Les **cinq** meilleurs conseils pour les entreprises qui choisissent un pare-feu

Repensez votre pare-feu comme le fondement flexible, fiable et sécurisé pour un nouveau monde d'environnements hybrides et distribués.

1 | Sortez des sentiers battus

À quoi ressemble le pare-feu moderne? Entièrement intégré à votre structure de pare-feu, mais surtout : capable d'appliquer la politique partout depuis un seul écran. La prochaine génération de pare-feu offre une politique unifiée à l'échelle des plateformes, des données sur appareils mobiles, du contexte et des informations sur les menaces, soit la visibilité dont vous avez besoin pour gérer toutes les connexions à votre réseau au moyen d'applications mobiles et de points de terminaison vulnérables.

2 | Voyez ce que contient le trafic chiffré

Le défi, lorsqu'il s'agit de savoir ce qui se passe avec le trafic chiffré, a toujours été le déchiffrement complet. Il s'agit d'un processus coûteux et peu pratique d'un point de vue juridique et opérationnel, qui rend votre réseau et votre infrastructure très vulnérables à tous les risques, de l'exfiltration de données (fuites) aux attaques par rançongiciel.

Le véritable défi a été de trouver un moyen de détecter les activités malveillantes dans le trafic chiffré. Votre nouveau pare-feu devrait accorder la priorité à cette capacité, dans le but d'offrir une visibilité maximale en utilisant une levée de déchiffrement et un coût minimaux.

3 | Exigez des informations sur les menaces immédiatement

Compte tenu de l'expansion de la surface d'attaque et des menaces de plus en plus sophistiquées qui pèsent sur les réseaux, les succursales et les infrastructures (souvent) vulnérables et obsolètes, tout cadre de renseignement doit avoir une longueur d'avance sur les cybercriminels. Il devrait repérer les menaces entrantes comme telles : des pourriels, des logiciels malveillants ou d'autres types d'attaques.

Ces informations devraient servir de connaissances de base pour ce que votre pare-feu devrait faire : vous fournir un contexte dynamique sur les appareils, les emplacements et les utilisateurs de votre réseau.

4 | Intégrez la résilience en sécurité

Les environnements hybrides, souvent constitués d'utilisateurs accédant régulièrement à votre réseau à l'aide d'appareils et d'applications vulnérables, offrent aux pirates de nombreux moyens séduisants d'infiltrer votre réseau, ce qui rend les infrastructures obsolètes particulièrement vulnérables et attrayantes. La réponse à ce problème est d'intégrer la résilience en sécurité.

La résilience en sécurité consiste à sécuriser le cœur de votre infrastructure de sécurité hautement disponible – votre pare-feu – afin que vous puissiez hiérarchiser les alertes et les tâches en fonction du risque, anticiper la suite des événements et automatiser les mises à jour de sécurité horaires ainsi que vos réponses aux attaques imprévues, ce qui vous permet de gagner du temps, d'éviter les frustrations et de réduire les coûts.

5 | Adoptez une approche globale

Pourquoi s'arrêter à un simple pare-feu, alors que vous pouvez tirer parti d'un certain nombre d'outils pour offrir plus de visibilité, plus de contexte et un moyen unifié de gérer le trafic et les renseignements? Grâce à une série d'outils permettant d'améliorer les performances de votre pare-feu, vous devriez être en mesure d'avoir une meilleure visibilité et de mieux comprendre le contexte sans payer davantage.

Le manque de connexion entre les services, les multiples tableaux de bord et l'architecture rendent la gestion des menaces extraordinairement complexe. Recherchez un pare-feu et des améliorations qui vous aident à prendre des décisions plus rapidement, à réduire votre temps d'attente et à fournir des mesures significatives et exploitables.

Découvrez comment Cisco Secure Firewall peut améliorer votre posture de sécurité et défendre votre entreprise contre des menaces de plus en plus sophistiquées. :

En savoir plus sur Cisco Secure Firewall

965044294 11/22