FICHE TECHNIQUE

FIREBOX V

Sécurité réseau de pointe pour votre environnement virtuel

Les entreprises de toutes tailles se tournent vers la virtualisation pour réduire les coûts et renforcer l'efficacité, la disponibilité et la flexibilité de leurs ressources informatiques. Mais la virtualisation a son coût. Les environnements virtuels sont complexes à gérer et vulnérables face aux menaces de sécurité. Les services informatiques doivent se tenir prêts. Aujourd'hui, les applications peuvent être sécurisées, les ressources maximisées et votre service informatique peut bénéficier des avantages d'un système de gestion unique et unifié et ce, sans courir le moindre risque de sécurité. WatchGuard FireboxV offre une sécurité réseau de pointe au monde de la virtualisation. Grâce à la surveillance en temps réel, à la prise en charge multi-WAN et à des solutions évolutives capables de s'adapter aux entreprises de toutes tailles, vos environnements virtuels sont tout aussi sécurisés que votre environnement physique.

Les solutions virtuelles de WatchGuard offrent une flexibilité de déploiement inégalée. Vous pouvez choisir de déployer une combinaison d'appliances matérielles et virtuelles, fonctionnant conjointement et gérées depuis une plateforme de gestion centralisée commune. Offrant tous les services de sécurité et réseau présents dans les appliances physiques, les appliances virtuelles WatchGuard peuvent être déployées par client, par service ou par application pour votre infrastructure virtuelle.

VIRTUALISEZ LE PARE-FEU DE PASSERELLE TRADITIONNEL POUR UNE FLEXIBILITÉ SANS PRÉCÉDENT

WatchGuard FireboxV protège non seulement le périmètre physique du datacenter, mais également la « périphérie virtuelle ». Désormais, vous pouvez aisément mettre en œuvre une politique qui isole les données de la base de données d'entreprise, de l'infrastructure de messagerie ou bien les informations RH confidentielles des données financières d'autres divisions, et ce, même lorsqu'elles résident sur les mêmes serveurs.

CONSOLIDEZ PLUSIEURS PARE-FEU POUR UN GAIN CONSIDÉRABLE EN EFFICACITÉ

Les fournisseurs de services (d'hébergement, de Cloud ou de sécurité managés) peuvent déployer plusieurs instances de FireboxV sur des serveurs situés sur le périmètre de leurs datacenters. Ces pare-feu virtuels sont isolés les uns des autres, de sorte que les accords de niveau de service (SLA) peuvent être garantis pour chaque client, et que les changements de configuration de l'un n'affecte pas les autres. Or, ils peuvent tous être gérés par le fournisseur à l'aide d'une seule et même console intuitive.

ÉLIMINEZ LES COÛTS MATÉRIELS REDONDANTS TOUT EN SÉCURISANT LES RÉSEAUX VIRTUELS – CONSOLIDATION DES FILIALES

Alors que les filiales et divisions de taille importante consolident leurs serveurs locaux (fichiers, impression, voix, etc.) en un seul dispositif, un pare-feu virtuel peut être déployé sur le serveur physique, isolant tout le trafic de l'Internet public. Un tunnel VPN unique peut offrir un accès sécurisé aux datacenters d'entreprise ou Clouds privés virtuels, générant ainsi d'importantes économies au niveau de chaque site sans le moindre compromis sur la sécurité.

FONCTIONNALITÉS ET AVANTAGES

- Exécution d'appliances virtuelles sur votre environnement virtuel
- Fonctionnalités et services UTM/NGFW de pointe dans l'infrastructure virtuelle
- WatchGuard Dimension™ est une solution de visibilité sur Cloud public et privé qui transforme instantanément les données brutes en renseignements de sécurité exploitables, incluse avec l'achat
- Facile à télécharger, activer, déployer et gérer (console centralisée, interface utilisateur Web, interface de ligne de commande)
- Exploitation de la flexibilité et de la disponibilité de vSphere et Hyper-V
- Plusieurs modèles pour les entreprises de toutes tailles
- Consolidation des campus, du Cloud/de l'hébergement, des filiales
- Déploiement par client, par service ou par application

Nom du modèle	Limite de cœurs de processeur	Nombre d'utilisateurs	Agents Host Sensor TDR	Pare-feu (Mbit/s)	VPN (Mbit/s)	Utilisateurs VPN
Small	2	50	50	2 000	400	50
Medium	4	250	150	4 000	1 500	600
Large	8	750	250	8 000	3 000	6 000
XLarge	16	1 500	250	Illimité	Illimité	10 000

FONCTIONS DE SÉCURITÉ

Pare-feu	Inspection dynamique des paquets, inspection au niveau de la couche applicative, pare-feu proxy
Proxies applicatifs	HTTP, HTTPS, FTP, DNS, TCP/UDP, POP3, POP3S, SMTP, IMAPS, and Explicit Proxy
Protection contre les menaces	Attaques de dénis de service (DoS), paquets fragmentés, menaces mixtes, etc.
Options de filtrage	Recherche Internet sécurisée, YouTube pour les établissements scolaires, Google pour les entreprises
Abonnements de sécurité	APT Blocker, IPS, Gateway AV (antivirus de passerelle), WebBlocker (filtrage d'URL), contrôle d'application, Data Loss Prevention (DLP, Prévention des fuites de données), Autorité de réputation (Reputation Enabled Defense), spamBlocker (antispam), Network Discovery (Découverte réseau), Threat Detection and Response, Access Portal

GESTION

Journalisation et notifications	WatchGuard, Syslog, SNMP v2/v3
Interfaces utilisateur	Interface utilisateur Web, interface de ligne de commande contrôlable par script
Création de rapports	WatchGuard Dimension propose plus de 100 rapports prédéfinis, ainsi que des outils de synthèse et de visibilité

FONCTIONS RÉSEAU

QoS	8 files d'attente prioritaires, DiffServ, file d'attente stricte modifiée
Attribution d'adresses IP	DHCP (client)
NAT	Statique, dynamique, 1:1, IPSec Traversal
Autres fonctionnalités	Routage statique, indépendance des ports

VPN ET AUTHENTIFICATION

Chiffrement	DES, 3DES, AES 128, 192 et 256 bits
IPSec	SHA-2, clé IKE pré-partagée, certificat tiers, IKE v1/v2, Suite B
SSO (authentification unique)	Systèmes d'exploitation mobiles, Windows, Mac OS X, RADIUS, SAML 2.0
Authentification	RADIUS, LDAP, Windows Active Directory, RSA SecurID, base de données interne, SAML 2.0

SÉCURITÉ RENFORCÉE À CHAQUE NIVEAU

Avec leur architecture unique qui les place au rang de produits de sécurité réseau les plus avancés, les plus rapides et les plus efficaces du marché, les solutions de WatchGuard offrent une protection complète contre les logiciels malveillants avancés, les ransomwares, les botnets, les chevaux de Troie, les virus, les téléchargements intempestifs (« drive-by downloads »), les pertes de données, l'hameçonnage, etc.

Fonctionnalités et services	TOTAL SECURITY SUITE	Basic Security Suite
Service de prévention d'intrusions (IPS)	✓	✓
Contrôle d'application	✓	✓
WebBlocker (filtrage d'URL)	✓	✓
spamBlocker (antispam)	✓	✓
Gateway AntiVirus (Antivirus de passerelle)	✓	✓
Reputation Enabled Defense (RED, Autorité de réputation)	✓	✓
Network Discovery (Découverte réseau)	✓	✓
APT Blocker	✓	
Protection contre les pertes de données (Data Loss Protection, DLP)	✓	
Threat Detection and Response	✓	
DNSWatch	✓	
Access Portal	✓	
IntelligentAV	✓	
Dimension Command	✓	
Support	**Gold (24 h/24, 7 j/7)**	Standard (24 h/24, 7 j/7)

PLUSIEURS OPTIONS D'ACHAT

La souplesse de la plateforme intégrée de WatchGuard permet de sélectionner exactement les composants de sécurité qui correspondent aux besoins de votre réseau d'entreprise. Que vous décidiez de mettre en place un premier niveau de sécurité ou de déployer un arsenal complet de protection réseau, nous avons regroupé les services de sécurité pour répondre à vos exigences.

CONSEILS ET ASSISTANCE D'EXPERTS

Un abonnement initial au service de support standard est inclus avec chaque modèle Firebox. Le service de support standard, inclus dans la Basic Security Suite, comprend une assistance technique 24 h/24 et 7 j/7 et les mises à jour logicielles. Une mise à niveau vers le service de support Gold est incluse dans la Total Security Suite de WatchGuard.

Pour plus d'informations, contactez votre intégrateur WatchGuard agréé ou rendez-vous sur le site www.watchguard.com.