas d'incident.

Des pratiques inadaptées en matière de sécurité peuvent cependant réduire à néant les bienfaits de la virtualisation. En effet, l'inconvénient avec cette technologie est qu'il devient très facile de connecter directement des machines ayant des niveaux de confidentialité différents. Le fait que les appliances IPS/IDS traditionnelles soient inutiles dans un environnement complètement virtualisé, une fois le réseau physique protégé, est un facteur aggravant.

Les entreprises doivent maintenir la qualité de la sécurité pour les environnements qui hébergent leurs applications métiers et leur informations sensibles, qu'ils soient hébergés physiquement ou virtualisés.

UNE VIRTUALISATION SÉCURISÉE

En partageant la même plate-forme matérielle pour l'hébergement des systèmes d'exploitation, des logiciels CRM/ERP ainsi que pour tous les services installés dans la DMZ, tous les services peuvent être affectés par l'apparition d'une seule vulnérabilité. C'est pourquoi la virtualisation soulève de nouveaux défis pour la protection des informations critiques de l'entreprise.

Afin de protéger correctement ces architectures multi-couches, les entreprises ont besoin d'une solution de sécurité virtuelle mature, permettant de gérer de façon globale les nombreux dispositifs de sécurité physiques et virtuels. Elles ont également besoin d'un support pour les migrations régulières des topologies maillées, la segmentation du réseau et une protection optimale de la communication intersites. L'appliance virtuelle Stormshield pour les entreprises est la solution qui répond à toutes ces attentes.

Intégré au cœur du système, le moteur de prévention d'intrusion breveté de Stormshield fournit une analyse protocolaire et comportementale en temps réel du flux

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

N°Cristal 09 69 32 96 29
APPEL NON SURTAXE

Page de contact email

*nécessite un abonnement

de données. Il allie plusieurs technologies pour garantir en amont une protection contre les milliers de menaces actuelles et futures.

L'appliance virtuelle Stormshield pour les grandes entreprises intègre une interface de gestion intuitive et efficace. La configuration de chaque profil de sécurité et le monitoring complet du réseau sont paramétrés de sorte que l'équipe de sécurité puisse garder le contrôle du réseau de l'entreprise. Certifiée EAL4+, testée et approuvée, notre appliance virtuelle intègre, au besoin, toutes les fonctionnalités attendues d'une solution de sécurité tout-en-un (UTM). L'entreprise peut également bénéficier d'un moteur d'évaluation des vulnérabilités en temps réel* qui réduit considérablement les risques pour les architectures sensibles.

Enfin, l'appliance virtuelle Stormshield contribue à sécuriser la mobilité en offrant une analyse en amont du flux de données provenant des tunnels IPSec ou VPN SSL sécurisés.

LA SÉCURITE À LA DEMANDE

Un des objectifs de la virtualisation est la réduction massive des coûts d'infrastructure. C'est la raison pour laquelle l'appliance virtuelle Stormshield pour les grandes entreprises est proposée à la demande, sans coût initial.

Pour bénéficier de la gamme complète de fonctions de sécurité proposées par les appliances virtuelles Stormshield pour les grandes entreprises, il leur suffit de s'abonner pour un an aux services et aux mises à jour du système et des protections. L'approche « à la demande » présente plusieurs avantages, notamment le contrôle total annuel des coûts et un retour sur investissement rapide pour une protection de pointe.

L'appliance virtuelle Stormshield pour les entreprises offre une sécurité éprouvée et proactive face aux futures menaces, garantissant aux grandes entreprises mondiales une véritable protection contre les menaces internes et externes. Cette solution sécurise à la fois la performance de leur réseau virtuel et la productivité des employés.

SPÉCIFICATIONS TECHNIQUES

	VU
Adresses IP protégées	Illimité
Machines virtuelles protégées	Illimité
Connexions simultanées	3 000 000
Nb max de Vlan	512
Nb max de tunnels VPN IPSec	10 000
Nb de clients VPN SSL simultanés	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)

OPTION
Gestion des risques avec Stormshield Vulnerability Manager

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