Cisco Secure Firewall pour les institutions financières

Sommaire

Intégration du réseau et de la sécurité

Contrôles de sécurité exceptionnels

Politiques et visibilité cohérentes

Faites de votre réseau une extension de votre architecture de sécurité

Avec des applications stratégiques qui s'exécutent de plus en plus dans des environnements hybrides et multicloud, et des utilisateurs qui ont besoin d'un accès sécurisé aux ressources, où qu'ils se trouvent, un pare-feu classique ne suffit plus. Le périmètre réseau, autrefois unique, est désormais constitué de plusieurs micropérimètres. Pour de nombreuses institutions financières, l'application est le nouveau périmètre, et les déploiements de pare-feu classiques ont évolué vers un ensemble hétérogène d'appliances physiques, virtuelles et cloud natives. C'est pourquoi elles ont du mal à prendre en charge les environnements des applications modernes. Le défi consiste à maintenir une visibilité cohérente, à appliquer les politiques et à uniformiser les informations sur les menaces sans créer de vulnérabilités qui exposent l'entreprise à des risques.

Cisco développe NetWORK, une approche plus agile, automatisée et intégrée de la sécurité du réseau qui harmonise les politiques sur l'ensemble des applications dynamiques modernes et sur des réseaux de plus en plus hétérogènes. Cisco Secure Firewall vous offre le meilleur niveau d'intégration entre les fonctionnalités et la sécurité du réseau, proposant ainsi une architecture plus sécurisée que jamais. Résultat : une gamme complète de solutions de sécurité qui protège vos applications et vos utilisateurs partout.

Bénéfices

- Sécurité unifiée et en temps réel des workloads et du réseau pour un contrôle intégré sur les environnements des applications dynamiques.
- Approche globale de la sécurité du réseau qui exploite et partage les informations provenant de sources stratégiques pour accélérer la détection, la réponse et la remédiation. Protégez les collaborateurs travaillant à distance grâce à un accès d'entreprise hautement sécurisé à tout moment, partout et sur tout type d'équipement, avec de puissantes fonctionnalités de prévention des menaces qui sécurisent l'entreprise, les équipes et les applications essentielles.
- Droit d'accès SecureX™ inclus avec chaque pare-feu Cisco® Secure Firewall, pour une approche étroitement intégrée de la sécurité qui permet de mettre en corrélation les menaces sur l'ensemble de la gamme Cisco Secure et de répondre plus rapidement aux incidents.

Plus de visibilité et de contrôle

Les menaces sont de plus en plus sophistiquées et les réseaux toujours plus complexes. Rares sont les institutions financières qui disposent des ressources nécessaires pour maintenir leurs systèmes à jour et repousser toutes les nouvelles menaces.

Au vu de la complexification des menaces et des réseaux, il est impératif d'adopter des outils appropriés pour protéger vos données, vos applications et vos réseaux. Les appliances Cisco Secure Firewall offrent la puissance et la flexibilité dont vous avez besoin pour anticiper les menaces. Leurs performances sont 3 fois supérieures à celles des appliances de la génération précédente et elles fournissent des fonctionnalités matérielles uniques pour inspecter le trafic chiffré à grande échelle. De plus, les règles de l'IPS Snort 3 sont lisibles et simplifient la sécurité. Vous disposez d'une visibilité et d'un contrôle dynamiques sur les applications grâce à l'intégration de Cisco Secure Workload, pour une protection constante des applications actuelles sur l'ensemble du réseau et des workloads.

Trouver le pare-feu idéal pour votre entreprise

Une gestion simplifiée et homogène des politiques

Avec la gamme Secure Firewall, vous bénéficiez d'une meilleure sécurité ainsi que d'outils de gestion flexibles et évolutifs. Cisco propose diverses options de gestion adaptées aux besoins de votre entreprise :

- **Cisco Secure Firewall Device Manager :** solution de gestion sur l'équipement pour Firewall Threat Defense qui gère un seul pare-feu localement
- **Cisco Secure Firewall Management Center :** qui gère un déploiement de pare-feu à grande échelle et est disponible dans tous les formats, notamment on-premise, dans le cloud privé, dans le cloud public et avec les logiciels SaaS
- **Cisco Defense Orchestrator :** gestionnaire cloud qui rationalise les politiques de sécurité et la gestion des équipements sur plusieurs produits Cisco, tels que Cisco Secure Firewall, Meraki® MX et les appareils Cisco IOS®

Nous proposons également Cisco Security Analytics and Logging pour une gestion évolutive des événements. Il améliore la détection des menaces et répond aux exigences de conformité dans toute l'entreprise, grâce à une plus longue rétention des données et à des fonctionnalités d'analyse des comportements.

L'histoire d'une réussite : Lake Trust Credit Union

Pourquoi choisir Cisco ?

La gamme Cisco Secure Firewall protège davantage votre réseau contre un ensemble toujours plus complexe et évolué de menaces. Avec Cisco, vous investissez dans une base à la fois agile et intégrée pour votre sécurité. Vous vous assurez ainsi le meilleur niveau de protection, aujourd'hui comme demain.

Du data center aux environnements cloud, en passant par les sites distants et on-premise, vous pouvez tirer parti des solutions Cisco pour transformer votre infrastructure réseau en extension de votre solution de pare-feu et profiter de contrôles de sécurité de pointe partout où vous en avez besoin.

En investissant aujourd'hui dans une appliance Cisco Secure Firewall, vous profitez d'une protection robuste contre les menaces les plus sophistiquées, sans compromettre les performances lors de l'inspection du trafic chiffré. En outre, l'intégration avec d'autres solutions Cisco et tierces vous permet de bénéficier d'une gamme vaste et complète de produits de sécurité qui fonctionnent de concert pour mettre en corrélation des événements auparavant déconnectés, éliminer les faux positifs et stopper les menaces plus rapidement.

Fonctionnalités avancées de Cisco Secure Firewall

Fonctionnalités avancées	Détails
Intégration de Cisco Secure Workload	• L'intégration de Cisco Secure Workload (anciennement Tetration) offre une visibilité complète et permet d'appliquer les politiques de manière cohérente et évolutive sur l'ensemble du réseau et des workloads pour les applications distribuées, dynamiques et modernes d'aujourd'hui.
Cisco Secure Firewall Cloud Native	• Conçue avec Kubernetes et disponible pour la première fois dans AWS, Cisco Secure Firewall Cloud Native est une solution conviviale d'accès aux applications pour les développeurs qui permet de créer une infrastructure cloud native hautement flexible.
Prise en charge des politiques dynamiques	• Les attributs dynamiques prennent en charge les balises VMware, AWS et Azure pour les situations où les adresses IP statiques ne sont pas disponibles. • Cisco est pionnier dans le domaine des politiques basées sur des balises avec la prise en charge de l'étiquetage SGT et des attributs Cisco ISE (Identity Services Engine).
Système de protection contre les intrusions Snort 3	• Le système open source de pointe Snort 3 fournit un niveau avancé de protection contre les menaces qui permet d'améliorer la détection et les performances, et de simplifier la personnalisation.
Détection et identification des serveurs TLS	• Permet d'appliquer les politiques de couche 7 sur le trafic TLS 1.3 chiffré. Assurez la visibilité et le contrôle dans un environnement chiffré dans lequel le déchiffrement et l'inspection de chaque flux de trafic ne sont pas réalisables. Les pare-feu de la concurrence divisent vos politiques de couche 7 avec un trafic TLS 1.3 chiffré.
Cisco Secure Firewall Management Center	• Gestion unifiée des pare-feu, du contrôle des applications, de la prévention des intrusions, du filtrage des URL et des politiques de protection contre les malwares. • L'intégration avec Cisco Secure Workload (anciennement Tetration) permet une visibilité et une application des politiques cohérentes pour les applications dynamiques sur l'ensemble du réseau et des workloads.
Cisco Defense Orchestrator	• Gestion des pare-feu dans le cloud pour manipuler facilement et de manière cohérente les politiques pour l'ensemble de vos pare-feu Cisco Secure.
Cisco Security Analytics and Logging	• Gestion hautement évolutive des événements liés aux pare-feu on-premise et dans le cloud, avec une analyse comportementale permettant de détecter les menaces en temps réel et de réduire le temps de réponse. Analyse continue affinant votre stratégie de sécurité pour une meilleure défense contre les prochaines attaques. • Répondez à vos besoins de conformité grâce à l'agrégation des journaux d'événements sur tous les pare-feu Cisco Secure Firewall. • Intégration étroite avec les gestionnaires de pare-feu pour une journalisation et une analyse étendues, et agrégation des données des journaux de pare-feu sous une seule et même vue intuitive.
Cisco SecureX	• Tirez parti de la plateforme SecureX pour détecter les menaces et y remédier plus rapidement. Chaque pare-feu sécurisé inclut des autorisations pour Cisco SecureX. Le nouveau ruban SecureX de Firewall Management Center permet aux équipes SecOps de basculer instantanément vers la plateforme ouverte SecureX, ce qui accélère la réponse aux incidents.
Threat Intelligence de Cisco Talos®	• Cisco Talos Intelligence Group est l'une des plus grandes équipes de Threat Intelligence au monde. Elle fournit rapidement des informations précises et exploitables sur les clients, les produits et les services Cisco. Talos gère les ensembles de règles officiels Snort.org, ClamAV et SpamCop.

Étapes suivantes

Pour en savoir plus sur Cisco Secure Firewall ou découvrir d'autres solutions de sécurité pour les services financiers, consultez notre catalogue de solutions. N'hésitez pas à contacter un commercial Cisco et à consulter les différentes options d'achat.

Siège social aux États-Unis
Cisco Systems, Inc.
San José. CA

Siège social en Asie-Pacifique
Cisco Systems (États-Unis) Pte. Ltd.
Singapour

Siège social en Europe
Cisco Systems International BV Amsterdam.
Pays-Bas

Cisco compte plus de 200 agences à travers le monde. Les adresses, numéros de téléphone et de fax sont répertoriés sur le site web de Cisco, à l'adresse : www.cisco.com/go/offices.

Imprimé aux États-Unis C45-3380706-00 02/23