Formation Sécuriser les réseaux avec Cisco Firepower Next Generation Firewall

Description de la formation Cisco Firewall

Cette **formation Sécuriser les réseaux avec Cisco Firepower Next Generation Firewall** vous montre comment déployer et utiliser le système de défense Cisco Firepower Threat Defense. Elle couvre les sujets suivants : l'installation et la configuration initiales des dispositifs et en incluant le routage, la haute disponibilité, la migration de l'ASA (Adaptive Security Appliance) vers Cisco Firepower Threat Defense, le contrôle du trafic et la traduction d'adresses réseau (NAT).

Vous apprendrez à mettre en œuvre les fonctionnalités avancées du pare-feu de nouvelle génération (NGFW) et du système de prévention des intrusions de nouvelle génération (NGIPS), notamment l'intelligence réseau, la détection des types de fichiers, la détection des logiciels malveillants sur le réseau et l'inspection approfondie des paquets. Vous verrez également comment configurer le VPN de 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.

Objectifs

À l'issue de cette **formation Cisco Firewall**, vous aurez acquis les connaissances et compétences nécessaires pour :

- Décrire les concepts clés des technologies NGIPS et NGFW et du système de défense contre les menaces Cisco Firepower, et identifier les scénarios de déploiement
- Effectuer les tâches initiales de configuration et d'installation des dispositifs de défense contre les menaces de Cisco Firepower

- 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 en utilisant 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 caractéristiques du renseignement de sécurité

À qui s'adresse cette formation ?

Public :

Cette formation Cisco Firewall s'adresse aux professionnels qui souhaitent apprendre comment déployer et gérer un Cisco Firepower NGIPS et NGFW dans leur environnement réseau.

Prérequis :

Pour suivre ce cours Cisco Firewall dans de bonnes conditions, Cisco recommande aux participants d'avoir une compréhension technique de la mise en réseau TCP/IP et de l'architecture réseau, et d'avoir une connaissance de base des concepts de pare-feu et d'IPS.

Contenu du cours Cisco Firewall

Présentation de Cisco Firepower Threat Defense

Examen de la technologie des pare-feu et IPS
Caractéristiques et composants de Firepower Threat Defense
Examen des plates-formes de Firepower
Cas d'utilisation de la mise en œuvre de Cisco Firepower

Configuration du dispositif Cisco Firepower Next Generation Firewall

Enregistrement des dispositifs à Firepower Threat Defense

FXOS et Firepower Device Manager

Configuration initiale de l'appareil

Gestion des dispositifs de NGFW

Examen des politiques du Centre de gestion de Firepower

Examen des objets

Examen de la configuration du système et de la surveillance de la santé

Gestion des appareils

Examen de la haute disponibilité de Firepower

Configuration de la haute disponibilité

Migration de Cisco ASA vers Firepower

Migration de Cisco ASA vers Firepower Threat Defense

Contrôle du trafic de Cisco Firepower Next Generation Firewall

Traitement des paquets de Firepower Threat Defense

Mise en œuvre de la QoS

Contournement de la circulation

Traduction d'adresses Cisco Firepower Next Generation Firewall

Principes de base du NAT

Implémentation de NAT

Exemples de règles NAT

Implémentation de NAT

Découverte de Cisco Firepower (Cisco Firepower Discovery)

Examen de la découverte du réseau

Configuration de la découverte du réseau

Mise en œuvre des politiques de contrôle d'accès

Examen des politiques de contrôle d'accès

Examen des règles de la politique de contrôle d'accès et des mesures par défaut

Mise en œuvre d'une inspection plus poussée

Examen des événements de connexion

Politique de contrôle d'accès Paramètres avancés

Considérations relatives à la politique de contrôle d'accès

Mise en œuvre d'une politique de contrôle d'accès

Security Intelligence

Examen de Security Intelligence

Examen des objets de Security Intelligence

Déploiement et enregistrement de Security Intelligence

Mise en œuvre de Security Intelligence

Contrôle des fichiers et protection avancée contre les logiciels malveillants

Examen des logiciels malveillants et de la politique des fichiers

Examen de la protection avancée contre les logiciels malveillants

Systèmes Next Generation de prévention des intrusions

Examen de la prévention des intrusions et des règles de Snort

Examen des variables et des ensembles de variables

Examen des politiques d'intrusion

VPN de site à site

Examen d'IPsec

Configuration VPN de site à site

Dépannage VPN de site à site

Mise en place d'un VPN de site à site

VPN d'accès à distance

Examen du VPN d'accès à distance

Examen de la cryptographie à clé publique et des certificats

Inscription au certificat d'examen

Configuration du VPN d'accès à distance

Mise en œuvre d'un VPN d'accès à distance

Décryptage SSL

Examen du décryptage SSL

Configuration des politiques SSL

Best Practices et surveillance du décryptage SSL

Techniques d'analyse détaillée

Examen de l'analyse des événements

Examen des types d'événements

Examen des données contextuelles

Examen des outils d'analyse

Analyse de la menace

Administration du système

Gestion des mises à jour

Examen des caractéristiques de la gestion des comptes utilisateurs

Configuration des comptes d'utilisateur

Administration du système

Dépannage de Cisco Firepower

Examen des erreurs de configuration courantes

Examen des commandes de dépannage

Dépannage de Firepower

Travaux Pratiques

Cette formation Cisco Firewall comporte de nombreux travaux pratiques qui vous inviteront à vous pencher sur les sujets suivants :

- Configuration initiale de l'appareil
- Gestion d'appareils
- Configuration de la haute disponibilité
- Migration de Cisco ASA vers Cisco Firepower Threat Defense
- Implémentation de la QoS
- Implémentation de NAT
- Configuration de la découverte du réseau
- Implémentation d'une politique de contrôle d'accès
- Implémentation de Security Intelligence
- Implémentation d'un VPN de site à site
- Implémentation d'un VPN d'accès à distance
- Analyse des menaces
- L'administration du système
- Dépannage de la puissance de feu