

WatchGuard® XTMv

Virtualisation de la sécurité pour les besoins de l'entreprise d'aujourd'hui

Fonctionnement d'appareils virtuels sur votre infrastructure virtuelle

- Fonctionnalités et services UTM et de pare-feu nouvelle génération de qualité dans l'infrastructure virtuelle
- Facile à télécharger, activer, déployer et gérer (WSM, Web, CLI)
- Tire parti de la souplesse et de la disponibilité vSphere et Hyper-V
- Plusieurs modèles adaptés aux organisations de toutes tailles
- Campus, nuage/hébergement, consolidation des succursales
- Déploiement par client, par service ou par application

Les organisations de toutes tailles adoptent la virtualisation dans le but de réduire les coûts et d'augmenter l'efficacité, la disponibilité et la souplesse de leurs ressources informatiques. La virtualisation ne se concrétise pas toutefois sans dépenses. Les environnements virtuels sont compliqués à gérer et vulnérables aux menaces à la sécurité. Les services informatiques doivent être prêts. Désormais, les applications peuvent être sécurisées, les ressources maximisées, et votre service informatique peut tirer profit de son système unique de gestion unifiée, sans aucun risque de sécurité en vue. WatchGuard XTMv offre au monde de la virtualisation le meilleur qui soit en matière de sécurité du réseau. Avec un monitoring en temps réel, une prise en charge multi-WAN et des solutions évolutives parfaitement adaptées à l'entreprise quelle que soit sa taille, les environnements virtuels peuvent être tout aussi sûrs que l'environnement physique.

Les solutions virtuelles de WatchGuard proposent une souplesse de déploiement exceptionnelle. Vous pouvez choisir de déployer un mélange de matériels et d'appareils virtuels, fonctionnant de concert et administrés à partir d'une plate-forme commune de gestion centralisée. Les appliances virtuelles de WatchGuard disposent des mêmes services de sécurité et de mise en réseau que les équipements physiques, et leur déploiement peut s'effectuer par client, par service ou par application, pour votre infrastructure virtuelle.

Virtualisation du pare-feu de passerelle traditionnel pour une souplesse sans précédent : protection du périmètre interne

WatchGuard XTMv protège autant le périmètre physique du centre de données que le périmètre virtuel. Vous pouvez désormais aisément appliquer une stratégie qui protège les données dans la base de données de l'entreprise et les isole de l'infrastructure de messagerie, ou les informations confidentielles du personnel des données financières d'autres divisions, même si elles opèrent sur les mêmes serveurs.

Consolidation de plusieurs pare-feu pour une efficacité à fort impact : protection multi-domaines

Les prestataires de services (services d'hébergement de messagerie, de cloud ou de sécurité managée) peuvent déployer plusieurs instances du XTMv sur des serveurs à la périmétrie de leurs datacenters. Ces pare-feu virtuels sont isolés les uns des autres, de façon qu'il soit possible de garantir des contrats de niveau de service (contrats SLA) à chaque environnement, et qu'une modification apportée à la configuration de l'un n'ait aucune incidence sur les autres. Et pourtant, le prestataire est capable de tous les gérer depuis une simple console intuitive.

Élimination des coûts matériels redondants et sécurité des réseaux virtuels : consolidation des succursales

À mesure que les succursales et divisions de plus grande taille consolident les serveurs locaux (fichiers, impression, voix, etc.) en un boîtier, il est possible de déployer un pare-feu virtuel sur le serveur physique, isolant tout le trafic de l'Internet public. Un simple tunnel VPN peut fournir un chemin de retour sûr vers les datacenters ou les clouds virtuels privés de l'entreprise, garantissant des économies de coûts dans chaque site sans compromettre la sécurité.

Éditions WatchGuard XTMv

	Small Office	Medium Office	Large Office	Datacenter
Débit et connexions				
Débit du pare-feu [†]	1 Gbits/s	2,5 Gbits/s	5 Gbits/s	Illimité
Interfaces virtuelles	10	10	10	10
Nœuds pris en charge (LAN IP)	Illimités	Illimités	Illimités	Illimités
Connexions simultanées (bidirectionnelles)	30 000	350 000	1 250 000	2 500 000
Prise en charge VLAN	50	75	400	4 000
Tunnels VPN				
Branch Office VPN	50	600	6 000	10 000
Mobile VPN IPSec	5	50	800	Illimité
VPN SSL Mobile (incl/max)	10/50	10/600	6 000/6 000	Illimité
Utilisateurs authentifiés	200	2 500	5 000	Illimité

Sécurité de nouvelle génération

Pare-feu	Inspection dynamique des paquets, inspection au niveau de la couche applicative, pare-feu proxy
Proxies applicatifs	HTTP, HTTPS, SMTP, FTP, DNS, TCP, POP3
Protection contre les menaces	Blocage des spywares, des attaques DoS, des paquets fragmentés ou malformés, des menaces mixtes et autres
Voix sur IP	H.323, SIP, sécurité de l'établissement de la communication et de la session
Services de sécurité par abonnement	Contrôle d'Application, Intrusion Prevention Service, Gateway AntiVirus, Reputation Enabled Defense, spamBlocker, WebBlocker

VPN et authentification

Chiffrement	DES, 3DES, AES 128, 192 et 256 bits
IPSec	SHA-1, MD5, clé IKE pré-partagée, certificat tiers
SSL	Client léger, Web
PPTP	Serveur et Passthrough
Basculement VPN	Oui
Single Sign-On	Authentification Active Directory transparente
XAUTH	RADIUS, LDAP, Secure LDAP, Windows Active Directory
Autre authentification des utilisateurs	VASCO, RSA SecurID, basé sur le Web, local, Services Terminal Server Microsoft et Citrix

Plate-forme et mise en réseau

Système d'exploitation	Fireware® XTM / Fireware XTM Pro
Prise en charge d'un hyperviseur	VMMware vSphere 4.1, 5.0, 5.1 / Windows Server 2008 R2, 2012 (Hyper-V)
Affectation d'adresses IP	Statique, DHCP (serveur, client, relais), DynDNS, PPPoE
Routage	Statique, dynamique (BGP4, OSPF, RIP v1/2), basé sur stratégie
QoS	8 files d'attente prioritaires, diffserv, file d'attente stricte modifiée
Prise en charge VLAN	Mode pont, balisage, routé
NAT	Statique, dynamique, 1:1, IPSec NAT Traversal, NAT basée sur stratégie, IP virtuelle
Autre mise en réseau	Indépendance des ports, basculement WAN, équilibrage de charge, mode transparent/d'insertion

Administration

Plate-forme d'Administration	WatchGuard System Manager (WSM) v11.5.2 ou plus
Alertes et notifications	SNMP v2/v3, e-mail, alerte du système de gestion
Prise en charge des serveurs	Journalisation, Rapports, Quarantaine, WebBlocker, Management
Web UI	Prend en charge les systèmes d'exploitation Windows, Mac et Linux avec les navigateurs les plus courants
CLI	Avec Direct Connect et scripts

Certifications

Réseau	Prêt pour IPv6 Gold (routage)
---------------	-------------------------------

POWERED BY FIREWARE® XTM

Les éditions Large Office et Datacenter de XTMv sont livrées avec la version Pro du système d'exploitation Fireware XTM, offrant les caractéristiques requises pour les réseaux les plus exigeants. La version Pro est disponible quand vous achetez une mise à niveau pour les éditions Small et Medium Office.

FONCTIONS RÉSEAU	FIREWARE XTM	FIREWARE XTM PRO
Routage	Routage statique, dynamique (RIP)	Dynamique (BGP4, OSPF, RIP v1/2), basé sur stratégie
NAT	Statique, dynamique, 1:1, IPSec Traversal, basée sur stratégie	IP virtuelle pour l'équilibrage de charge côté serveur
SSL	10 tunnels SSL disponibles	Nombre maximum de tunnels SSL disponibles par édition
Autres fonctionnalités	Indépendance des ports, mode transparent/d'insertion, basculement multi-WAN	Équilibrage de charge côté serveur, équilibrage de charge multi-WAN

UN SUPPORT ET DES CONSEILS D'EXPERTS

Un abonnement initial au service LiveSecurity® est inclus avec chaque solution XTMv. LiveSecurity garantit un support technique d'urgence, des mises à jour logicielles pour que le code soit toujours actualisé, et des alertes concises en cas de menaces.

LA SÉCURITÉ VIRTUELLE PROPOSÉE EN OFFRE GROUPÉE

Protégez dans sa totalité votre infrastructure virtuelle avec l'offre groupée XTM Security. Cette offre groupée comprend l'édition XTMv de votre choix, plus Application Control, Intrusion Prevention Service, Gateway AV, WebBlocker, Reputation Enabled Defense et spamBlocker, ainsi que LiveSecurity* pour l'assistance et la maintenance. Une offre très intéressante qui permet d'effectuer un achat groupé et d'économiser !

*Les offres groupées XTMv Security pour les éditions Small/Medium Office incluent LiveSecurity standard avec un support technique 12 h/24, 5 j/7. Les offres groupées XTMv Security pour les éditions Large Office et Datacenter incluent LiveSecurity Plus avec un support technique 24 h/24, 7 j/7.

†Les débits peuvent varier selon l'environnement et la configuration, y compris l'infrastructure de virtualisation. Contactez votre revendeur WatchGuard, ou appelez directement WatchGuard qui vous aidera à choisir le bon modèle pour votre réseau.

SERVICE COMMERCIAL FRANCE 01 40 90 30 35

SERVICE COMMERCIAL INTERNATIONAL +1.206.613.0895 www.watchguard.fr