5 raisons d'actualiser votre pare-feu Cisco Secure Firewall

C'est sur le pare-feu que repose la sécurité depuis des décennies. C'est un partenaire fiable pour bloquer les menaces, et dans un environnement hybride, où les utilisateurs accèdent à votre réseau et à vos données sensibles à distance, son rôle est d'autant plus important. Pour s'adapter dans un monde en constante évolution, votre pare-feu doit être capable de simplifier la gestion, d'apporter de la clarté et d'unifier la sécurité du réseau, des workloads et des applications dans les environnements multicloud. **Découvrez pourquoi il est temps pour vous d'actualiser votre pare-feu Cisco Secure Firewall :**

1 Équipez votre entreprise pour les modes de travail hybrides

Les lieux de travail ont considérablement changé ces dernières années, à mesure que les entreprises se tournent vers un modèle de travail hybride. Le travail hybride bénéficie aux employeurs, qui réduisent leurs coûts, et aux collaborateurs, qui profitent d'un meilleur équilibre entre vie professionnelle et vie privée. Mais il présente également une nouvelle difficulté : comment permettre aux équipes de travailler à distance et d'accéder aux ressources stratégiques de l'entreprise sans accroître les risques ? Grâce à la version 7.2 de Cisco Secure Firewall Threat Defense et à la technologie d'accélération cryptographique intégrée à la gamme 3100 – dont les performances VPN sont jusqu'à 17 fois plus rapides –, vous pouvez envisager le télétravail sereinement et disposer d'un accès à distance dédié et sécurisé qui n'altérera pas votre productivité.

2 Retrouvez de la visibilité sur le trafic chiffré

C'est un fait : les hackers aiment innover. Avec le développement du chiffrement, ils se cachent désormais dans le trafic chiffré, conçu pour préserver la confidentialité des données. Les protocoles modernes, tels que TLS 1.3 et QUIC, rendent la conformité plus complexe, et le défi d'autant plus difficile à relever : déchiffrer tout ce trafic est un processus trop gourmand en ressources et peu pratique. La plateforme de visibilité sur le trafic chiffré de Cisco Secure Firewall 7.2 possède un atout de taille. Elle permet de détecter les menaces sans déchiffrement, d'identifier les applications malveillantes, notamment un navigateur Tor ou un VPN non autorisé, mais aussi de déceler et de traiter le « Shadow IT ». Vous profitez d'une visibilité supérieure, sans compromettre votre conformité et sans rencontrer les difficultés propres au déchiffrement.

cisco SECURE

3 Accélérez les inspections grâce à une technologie de pointe

Les hackers exploitent les vulnérabilités à l'aide de technologies de pointe qu'ils utilisent régulièrement pour lancer leurs attaques, provoquant des latences de réseau et des interruptions d'activités. Avec Cisco Secure Firewall et sa plateforme d'inspection Snort 3, vos capacités d'inspection sont 3 fois plus rapides. Exécutez davantage de règles de sécurité et profitez d'une visibilité accrue sans pour autant ralentir le réseau ni perturber l'expérience des utilisateurs.

4 Protégez-vous en temps réel avec des mises à jour automatiques

Les vecteurs de menace évoluent rapidement. Débordées, les équipes de sécurité sont constamment confrontées aux ransomwares, aux exfiltrations de données et aux programmes malveillants. Cisco Talos, la plus grande équipe spécialisée en Threat Intelligence au monde, analyse continuellement les dernières menaces et présente régulièrement de nouvelles techniques de réduction des risques. Avec Firewall Threat Defense et Talos, vous pouvez automatiser vos moyens de réponse aux menaces et le traitement des vulnérabilités connues, et profiter d'une meilleure visibilité pour protéger l'intégrité de votre entreprise.

5 Gagnez en efficacité grâce à une gestion centralisée

Dans le monde multicloud dynamique d'aujourd'hui, vous avez besoin d'un gestionnaire de pare-feu qui permette aux équipes IT de ne pas avoir à gérer plusieurs environnements et d'éliminer les silos engendrés par l'utilisation d'outils de sécurité disparates. Avec Cisco Secure Firewall Management Center (FMC), vous centralisez la gestion de plusieurs centaines de pare-feu et bénéficiez d'une visibilité détaillée sur les incidents depuis une seule et même interface. De plus, grâce à la version cloud de FMC depuis Cisco Defense Orchestrator, vous centralisez la gestion dans le cloud en réduisant vos coûts d'exploitation et en augmentant l'efficacité de vos équipes. Les bénéfices de Firewall Management Center ont été vérifiés : réduction des flux d'opérations réseau jusqu'à 95 %, diminution du risque de faille jusqu'à 80 % et ROI de 195 %.

Mettez à jour votre logiciel Cisco Secure Firewall dès maintenant

Nous avons simplifié la mise à jour de votre logiciel Cisco Secure Firewall. Profitez de notre programme LevelUp pour actualiser votre système.

Mettre à jour mon logiciel de pare-feu

Gagnez du temps et de l'argent lors de la prochaine actualisation de votre pare-feu

Convertissez vos configurations de pare-feu de manière fluide avec l'outil de migration Cisco Secure Firewall.

Mettre à jour mon matériel de pare-feu

Étude sur l'impact économique total de Cisco Secure Firewall menée par le cabinet d'étude Forrester, mars 2022