Présentation abrégée

Cisco Network as an Enforcer

Segmentez le réseau pour contenir les risques

Alors que le nombre de connexions Internet augmente de minute en minute, votre réseau est continuellement en proie à des cyberattaques avancées, menées par des hackers professionnels. Chaque connexion réseau, qu'elle soit créée par des services cloud, la mobilité, l'Internet des objets (IoT) ou une autre activité, représente une porte d'entrée potentielle pour les hackers. Le plus difficile reste d'établir un équilibre entre l'accès réseau dont ont besoin les utilisateurs et les terminaux et l'atténuation des risques.

Fort heureusement, votre réseau Cisco® intègre déjà les technologies pour y parvenir. Il vous suffit de les activer pour transformer votre réseau en exécuteur de politiques de sécurité du réseau. Par exemple, vous pouvez bloquer les menaces avec Cisco TrustSec® et Cisco Identity Services Engine (ISE) pour segmenter votre réseau. Grâce à une approche sous forme logicielle de la segmentation du réseau, vous pouvez protéger chaque segment en appliquant des politiques de groupe spécifiques qui déterminent l'accès des utilisateurs en fonction de leur rôle et de leurs besoins professionnels.

Le résultat ? Vous contrôlez et sécurisez l'accès au réseau en fonction de rôles utilisateur et indépendamment de la topologie et de l'accès. Vous diminuez considérablement votre surface d'exposition aux attaques. Par conséquent, même si des hackers s'infiltrent dans votre réseau, leurs mouvements sont limités et ils sont incapables de causer des dégâts à grande échelle.

Appliquez une politique de sécurité dynamique de manière centralisée

Avec votre réseau Cisco qui agit comme exécuteur des politiques de sécurité réseau, vous appliquez vos règles de sécurité à l'ensemble du réseau de manière centralisée. Les utilisateurs et terminaux autorisés bénéficient de l'accès qui leur correspond, et l'impact de l'attaque est maîtrisé. Cisco ISE sert de moteur central de politiques. Il prend des décisions de contrôle d'accès en temps réel pour les commutateurs, les routeurs et les appareils de sécurité Cisco.

Par ailleurs, vous réduisez le champ d'application, le coût et la complexité des audits de conformité réseau avec la norme PCI DSS (Payment Card Industry Data Security Standard) et la loi HIPAA (Health Insurance Portability and Accountability Act) de 1996.

Utilisez la solution Cisco Network as an Enforcer pour atténuer les risques, améliorer l'efficacité opérationnelle de la sécurité et faciliter la mise en conformité du réseau.

Étapes suivantes

Pour tout savoir sur la solution Cisco d'utilisation du réseau comme exécuteur de fonctions de sécurité, rendez-vous sur la page consacrée à la sécurité des réseaux d'entreprise.

Tirez parti de la technologie d'application des politiques de sécurité déjà déployée dans votre réseau pour :

- Rapidement isoler et maîtriser les menaces sur toute votre infrastructure.
- Limiter les retombées d'une intrusion en segmentant votre réseau.
- Appliquer un contrôle d'accès granulaire et cohérent de manière centralisée pour l'ensemble des utilisateurs, des terminaux, des emplacements, etc.

« La solution Cisco nous permet d'identifier de façon très précise les utilisateurs et les ressources auxquelles ils tentent d'accéder, depuis le point d'accès sans fil ou le commutateur. Cela nous permet de classer correctement les utilisateurs par catégorie et de définir une politique adaptée aux exigences de la sécurité de l'information. »

Roman Scarabot-Mueller
Responsable de l'infrastructure,
Mondi Group International

C45-734478-00 06/15