Cinq raisons de mettre à niveau votre pare-feu Cisco Secure Firewall

Depuis des décennies, le pare-feu est le principal outil de sécurité, une sentinelle de confiance. C'est un partenaire fiable pour bloquer les menaces. Toutefois, les environnements hybrides, dans lesquels les utilisateurs à distance accèdent à votre réseau et à vos données sensibles de n'importe où, ont rendu votre pare-feu encore plus essentiel. Dans ce monde en évolution, vous avez besoin d'un pare-feu qui simplifie l'administration, apporte une meilleure visibilité et harmonise la sécurité du réseau, de la charge de travail et des applications dans les environnements à nuages multiples.

Voici pourquoi vous devriez mettre à niveau votre pare-feu Cisco Secure Firewall :

1 Autonomiser votre personnel

Le lieu de travail a considérablement évolué ces dernières années. De plus en plus d'entreprises s'orientent vers un modèle de travail hybride, qui permet aux employeurs de réduire les coûts opérationnels et aux employés de mieux concilier vie professionnelle et vie privée. Mais cela pose un nouveau défi aux entreprises : comment permettre aux employés de travailler à distance, avec un accès aux ressources essentielles, sans accroître le risque. Grâce à la version 7.2 de Secure Firewall Threat Defense et à l'accélérateur de chiffrement intégré à la série 3100 – qui améliore de 17 fois la performance du VPN – vous pouvez adopter en toute confiance le télétravail et profiter d'un accès à distance sécurisé et dédié sans compromettre la productivité.

2 Gagner en visibilité sur le trafic chiffré

C'est un fait : les attaquants aiment innover. Avec la prolifération du chiffrement, les attaquants se cachent dans le trafic chiffré conçu pour garantir la confidentialité des données. Cet enjeu est exacerbé par les protocoles modernes comme TLS 1.3 et QUIC, qui rendent difficile de se conformer aux exigences. Le déchiffrement de tout ce trafic exige trop de ressources et est peu pratique. La version 7.2 de Secure Firewall propose une plateforme de visibilité chiffrée qui offre un avantage considérable. Découvrez les menaces sans déchiffrement. Détectez les applications malveillantes, comme le navigateur Tor Browser et les VPN non autorisés. Identifiez et traitez l'informatique de l'ombre. Vous pouvez maintenant bénéficier d'une visibilité supérieure sans faire ce compromis sur la conformité, le tout sans les inconvénients du déchiffrement.

© 2023 Cisco et/ou ses sociétés affiliées. Tous droits réservés.

cisco SECURE

3 Inspection rapide grâce à une technologie de pointe

Les attaquants exploitent les vulnérabilités, utilisant régulièrement des technologies de pointe pour lancer des attaques qui épuisent les ressources, provoquant une latence du réseau et une interruption des activités. Grâce à la plateforme d'inspection Snort 3 de Cisco Secure Firewall, profitez d'une inspection trois fois plus rapide. Exécutez davantage de règles de sécurité informatique et bénéficiez d'une meilleure visibilité sans ralentir le réseau ni perturber l'expérience des utilisateurs.

4 Protection en temps réel avec mises à jour automatiques

Les vecteurs de menaces évoluent rapidement. Les équipes des opérations de sécurité débordées se battent constamment contre les attaques par rançongiciel, l'exfiltration de données et les programmes malveillants. Cisco Talos, la plus grande équipe commerciale de vigie des cybermenaces au monde, analyse en permanence les dernières menaces mondiales et publie régulièrement de nouvelles techniques d'atténuation. Grâce à Firewall Threat Defense et à Talos, vous pouvez automatiser la réponse aux menaces et maîtriser les vulnérabilités connues avant qu'elles n'apparaissent sur votre radar, protégeant ainsi l'intégrité de votre entreprise à l'aide d'une visibilité supérieure.

5 Augmenter l'efficacité grâce à une gestion centralisée

Dans ce monde dynamique à nuages multiples, vous avez besoin d'un gestionnaire de pare-feu qui élimine la nécessité pour les équipes de gérer plusieurs environnements et supprime les silos d'outils de sécurité variés. Grâce au Cisco Secure Firewall Management Center (FMC), vous pouvez gérer de manière centralisée des centaines de pare-feux et obtenir une visibilité approfondie des incidents de sécurité à partir d'un seul et même écran. Et maintenant, grâce au FMC fourni dans le nuage au moyen du gestionnaire de périphériques Defense Orchestrator de Cisco, réduisez les coûts opérationnels et augmentez l'efficacité de votre équipe grâce à une gestion centralisée en nuage. Les améliorations apportées au FMC ont été validées pour réduire les flux de travail liés à l'exploitation du réseau jusqu'à 95 %, réduire le risque de violation jusqu'à 80 % et offrir un rendement du capital investi de 195 %.

Mettez à jour votre logiciel Cisco Secure Firewall maintenant

Nous avons simplifié la mise à jour de votre logiciel Cisco Secure Firewall. Obtenez une mise à jour par le biais de notre programme LevelUp.

Mettre à jour mon logiciel de pare-feu

Gagnez du temps et de l'argent lors de la prochaine mise à niveau de votre pare-feu

Convertissez en toute transparence vos configurations de pare-feu grâce à l'outil de migration Secure Firewall.

Mettre à jour mon matériel de pare-feu

© 2023 Cisco et/ou ses sociétés affiliées. Tous droits réservés. Cisco et le logo de Cisco sont des marques de commerce ou des marques déposées de Cisco et/ou de ses sociétés affiliées aux États-Unis et dans d'autres pays. Pour voir la liste des marques de commerce de Cisco, consultez l'adresse : www.cisco.com/go/trademarks. Les marques de commerce tierces mentionnées appartiennent à leurs détenteurs respectifs. L'utilisation du terme « partenaire » ne sous-entend aucune relation de partenariat entre Cisco et toute autre société. 975695121 1/23

The Total Economic Impact of Cisco Secure Firewall, Forrester Research, mars 2022