Security

Securing Networks with Cisco Firepower Next Generation Firewall

SSNGFW

Version : 1.0
5 Jours

Objectifs

A l'issue de ce cours, le stagiaire sera en mesure d'atteindre ses objectifs :

- 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 et les tâches de configuration du périphérique Cisco Firepower Threat Defense
- Décrire comment gérer le trafic et implémenter la qualité de service (QoS) à l'aide de Cisco Firepower Threat Defense
- Décrire comment implémenter NAT à l'aide de Cisco Firepower Threat Defense
- Effectuez une découverte initiale du réseau à l'aide de Cisco Firepower pour identifier les hôtes, les applications et les services
- Décrire le comportement, l'utilisation et la procédure de mise en œuvre des stratégies de contrôle d'accès
- Décrire les concepts et les procédures de mise en œuvre des fonctionnalités de renseignement de sécurité
- Décrire Cisco Advanced Malware Protection (AMP) pour les réseaux 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 des politiques d'intrusion
- Décrire les composants et la configuration d'un VPN de site à site
- Décrire et configurer un VPN SSL d'accès distant qui utilise Cisco AnyConnect®
- Décrire les capacités de décryptage SSL et leur utilisation

Public Concerné

- Administrateurs de sécurité
- Consultants en sécurité
- Administrateurs réseau
- Ingénieurs système
- Personnel de support technique
- Intégrateurs et partenaires Cisco

Pour plus d'informations : info@learneo.fr ou 01 53 20 37 00

Pré-requis

Avant de suivre ce cours, le stagiaire doit posséder les compétences et les connaissances suivantes :

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

Plan du cours détaillé

1. Présentation de Cisco Firepower Threat Defense
   - 1.1. Examen du pare-feu et de la technologie IPS
   - 1.2. Caractéristiques et composants de la défense contre les menaces de puissance de feu
   - 1.3. Examen des plates-formes de puissance de feu
   - 1.4. Examen des licences de défense contre les menaces de puissance de feu
   - 1.5. Cas d'utilisation d'implémentation de Cisco Firepower
2. Configuration du périphérique Cisco Firepower NGFW
   - 2.1. Enregistrement du dispositif de défense contre les menaces de puissance de feu
   - 2.2. FXOS et Firepower Device Manager
   - 2.3. Configuration initiale de l'appareil
   - 2.4. Gestion des appareils NGFW
   - 2.5. Examen des politiques du Firepower Management Center
   - 2.6. Examen des objets
   - 2.7. Examen de la configuration du système et de la surveillance de l'intégrité
   - 2.8. Gestion d'appareils
   - 2.9. Examen de la haute disponibilité de la puissance de feu
   - 2.10. Configuration de la haute disponibilité
   - 2.11. Migration de Cisco ASA vers Firepower
   - 2.12. Migration de Cisco ASA vers Firepower Threat Defense
3. Contrôle du trafic Cisco Firepower NGFW
   - 3.1. Traitement des paquets de défense contre les menaces de puissance de feu
   - 3.2. Implémentation de la QoS
   - 3.3. Contournement du trafic
4. Traduction d'adresse Cisco Firepower NGFW
   - 4.1. Notions de base NAT
   - 4.2. Implémentation de NAT
   - 4.3. Exemples de règles NAT
   - 4.4. Implémentation de NAT
5. Cisco Firepower Discovery
   - 5.1. Examen de la découverte du réseau

5.2. Configuration de la découverte du réseau

6. Implémentation de stratégies de contrôle d'accès

6.1. Examen des politiques de contrôle d'accès
6.2. Examen des règles de stratégie de contrôle d'accès et de l'action par défaut
6.3. Mise en œuvre d'une inspection supplémentaire
6.4. Examen des événements de connexion
6.5. Paramètres avancés de la stratégie de contrôle d'accès
6.6. Considérations relatives à la politique de contrôle d'accès
6.7. Implémentation d'une politique de contrôle d'accès

7. Intelligence de sécurité

7.1. Examen des renseignements de sécurité
7.2. Examen des objets de renseignement de sécurité
7.3. Déploiement et journalisation de Security Intelligence
7.4. Implémentation de Security Intelligence

8. Contrôle des fichiers et protection avancée contre les logiciels malveillants

8.1. Examen des politiques relatives aux programmes malveillants et aux fichiers
8.2. Examen de la protection avancée contre les logiciels malveillants

9. Systèmes de prévention des intrusions de nouvelle génération

9.1. Examen de la prévention des intrusions et des règles Snort
9.2. Examen des variables et des ensembles de variables
9.3. Examen des politiques d'intrusion

10. VPN de site à site

10.1. Examen IPsec
10.2. Configuration VPN de site à site
10.3. Dépannage de VPN de site à site
10.4. Implémentation d'un VPN de site à site

11. VPN d'accès à distance

11.1. Examen du VPN d'accès à distance
11.2. Examen de la cryptographie à clé publique et des certificats
11.3. Examen de l'inscription au certificat
11.4. Configuration VPN d'accès à distance
11.5. Implémentation d'un VPN d'accès à distance

12. Décryptage SSL

12.1. Examen du déchiffrement SSL
12.2. Configuration des politiques SSL
12.3. Meilleures pratiques et surveillance du déchiffrement SSL

13. Techniques d'analyse détaillées

13.1. Examen de l'analyse des événements
13.2. Examen des types d'événements
13.3. Examen des données contextuelles
13.4. Examen des outils d'analyse
13.5. Analyse des menaces

14. L'administration du système
14.1. Gérer les mises à jour
14.2. Examen des fonctionnalités de gestion des comptes d'utilisateurs
14.3. Configuration des comptes d'utilisateurs
14.4. L'administration du système

15. Dépannage de Cisco Firepower
15.1. Examen des erreurs de configuration courantes
15.2. Examen des commandes de dépannage
15.3. Dépannage de la puissance de feu

Laboratoire

- 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

Mode d'évaluation des acquis

Evaluation par le formateur oralement chaque jour et auto-évaluation formalisée sur le Moodle.

Certification

Cette formation vous aide à vous préparer à l'examen 300-710 SNCF