Présentation abrégée

Cisco ASA avec fonctionnalités FirePOWER

La solution de sécurité avancée pour les PME et les entreprises multisites

Les entreprises, quelle que soit leur taille, sont confrontées à des attaques dont les répercussions sont toujours plus coûteuses et qui mettent en danger les données des clients, les secrets commerciaux et la propriété intellectuelle. L'**enquête sur les failles de sécurité réalisée en 2013** à la demande du gouvernement britannique a révélé que 87 % des PME ont été touchées en 2012. Afin de renforcer leur sécurité, les grandes entreprises demandent à leurs partenaires, les cabinets d'avocats par exemple, de renforcer leur défense afin de réduire le risque de devenir eux-mêmes un vecteur d'attaque.

Les PME et les entreprises multisites ont besoin d'une solution de protection avancée. Toutefois, elles n'ont à ce jour que peu bénéficié des produits de gestion unifiée des menaces et des pare-feu de nouvelle génération concurrents (NGFW). Contrairement aux approches traditionnelles, les pare-feu Cisco de nouvelle génération (NGFW) présentent des fonctionnalités de protection avancées contre les programmes malveillants ainsi que des IPS de nouvelle génération (NGIPS). Les derniers modèles de pare-feu de nouvelle génération Cisco® ASA avec fonctionnalités FirePOWER™ ont été pensés pour les applications des PME et des succursales en particulier. Ils offrent des fonctionnalités de défense intégrées, avec des coûts d'achat et d'exploitation faibles, ainsi qu'une gestion simplifiée.

La solution est proposée dans un format permettant une installation sur un bureau (5506-X) et en boîtier unique pour un montage en rack 1RU (5508-X, 5516-X). Il existe également des versions du modèle de bureau équipé d'un point d'accès sans fil intégré (5506W-X) afin de simplifier la mise en réseau des PME.

Une appliance ultrarésistante (5506H-X) a été conçue pour les systèmes de contrôle industriel et les applications d'infrastructure vitales. Elle dispose d'une plage de températures de fonctionnement étendue et peut être déployée en bureau ou sur rail DIN [1], en rack ou en montage mural.

Valeur supérieure. Protection supérieure contre les menaces. Options de gestion souples.

Les solutions de pare-feu de nouvelle génération Cisco affichent une valeur supérieure et disposent de fonctionnalités de pointe en matière de protection contre les menaces, notamment un pare-feu, le contrôle des applications, le NGIPS, le filtrage des adresses URL, Cisco Advanced Malware Protection (AMP) et le VPN. Grâce à une visibilité et un contrôle exceptionnels ainsi qu'à une hiérarchisation automatique des menaces, les fausses alertes qui alourdissaient inutilement le travail du personnel sont désormais gérées de manière efficace.

Avantages

- **Système de défense supérieur** équipé de la technologie de sécurité de pointe présente sur les grands pare-feu de nouvelle génération Cisco®
- **Solution aux dimensions adaptées, accessible** aux PME au budget limité et présentant un coût total d'acquisition faible
- **Fonctionnalités de gestion simplifiée dans le boîtier ou, en option, fonctionnalités de gestion centralisée** pour les installations comportant plusieurs appareils

[1] Rail DIN - Le terme provient des spécifications initiales publiées par le Deutsches Institut für Normung (DIN) en Allemagne, spécifications qui ont depuis été reprises pour des normes européennes (EN) et internationales (ISO).

Points d'épreuve

- Cisco ASA est, selon l'étude IDC Worldwide Quarterly Security Appliance Tracker® de 2014, le pare-feu le plus déployé dans le monde.
- Le client VPN Cisco AnyConnect est leader sur le marché mondial, fort de plus 100 millions de déploiements et entièrement compatible avec Cisco ASA avec les services FirePOWER.
- Cisco ASA avec les services FirePOWER utilise les flux quotidiens de menaces fournis par Cisco Security Intelligence afin de permettre une détection rapide des menaces.

Fonctionnalités

Cisco ASA 5506-X, 5506W-X, 5506H-X, 5508-X et 5516-X avec les services FirePOWER

Assistance utilisateur/nœud	Illimitée par défaut
Facteur de forme bureau (5506-X, 5506W-X)	20,11 x 22,65 x 4,39 cm
Facteur de forme montage en rack (5508-X, 5516-X)	43,68 x 28,67 x 4,36 cm
Facteur de forme durci (5506H-X)	22,98 x 22,98 x 6,9 cm
Ports d'E/S intégrés	8 x 1GE
VPN	
Pairs VPN	50 à 300
Prise en charge de la mobilité	AnyConnect 4.x ; Apple iOS natif et clients Android
Débit	
Pare-feu « stateful » maximal	750 Mbit/s à 1,8 Gbit/s
AVC maximum	250 à 850 Mbit/s
AVC et NGIPS maximum	125 à 600 Mbit/s
Haute disponibilité	Oui : Mode actif/veille* Actif/actif (5508-X et 5516-X uniquement)
Fonctionnalités NGFW	
AVC	Fournies avec SmartNet
Applications prises en charge	Plus de 3 000
Filtrage des URL	Abonnement
Catégories ; Total	80+ ; 280+ millions
NGIPS	Abonnement
Signatures	6 000+
AMP - Défense contre les menaces	Abonnement
Équipe dirigeante	
Gestion on-box intégrée	Incluse par défaut
Gestion centralisée	Licence optionnelle

* Nécessite une licence Security Plus.

Pour les spécifications techniques supplémentaires, consultez la fiche technique ASA avec les services FirePOWER.

Les solutions de sécurité Cisco permettent également d'accélérer la résolution des incidents, tandis que les clients témoignent souvent de la diminution du délai de correction, de plusieurs semaines à quelques heures.

Bien que spécifiquement conçus pour les PME et les entreprises du marché intermédiaire, les modèles Cisco NGFW offrent les mêmes technologies supérieures de protection contre les menaces que les autres pare-feu de nouvelle génération de la gamme Cisco ASA 5500-X, notamment les modèles Cisco ASA 5525-X et 5585-X auxquels NSS Labs a attribué en 2014 la note la plus élevée en matière de sécurité dans sa carte de la sécurité des pare-feu de nouvelle génération **(Next-Generation Firewall Security Value Map)**. Ces pare-feu Cisco de nouvelle génération incluent la gestion intégrée sur périphérique pour les déploiements d'instances uniques et la prise en charge de la gestion centralisée avec le système Cisco FireSIGHT Management, si nécessaire.

Fonctions standard de Cisco ASA avec les services FirePOWER

- **Visibilité et contrôle des applications (AVC) granulaires de Cisco :** Cisco AVC prend en charge plus de 3 000 contrôles de couches applicatives basés sur les risques. Par exemple, vous pouvez rendre les médias sociaux populaires accessibles en lecture seule, et ainsi vous conformer à différentes réglementations, notamment celle de la loi HIPPA pour la gestion électronique de l'assurance maladie et celle de la FINRA, l'instance indépendante de régulation des services financiers, et appliquer des politiques d'utilisation acceptables.
- **Pare-feu réseau, prise en charge de VPN d'accès à distance et site à site :** Cisco propose les pare-feu et les VPN les plus fiables et les plus déployés au monde. Intégration aisée du client VPN optionnel Cisco AnyConnect® avec Cisco ASA avec les services FirePOWER. Cisco AnyConnect 4.0 dispose d'un VPN permanent avec contrôle granulaire des applications. En outre, Cisco ASA prend en charge Cisco AnyConnect Mobile et les clients VPN natifs Android et iOS.

Options d'abonnement aux services Cisco FirePOWER

- **NGIPS** fournit des informations contextuelles de pointe, une visibilité et un contrôle complets pour les utilisateurs, les périphériques, les applications et le contenu, et une prévention des menaces avancée.
- **AMP** dispose d'une technologie de pointe qui permet de détecter, comprendre, stopper et, le cas échéant, éradiquer les programmes malveillants que les autres couches de sécurité n'ont pas détectés.
- **Le filtrage des URL basé sur la réputation** bloque les adresses Web présentant un risque élevé. Les spams, virus basés sur des URL, attaques par hameçonnage et logiciels espions sont susceptibles de diriger les utilisateurs vers des adresses URL malveillantes. Cisco effectue une analyse précise de toutes les URL et associe à chacune un score de réputation. Les utilisateurs peuvent ainsi éviter les adresses Web qui présentent un risque élevé.

Étape suivante

Dans un premier temps, contactez un partenaire Cisco proche de chez vous : Trouver un partenaire Cisco.

C45-733830-01 03/15