SSNGFW-SECURING NETWORKS WITH CISCO FIREPOWER NEXT GENERATION FIREWALL V1.0

Course Code: 100700

Le cours « Sécurisation des réseaux avec le pare-feu nouvelle génération Cisco Firepower (SSNGFW) v1.0 » vous montre comment déployer et utiliser le système Cisco Firepower® Threat Defense.

Ce cours pratique vous permet d'acquérir les connaissances et les compétences nécessaires à l'utilisation et à la configuration de la technologie Cisco Firepower Threat Defense, en commençant avec l'installation et la configuration initiales des appareils et en incluant le routage, la haute disponibilité, la migration de Cisco Adaptive Security Appliance (ASA) vers Cisco Firepower Threat Defense, le contrôle du trafic et la traduction d'adresses réseau (NAT). Vous apprendrez à mettre en œuvre des fonctions avancées de pare-feu de nouvelle génération (NGFW) et de système de prévention des intrusions de nouvelle génération (NGIPS), notamment l'intelligence réseau, la détection des types de fichiers, la détection des logiciels malveillants basés sur le réseau et l'inspection approfondie des paquets. Vous apprendrez également à configurer le VPN site à site, le VPN d'accès à distance et le décryptage SSL avant de passer à l'analyse détaillée, à l'administration système et au dépannage.

Ce cours vous aide à vous préparer à l'examen, Securing Networks with Cisco Firepower (300-710 SNCF), qui mène aux certifications CCNP Security et Cisco Certified Specialist - Network Security Firepower. L'examen 300-710 SNCF comporte également un deuxième cours de préparation, Securing Networks with Cisco Firepower Next-Generation Intrusion Prevention System (SSFIPS). Vous pouvez suivre ces cours dans n'importe quel ordre.

Ce que vous apprendrez

- Décrire les concepts clés de la technologie NGIPS et NGFW et du système Cisco Firepower Threat Defense, et identifier les scénarios de déploiement.
- Effectuer la configuration initiale du dispositif Cisco Firepower Threat Defense et les tâches d'installation.
- Décrire comment gérer le trafic et mettre en œuvre la qualité de service (QoS) en utilisant Cisco Firepower Threat Defense.

- Décrire comment mettre en œuvre la NAT à l'aide de Cisco Firepower Threat Defense.
- Effectuer une découverte initiale du réseau, en utilisant Cisco Firepower pour identifier les hôtes, les applications et les services.
- Décrire le comportement, l'utilisation et la procédure de mise en œuvre des politiques de contrôle d'accès.
- Décrire les concepts et les procédures de mise en œuvre des fonctions de renseignement de sécurité
- Décrire Cisco Advanced Malware Protection (AMP) for Networks et les procédures de mise en œuvre du contrôle des fichiers et de la protection avancée contre les logiciels malveillants.
- Mettre en œuvre et gérer les politiques d'intrusion
- Décrire les composants et la configuration d'un VPN site à site.
- Décrire et configurer un VPN SSL d'accès à distance qui utilise Cisco AnyConnect
- Décrire les capacités de décryptage SSL et leur utilisation
- Mettre en œuvre Cisco Firepower NGFW pour fournir une protection avancée contre les menaces avant, pendant et après les attaques.
- Acquérir des compétences de pointe pour des responsabilités à forte demande axées sur la sécurité.

Qui doit être présent

- Administrateurs de sécurité
- Consultants en sécurité
- Administrateurs de réseaux
- Ingénieurs du système
- Personnel d'assistance technique
- Intégrateurs et partenaires Cisco

Prérequis

- Connaissance de TCP/IP et des protocoles de routage de base.
- Familiarité avec les concepts de pare-feu, de VPN et de système de prévention des intrusions (IPS).

Visitez-nous à www.globalknowledge.ca/fr ou appelez-nous au 1-866-716-6688.

Date de création: 5/9/2025 6:51:51 AM