5 conseils pour choisir un pare-feu

Sommaire

Repensez votre pare-feu pour en faire un socle de sécurité flexible et fiable pour vos nouveaux environnements hybrides et distribués.

1. Sortir des sentiers battus

À quoi ressemble le pare-feu moderne ? Il est entièrement intégré dans votre infrastructure réseau et surtout capable d'appliquer des politiques partout, à partir d'une seule et même interface. Le pare-feu de nouvelle génération fournit une politique unifiée sur l'ensemble des plateformes, des informations sur les appareils mobiles, le contexte et les menaces, c'est-à-dire toute la visibilité dont vous avez besoin pour gérer les connexions à votre réseau qui ont lieu par le biais d'applications et de terminaux vulnérables, partout.

2. Avoir de la visibilité sur le contenu du trafic chiffré

Depuis toujours, le véritable obstacle qui vous empêche de voir le contenu chiffré est la capacité à le déchiffrer entièrement. C'est un processus coûteux et non envisageable d'un point de vue juridique et opérationnel, car il rend votre réseau et votre infrastructure hautement vulnérables à toutes les menaces, de l'exfiltration de données (failles) aux attaques par ransomwares.

Le vrai défi est de trouver un moyen de détecter les activités malveillantes à l'intérieur du trafic chiffré. Votre nouveau pare-feu doit avoir cette fonctionnalité en priorité afin d'obtenir une visibilité maximale avec moins d'effort de déchiffrement, et moins de dépenses associées.

3. Obtenir des informations sur les menaces de manière immédiate

Alors que la surface d'exposition aux attaques s'étend avec des menaces toujours plus sophistiquées visant les réseaux, les succursales et (souvent) les infrastructures vulnérables et obsolètes, les plateformes de Threat Intelligence doivent prendre une longueur d'avance sur les cybercriminels. Elles doivent identifier les menaces en fonction de leur nature exacte (spam, malware ou autres types d'attaques).

Ces informations doivent servir de base pour déterminer les actions de votre pare-feu : en vous donnant du contexte dynamique sur les équipements, les emplacements et les utilisateurs sur l'ensemble du réseau.

4. Intégrer la résilience dans votre stratégie de sécurité

Les environnements hybrides, comportant souvent des utilisateurs qui se connectent chaque jour au réseau par le biais d'appareils et d'applications vulnérables, sont une occasion en or pour les pirates de s'infiltrer dans votre réseau et de mettre en danger les infrastructures obsolètes, cibles rêvées, car particulièrement vulnérables. Pour éviter ce risque, vous devez renforcer la résilience de vos systèmes de sécurité.

La résilience consiste à sécuriser le noyau de votre infrastructure de sécurité hautement disponible : le pare-feu. L'objectif est de hiérarchiser les alertes et les tâches en fonction du risque, d'anticiper les problèmes, et d'automatiser des mises à jour de sécurité horaires ainsi que la réponse aux attaques imprévues, pour gagner du temps, fluidifier l'expérience et réduire les coûts.

5. Suivre une approche holistique

Pourquoi utiliser uniquement un pare-feu, alors que vous pouvez exploiter d'autres outils pour obtenir plus de visibilité et de contexte, et pour gérer le trafic et les informations de manière unifiée ? Grâce à une suite d'outils qui améliore les performances de votre pare-feu, vous gagnez en visibilité et en capacité d'analyse du contexte sans payer plus.

La déconnexion entre les services, les différents tableaux de bord et l'architecture rend la gestion des menaces particulièrement complexe. Recherchez un pare-feu et des améliorations qui vous aident à prendre des décisions plus rapidement, à réduire les délais de détection et à fournir des indicateurs pertinents et exploitables.

Découvrez comment Cisco Secure Firewall peut renforcer la sécurité de l'ensemble de votre infrastructure et défendre votre entreprise contre des menaces toujours plus sophistiquées :

En savoir plus sur Cisco Secure Firewall

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 C95-3416352-00 01/23