06. Prévention des intrusions - *NEW*

Une protection complète et intégrée

Face à l'évolution des cyberattaques, vous avez besoin d'une visibilité et d'informations toujours plus précises sur l'ensemble des menaces afin d'assurer une protection complète du réseau. Les différents besoins et priorités au sein de l'entreprise appellent également à une mise en oeuvre cohérente des politiques de sécurité. Pour répondre à ces nouvelles exigences opérationnelles et renforcer la sécurité dans votre entreprise, l'adoption d'un système de prévention des intrusions (NGIPS) dédié est devenue indispensable.

Visibilité

Avec Firepower Management Center, vous avez accès à davantage de données contextuelles sur votre réseau pour pouvoir ajuster vos politiques de sécurité. Vous pouvez voir les apps, signes de compromission, profils d'hôte, trajectoire des fichiers, opérations de sandboxing, informations concernant les vulnérabilités et bien d'autres...

Flexibilité

Le système NGIPS Cisco Firepower offre des options de déploiement flexibles pour répondre à tous les besoins de l'entreprise. Il peut être déployé sur le périmètre du réseau, au niveau de la couche distribution/coeur du data center, ou derrière le pare-feu pour protéger les ressources stratégiques, l'accès invité et les connexions WAN.

Efficacité

Les systèmes NGIPS reçoivent de nouvelles signatures et règles toutes les deux heures, pour garantir une protection optimale. Cisco Talos s'appuie sur le plus grand réseau de détection des menaces au monde pour optimiser l'efficacité de tous les produits de sécurité Cisco.

Intégration

Le déploiement du système NGIPS Firepower sur votre réseau est rapide et ne nécessite aucune modification matérielle majeure. Activez et gérez différentes applications de sécurité depuis une interface unique avec Firepower Management Center.

Coûts opérationnels

Utilisez l'automatisation NGIPS pour augmenter l'efficacité opérationnelle et réduire les coûts en distinguant le simple bruit des événements exploitables. Hiérarchisez les menaces pour simplifier le travail de vos équipes et améliorez votre sécurité en appliquant des politiques recommandées en fonction des vulnérabilités de votre réseau.

Des applicances ultra performantes

Les appliances Cisco Firepower (séries 4100 et 9000) et FirePOWER (séries 7000 et 8000) sont spécialement conçues pour offrir un débit adapté à vos besoins, une conception modulaire et une évolutivité exceptionnelle. Elles intègrent une conception à faible latence et à passage unique et des interfaces fail-to-wire.

Trouvez le système de prévention des intrusions nouvelles génération idéal

FirePower Série 4100

• Conçu pour les environnements ultraperformants à la périphérie d'Internet
• Inspection des menaces entre 10 et 20 Gbit/s
• Cisco Application Visibility and Control intégré avec AMP et URL en option
• Interfaces fail-to-wire disponibles

FirePower Série 7000

• Conçu pour les services commerciaux et les bureaux distants
• Inspection des menaces entre 50 Mbit/s et 1,25 Gbit/s
• 8 à 12 interfaces de surveillance
• Small Form-Factor Pluggable (SFP) : 2 modèles

Réseaux FirePower Série 9000

• Conçu pour les opérateurs télécoms et les déploiements de data centers
• Inspection des menaces jusqu'à 90 Gbit/s
• Cisco Application Visibility and Control intégré avec AMP et URL en option
• Interfaces fail-to-wire disponibles

NGIPSv pour VMware

• Petites succursales et bureaux distants
• Inspection des menaces jusqu'à 800 Mbit/s
• Data center est-ouest/serveurs critiques PCI
• Fonctionnalités complètes du système NGIPS et de ses options

FirePower Série 8000

• Conçu pour les déploiements d'entreprise et de réseaux locaux
• Inspection des menaces jusqu'à 60 Gbit/s
• Évolutivité empilable
• Interfaces fail-to-wire disponibles

Solutions de protection FirePower pour ISR Cisco (NGFWv)

• Conçue pour les succursales et les bureaux distants
• Inspection des menaces jusqu'à 800 Mbit/s
• Déploiement sur des routeurs série 4000 et ISR G2
• Sécurité renforcée et réduction des coûts liés au réseau WAN

Besoin d'infos ou d'un devis ?

CONTACT