Introduction à Cisco Cisco Secure Firewall Threat Defense Virtual

Cisco Cisco Secure Firewall Threat Defense Virtual (défense contre les menaces virtuelles) apporte la fonctionnalité de pare-feu de prochaine génération à des environnements virtualisés, ce qui permet à des politiques de sécurité cohérentes de faire le suivi des charges de travail dans vos environnements physiques, virtuels et en nuage, et entre les nuages.

De nos jours, les entreprises s'appuient sur un ensemble de points de contrôle physiques et virtuels pour répondre à leurs besoins en matière de sécurité de réseau. Elles ont besoin de la souplesse nécessaire pour déployer différents pare-feu physiques et virtuels dans un large éventail d'environnements tout en mettant en œuvre des politiques cohérentes dans les sites distants, les centres de données et tous les points situés entre eux. De la consolidation des centres de données aux réaffectations de bureaux, en passant par les fusions et les acquisitions, sans oublier les pics saisonniers de la demande pesant sur vos applications, la gamme de pare-feu virtuels de Cisco vous aide à simplifier la gestion de la sécurité grâce à la commodité des politiques unifiées et à la souplesse vous permettant de les déployer partout.

Cisco Secure Firewall Threat Defense Virtual combine le pare-feu réseau éprouvé de Cisco avec l'IPS Snort, le filtrage des URL et la défense contre les logiciels malveillants. Cela simplifie la protection contre les menaces grâce au déploiement de politiques de sécurité cohérentes dans les environnements de nuage physique, privé et public. Obtenez une visibilité approfondie de votre réseau et détectez rapidement l'origine et l'activité des menaces. Arrêtez ensuite les attaques avant qu'elles n'impactent sur vos opérations.

Cisco Secure Firewall Threat Defense Virtual est la solution virtualisée la plus prisée. Hiérarchisez les menaces grâce à des classements de risques automatisés et des indicateurs d'impact afin de concentrer vos ressources sur les événements nécessitant une action immédiate. La transférabilité des licences offre la possibilité de passer de votre nuage privé sur site au nuage public tout en maintenant des politiques cohérentes et une gestion unifiée pour tous vos périphériques. Les licences logicielles Smart de Cisco facilitent le déploiement, la gestion et le suivi des instances de pare-feu virtuel.

• Gestion du périphérique Cisco Secure Firewall Threat Defense Virtual, à la page 1

Gestion du périphérique Cisco Secure Firewall Threat Defense Virtual

Vous avez deux options pour gérer votre Cisco Secure Firewall Threat Defense Virtual.

Cisco Secure Firewall Management Center

Si vous gérez un grand nombre d'appareils, ou si vous voulez utiliser les fonctions et configurations plus complexes que permet défense contre les menaces, utilisez centre de gestion pour configurer vos appareils au lieu du gestionnaire d'appareil intégré.

Important Vous ne pouvez pas utiliser à la fois gestionnaire d'appareil et centre de gestion pour gérer l'appareil défense contre les menaces. Une fois que la gestion intégrée gestionnaire d'appareil est activée, il ne sera plus possible d'utiliser centre de gestion pour gérer le périphérique défense contre les menaces, à moins de désactiver la gestion locale et de reconfigurer la gestion pour utiliser centre de gestion. D'un autre côté, lorsque vous enregistrez le périphérique défense contre les menaces sur centre de gestion, le service de gestion intégrée gestionnaire d'appareil est désactivé.

Mise en garde Actuellement, Cisco n'offre pas la possibilité de migrer votre configuration gestionnaire d'appareil vers centre de gestion et vice versa. Tenez-en compte lorsque vous choisissez le type de gestion que vous configurez pour le périphérique défense contre les menaces.

Cisco Secure Firewall device manager

Le gestionnaire d'appareil est un gestionnaire intégré.

Le gestionnaire d'appareil est une interface de configuration Web incluse sur certains des périphériques défense contre les menaces. gestionnaire d'appareil vous permet de configurer les fonctions de base du logiciel qui sont le plus souvent utilisées pour les petits réseaux. Il est spécialement conçu pour les réseaux qui comprennent un seul périphérique ou quelques-uns, pour lesquels vous ne souhaitez pas utiliser un gestionnaire de périphériques multiples de grande puissance qui permet de contrôler un grand réseau contenant un grand nombre des périphériques défense contre les menaces.

Remarque Consultez Guide Cisco Secure Firewall Device Manager Configuration pour obtenir la liste des périphériques défense contre les menaces qui prennent en charge gestionnaire d'appareil.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.