Aperçu

Avantages

- **Éliminez plus de menaces** – connues et inconnues – avec la protection contre la menace la plus efficace du secteur.
- **Bénéficiez d'une meilleure visibilité** et d'un meilleur contrôle des utilisateurs, des applications, des appareils, des menaces et des vulnérabilités sur votre réseau.
- **Détectez et agissez plus** rapidement en réduisant le délai de détection des programmes de quelques mois à quelques heures et en mettant plus rapidement en œuvre un correctif.
- **Réduisez la complexité** et simplifiez vos opérations en regroupant toutes les fonctions de sécurité en une interface de gestion unique.
- **Optimisez votre réseau** en intégrant d'autres solutions de sécurité et de réseau Cisco.

Pare-feu de nouvelle génération Cisco Firepower

Premier pare-feu de nouvelle génération du secteur, entièrement intégré et axé sur les menaces

La plupart des pare-feu de nouvelle génération (NGFW) sont fortement axés sur l'activation du contrôle des applications, mais très peu sur leurs capacités de défense contre les menaces. Pour compenser, certains NGFW tenteront de rehausser leur capacité de prévention des intrusions de première génération par l'ajout d'une gamme de produits non intégrés. Cependant, cette méthode n'est pas optimale pour protéger votre entreprise contre les risques que posent les attaquants et les programmes malveillants virulents. De plus, une fois que vos systèmes sont infectés, ils n'offrent aucun soutien rapide pour l'évaluation, le confinement et la correction du problème.

Vous avez donc besoin d'un pare-feu de nouvelle génération intégré qui est axé sur les menaces. Un pare-feu qui fournit non seulement le contrôle granulaire des applications, mais également une protection efficace contre les menaces liées aux attaques de programmes malveillants virulents et évasifs.

Le pare-feu de nouvelle génération Cisco Firepower[MC] est le premier pare-feu de nouvelle génération axé sur les menaces et entièrement intégré de l'industrie. Il offre une gestion de politique unifiée et élaborée des fonctions de pare-feu, de contrôle des applications, de prévention des menaces et de protection avancée contre les programmes malveillants, allant du réseau jusqu'au point d'extrémité.

Il peut être déployé sur les appareils Cisco Firepower 4100 et 9300 pour offrir une plateforme de sécurité de nouvelle génération optimisée pour la densité et la performance en périphérie de l'Internet et d'autres environnements à haute performance.

Protégez votre entreprise, avant, pendant et après une attaque

Les appareils Cisco Firepower NGFW proposent le pare-feu dynamique le plus déployé de l'industrie et offrent un contrôle granulaire sur plus de 4 000 applications commerciales. Son interface de gestion unique offre une visibilité unifiée s'étendant du réseau jusqu'au point d'extrémité. Les appareils Cisco Firepower NGFW permettent une gestion de politique élaborée qui contrôle les accès, bloque les attaques, protège contre les programmes malveillants et fournit des outils intégrés pour détecter et confiner les attaques, puis se rétablir des attaques qui ont réussi à s'infiltrer.

Les appareils Cisco Firepower NGFW sont uniques dans le secteur, car c'est la seule nouvelle génération qui :

- fournit un système de prévention des intrusions de prochaine génération (NGIPS) qui assure une protection de pointe dans le secteur;
- offre une solution de protection avancée entièrement intégrée contre les programmes malveillants, capable de surmonter les menaces connues et inconnues, ainsi qu'un bac de sable intégré;
- vous donne la possibilité de détecter et de confiner les infections par programmes malveillants;
- effectue automatiquement la corrélation des événements menaçants et des vulnérabilités sur votre réseau de sorte que vous puissiez concentrer vos ressources sur les menaces les plus graves;
- analyse les faiblesses de votre réseau et recommande les meilleures politiques de sécurité à instaurer;
- intègre un certain nombre de produits de sécurité réseau de Cisco® pour rentabiliser vos investissements antérieurs et offrir une sécurité renforcée.

Prochaines étapes

Pour de plus amples renseignements, rendez-vous sur notre site Web à l'adresse www.cisco.com/go/NGFW.

C45-736624-00 02/16