CISCO
SECURE

Aperçu
Document public de Cisco

Cisco Secure Firewall

Intégration du réseau et de la sécurité

Contrôles de sécurité de niveau mondial

Politique cohérente et visibilité

Transformez l'ensemble de votre réseau en une extension de votre architecture de sécurité

Puisque nos applications essentielles à l'entreprise sont tant en nuage que sur site et que nos utilisateurs pouvoir accéder de façon sécurisée aux ressources où qu'ils soient, l'approche avec pare-feu traditionnel n'est plus adéquate. Notre périmètre de réseau unique a évolué vers plusieurs micro-périmètres. Pour de nombreuses entreprises, l'application est le nouveau périmètre, et les déploiements de pare-feu actuels ont donc évolué vers une combinaison d'appareils physiques, virtuels et en nuage. Les entreprises ont du mal à prendre en charge les environnements des applications modernes. Elles font désormais face à de nombreux défis comme maintenir une visibilité cohérente, assurer l'application des politiques et garantir une visibilité uniforme des menaces sans cependant créer de vulnérabilités qui pourraient exposer l'entreprise à des risques.

C'est pourquoi, chez Cisco, nous développons NetWORK, une vision axée sur la sécurité réseau qui permet une approche automatisée, plus agile et intégrée pour harmoniser les politiques et leur application sur les applications dynamiques modernes et sur des réseaux de plus en plus hétérogènes. Secure Firewall vous offre l'ensemble le plus complet d'intégrations entre les principales fonctions de mise en réseau et la sécurité du réseau, offrant ainsi l'architecture la plus sécurisée de tous les temps. Le résultat est une gamme complète de solutions de sécurité qui protège vos applications et vos utilisateurs partout.

Avantages

- Sécurité unifiée et en temps réel pour la charge de travail et le réseau qui offre un contrôle intégré dans les environnements des applications dynamiques
- Approche de la sécurité du réseau par plateforme qui tire parti de l'utilisation et du partage des renseignements provenant de sources clés pour accélérer la détection, la réponse et la correction; protection des télétravailleurs grâce à un accès d'entreprise hautement sécurisé à tout moment, en tout lieu et à partir de tout appareil, grâce à de puissantes fonctionnalités de prévention des menaces qui protègent l'entreprise, les utilisateurs et les applications essentielles
- Droit à SecureX™ compris avec chaque pare-feu Cisco® Secure Firewall, ce qui crée une approche de sécurité étroitement intégrée qui permet la corrélation des menaces dans l'ensemble de la gamme Cisco Secure et accélère la réponse en cas d'incident

Pourquoi choisir Cisco?

La gamme Cisco Secure Firewall offre une plus grande protection pour votre réseau contre un ensemble de menaces de plus en plus complexe et en constante évolution. Grâce à Cisco, vous investissez dans une base de sécurité à la fois agile et intégrée, qui vous mènera à la posture de sécurité la plus solide qui soit, aujourd'hui comme dans le futur.

De vos centres de données, de vos succursales, de vos environnements infonuagiques et de partout entre ces différents points, vous serez en mesure de tirer parti de la puissance de Cisco. Vous pourrez ainsi transformer votre infrastructure réseau existante en une extension de votre solution de pare-feu et profiter de contrôles de sécurité de classe mondiale partout où vous en avez besoin.

Investir aujourd'hui dans un dispositif de la gamme Secure Firewall vous procure une protection solide contre les menaces les plus sophistiquées, sans compromettre les performances pendant l'inspection du trafic chiffré. En outre, l'intégration avec d'autres solutions de Cisco et avec des solutions tierces vous donne accès à une vaste gamme complète de produits de sécurité, qui travaillent ensemble pour corréler des événements auparavant déconnectés, éliminer le bruit et arrêter plus rapidement les menaces.

Une visibilité et un contrôle supérieurs

Les menaces sont plus sophistiquées et les réseaux, plus complexes. Très peu d'entreprises, sinon aucune, ne disposent des ressources nécessaires pour se tenir au fait des nouvelles menaces et repousser efficacement toutes ces menaces émergentes et en constante évolution.

À mesure que les menaces et les réseaux deviennent plus complexes, il est impératif d'avoir les bons outils pour protéger vos données, vos applications et vos réseaux. Les pare-feu Cisco Secure ont la puissance et la flexibilité dont vous avez besoin pour garder une longueur d'avance sur les menaces. Ils offrent des performances spectaculaires, trois fois supérieures à celles des appareils de la génération précédente, ainsi que des capacités matérielles uniques pour l'inspection du trafic chiffré à grande échelle. Quant aux règles lisibles par un humain de Snort 3 IPS, elles aident à simplifier la sécurité. L'intégration de Cisco Secure Workload, qui offre la visibilité et le contrôle dynamiques des applications, permet quant à elle d'assurer une protection cohérente des applications modernes sur l'ensemble du réseau et de la charge de travail.

Trouvez le pare-feu idéal pour votre entreprise

Gestion simplifiée et cohérente des politiques

Grâce à la gamme Secure Firewall, vous obtenez une posture de sécurité renforcée, dotée de capacités de gestion flexibles et prêtes pour l'avenir. Cisco offre une variété d'options de gestion adaptées qui sauront répondre aux besoins de votre entreprise :

- **Cisco Secure Firewall Device Manager :** Gère un seul pare-feu local; une solution de gestion sur l'appareil pour Firewall Threat Defense
- **Cisco Secure Firewall Management Center :** Gère un déploiement de pare-feu à grande échelle; disponible dans tous les formats, y compris sur place, en nuage privé, en nuage public et en logiciel-service (SaaS)
- **Cisco Defense Orchestrator :** Gestionnaire en nuage qui simplifie les politiques de sécurité et la gestion des périphériques sur plusieurs produits Cisco, tels que Cisco Secure Firewall, Meraki MX et les périphériques Cisco IOS®

Cisco offre également Cisco Security Analytics and Logging pour une gestion évolutive des journaux, ce qui améliore la détection des menaces et respecte les mandats de conformité dans l'ensemble de l'entreprise grâce à une rétention plus longue et à des capacités d'analyse comportementale.

Témoignages de clients

Fonctionnalités avancées de Cisco Secure Firewall

Fonctionnalités avancées	Détails
Intégration de Cisco Secure Workload	• L'intégration de Cisco Secure Workload (Tetration) offre une visibilité complète et une mise en application cohérente et évolutive des politiques pour les applications distribuées et dynamiques modernes sur l'ensemble du réseau et de la charge de travail
Cisco Secure Firewall Cloud Native	• Conçu avec Kubernetes et offert pour la première fois dans AWS, Secure Firewall Cloud Native est une solution d'accès aux applications conviviale pour les développeurs qui permet de créer une infrastructure hautement élastique en nuage
Soutien dynamique des politiques	• 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 une pionnière en matière de politiques basées sur les étiquettes grâce à la prise en charge des attributs de Cisco Identity Services Engine (ISE) et des étiquettes de groupe de sécurité (SGT).
Système de prévention des intrusions Snort 3	• Snort 3, un logiciel libre de pointe et la prochaine étape dans la protection contre les menaces, permet d'améliorer la détection, de simplifier la personnalisation et d'améliorer les performances
Identité et découverte du serveur TLS (Transport Layer Security)	• Permet de maintenir les politiques de couche 7 sur le trafic chiffré TLS 1.3. Assurez la visibilité et le contrôle dans un monde chiffré où il n'est pas réaliste de déchiffrer et d'inspecter chaque flux de trafic. Sans oublier que les pare-feu concurrents brisent vos politiques de couche 7 avec un trafic TLS 1.3 chiffré
Cisco Secure Firewall Management Center	• Procure une gestion unifiée des pare-feu, de contrôle des applications, de prévention des intrusions, de filtrage des URL et des politiques de défense contre les logiciels malveillants • L'intégration de Cisco Secure Workload (Tetration) offre une visibilité complète et une mise en application cohérente et évolutive des politiques pour les applications dynamiques sur l'ensemble du réseau et de la charge de travail
Cisco Defense Orchestrator	• Une gestion de pare-feu en nuage qui vous aide à gérer de manière cohérente et facile les politiques sur l'ensemble de vos pare-feu Cisco Secure
Cisco Security Analytics and Logging	• Gestion hautement évolutive des journaux de pare-feu sur place et dans le nuage avec analyse comportementale pour la détection des menaces en temps réel, pour des temps de réponse plus rapides. Analyse continue qui vous permet d'affiner votre posture de sécurité pour mieux vous défendre contre les tentatives futures. • Répond à vos besoins en matière de conformité grâce à l'agrégation des journaux sur l'ensemble des pare-feu Cisco Secure • Intégration étroite avec les gestionnaires de pare-feu pour une journalisation et une analyse étendues, sans oublier l'agrégation des données de journalisation du pare-feu dans une vue intuitive unique
Cisco SecureX	• Tirez parti de la plateforme SecureX pour accélérer la détection et la correction des menaces. Chaque pare-feu Secure inclut les droits pour Cisco SecureX. Le nouveau ruban SecureX du Firewall Management Center permet à SecOps de basculer instantanément vers la plateforme ouverte de SecureX, ce qui accélère la réponse en cas d'incident
Informations sur les menaces de Cisco Talos®	• Le groupe Cisco Talos Intelligence Group est l'une des plus grandes équipes commerciales de vigie des cybermenaces au monde. Il fournit des informations précises, rapides et concrétisables sur les menaces pour les clients, les produits et les services Cisco. Talos maintient les règles officielles de Snort.org, de ClamAV et de SpamCop

Prochaines étapes

Pour en savoir plus sur Cisco Secure Firewall, consultez https://www.cisco.com/site/ca/fr/products/security/firewalls/index.html.

Pour consulter les options d'achat et discuter avec un représentant commercial de Cisco, rendez-vous sur https://www.cisco.com/c/fr_ca/buy.html.

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

Siège social en Asie-Pacifique
Cisco Systems (USA) Pad 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 numéros de télécopieur sont répertoriés sur le site Web de Cisco, à l'adresse **www.cisco.com/go/offices**.

Imprimé aux États-Unis C45-736624-06 05/22