FICHE TECHNIQUE

FIREBOX CLOUD

Étendre le périmètre de sécurité WatchGuard au Cloud public

C'est un fait : les entreprises sont en train de migrer les services depuis les serveurs sur site vers le Cloud. Les serveurs de messagerie, les serveurs Web, les systèmes de gestion de la relation client (CRM) et le stockage des fichiers migrent vers des services Cloud. Avec une telle quantité de données sensibles déplacées vers le Cloud, la sécurité est primordiale. Firebox Cloud de WatchGuard permet aux administrateurs réseau d'étendre leur périmètre de sécurité afin de protéger les serveurs exécutés sur des environnements Cloud publics.

Alors que les fournisseurs de services Cloud sont responsables de la sécurité du Cloud, la protection de vos données sensibles lors de leur transfert vers et depuis le Cloud est de votre responsabilité. Dans ce modèle de responsabilité partagée, il est essentiel que les administrateurs prennent toutes les mesures possibles pour protéger leurs données et repousser les cyber-criminels. WatchGuard Firebox Cloud apporte la protection des appliances UTM Firebox® primées de WatchGuard aux environnements Cloud publics. L'appliance Firebox Cloud peut rapidement et aisément être déployée pour protéger les serveurs dans un Cloud public contre les attaques telles que les botnets, les scripts intersites, les tentatives d'injection SQL, et autres vecteurs d'attaque.

CRÉÉE POUR L'ENVIRONNEMENT CLOUD

Contrairement à de nombreux services UTM dans le Cloud, l'appliance Firebox Cloud de WatchGuard a été conçue spécialement pour s'exécuter dans chaque environnement Cloud et fournit une interface utilisateur rationalisée qui supprime les éléments non pertinents. Firebox Cloud simplifie également le processus de création de connexions sécurisées vers votre environnement Cloud public en activant des tunnels VPN « de WatchGuard à WatchGuard ».

EXTENSION DU PÉRIMÈTRE DE SÉCURITÉ WATCHGUARD

Les TPE/PME et les entreprises multisites exécutant une partie de leur infrastructure dans le Cloud peuvent rationaliser leurs efforts de configuration et de maintenance en étendant leur périmètre de sécurité avec Firebox Cloud. La combinaison de Firebox Cloud avec les appliances Firebox physiques évite la nécessité de se familiariser avec une autre gamme de produits pour protéger un Cloud privé virtuel (VPC).

VISIBILITÉ SUR LE BIG DATA

WatchGuard Firebox Cloud est entièrement compatible avec WatchGuard Dimension, une solution Cloud de visibilité sur la sécurité réseau qui est incluse de série dans le produit phare de WatchGuard, sa plateforme de gestion unifiée des menaces (UTM) et de pare-feu de prochaine génération. Dimension offre une suite de puissants outils de visibilité « Big Data » et de génération de rapports qui permettent d'identifier et de consolider instantanément les problèmes et tendances de sécurité majeurs, ainsi que de fournir des informations exploitables pour définir des stratégies de sécurité efficaces pour l'ensemble de vos environnements.

PLUSIEURS OPTIONS D'ACHAT

Pour obtenir et utiliser rapidement et facilement votre instance Firebox Cloud, WatchGuard propose plusieurs options d'achat. Vous pouvez acheter une licence BYOL (Bring-Your-Own-License) auprès d'un partenaire WatchGuard de confiance afin de bénéficier de ses compétences et de son expertise. Il est également possible d'acheter une instance mesurée (par ex., paiement à l'heure) directement disponible sur le marché.

FONCTIONNALITÉS ET AVANTAGES

- Déploiement simple et rapide de VPC pour se protéger contre les attaques telles que les botnets, les scripts intersites, les tentatives d'injection SQL, et autres vecteurs d'attaque.
- Gain de temps grâce à une interface utilisateur rationalisée conçue pour chaque plateforme Cloud.
- Simplification du processus de création de connexions sécurisées vers votre environnement Cloud public.
- Meilleure visibilité réseau grâce à la solution de visibilité réseau primée de WatchGuard, Dimension.
- Plusieurs options d'achat adaptées à votre utilisation.

FIREBOX CLOUD

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	250	4 000	1 500	600
Large	8	750	250	8 000	3 000	6 000
XLarge	16	1 500	250	Illimité	Illimité	10 000

REMARQUE : Les valeurs des spécifications s'appliquent uniquement au modèle d'abonnement BYOL.

FONCTIONNALITÉS CLOUD

Environnements pris en charge	Amazon Web Services (AWS)
Modèles d'abonnement	BYOL (Bring-Your-Own-License), On-Demand

FONCTIONS DE SÉCURITÉ

Pare-feu	Inspection dynamique des paquets, inspection au niveau de la couche applicative, pare-feu proxy
Proxies applicatifs	HTTP, HTTPS, SMTP, FTP, DNS, TCP-UDP, POP3
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), Threat Detection and Response

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
SSO (authentification unique)	Systèmes d'exploitation mobiles, Windows, Mac OS X, RADIUS
Authentification	RADIUS, LDAP, Windows Active Directory, RSA SecurID, base de données interne

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.

Services	TOTAL SECURITY SUITE	Basic Security Suite
Service de prévention d'intrusions (IPS)	✓	✓
Contrôle d'application	✓	✓
WebBlocker (Filtrage du contenu/des URL)	✓	✓
Gateway AntiVirus (GAV, antivirus de passerelle)	✓	✓
Reputation Enabled Defense (RED, Autorité de réputation)	✓	✓
APT Blocker	✓	
Data Loss Prevention (DLP, Prévention des fuites de données)	✓	
Dimension Command	✓	
Threat Detection and Response (avec WatchGuard Host Sensor)	✓	
Support	Gold (24 h/24, 7 j/7)	Standard (24 h/24, 7 j/7)

UNE OFFRE. TOTAL SECURITY.

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.

FRANCE 01 40 90 30 35 SERVICE COMMERCIAL INTERNATIONAL +1.206.613.0895 www.watchguard.fr