SECURING NETWORKS WITH CISCO FIREPOWER NEXT GENERATION FIREWALL

Cette formation vous apprend comment déployer et utiliser le système Cisco Firepower® Threat Defense (FTD). Sa partie pratique vous permet d'acquérir les connaissances nécessaires pour utiliser et configurer la technologie Cisco® Firepower Threat Defense, en commençant par l'installation et la configuration initiales de ce système.

CURSUS:
CISCO

CODE DE LA FORMATION:
CS-SC-SSNGFW

ÉDITEUR OU CONSTRUCTEUR:
CISCO

VERSION:
1.0

DURÉE:
5 JOURS

PRÉREQUIS:

Pour bénéficier pleinement de ce cours, vous devez disposer de:

- Très bonnes connaissances de la pile TCP/IP ainsi que des protocoles de routage de base.
- Familiarité avec les concepts relatifs aux pare-feux (firewalls), les VPNs et les systèmes de prévention des intrusions (IPS).

Le suivis des cours CCNA et SFNDU est fortement recommandé

PUBLIC:

Cette formation s'adresse aux:

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

OBJECTIFS:

Après avoir suivi ce cours, vous devriez pouvoir:

- 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 Cisco Firepower Threat Defense.
- Décrire comment gérer le trafic et implémenter la qualité de service (QoS) à l'aide du Cisco Firepower Threat Defense.
- Décrire comment implémenter NAT à l'aide du Cisco Firepower Threat Defense.
- Effectuez une découverte 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 d'implémentation des règles de contrôle d'accès (ACLs).
- Décrire les concepts et les procédures de mise en œuvre des fonctionnalités « security intelligence ».

- Décrire le concept du Cisco Advanced Malware Protection (AMP) pour les réseaux ainsi que 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 règles de détection d'intrusion.

- Décrire les composants et la configuration d'un VPN de site à site.
- Décrire et configurer un VPN SSL pour l'accès distant en utilisant le client Cisco AnyConnect®.
- Décrire les fonctionnalités de déchiffrement SSL et leur utilisation.

CONTENU:

Présentation du Cisco Firepower Threat Defense

- Etude du pare-feu et de la technologie IPS
- Caractéristiques et composants du Cisco Firepower Threat Defense
- Etude des plateformes Firepower
- Etude des licences du Cisco Firepower Threat Defense
- Cas d'implémentation du Cisco Firepower

Configuration du Cisco Firepower NGFW

- Enregistrement du de Cisco Firepower Threat Defense
- Le FXOS et le Firepower Device Manager
- Configuration initiale du Cisco Firepower Threat Defense
- Gestion des NGFWs
- Etude des règles du Firepower Management Center
- Etudes des objets
- Etude de la configuration et du Health Monitoring
- Gestion d'appareils
- Etude de la haute disponibilité (HA)
- Configuration de la haute disponibilité (HA)
- Migration du Cisco ASA vers le Firepower
- Migration du Cisco ASA vers Firepower Threat Defense

Acheminement du trafic sur le Cisco Firepower NGFW

- Traitement des paquets sur le Cisco Firepower Threat Defense
- Implémentation de la QoS
- Contournement du trafic

Traduction d'adresse Cisco Firepower NGFW

- Notions de base sur le NAT
- Implémentation du NAT
- Exemples de règles NAT

Cisco Firepower Discovery

- Etude de la découverte du réseau
- Configuration de la découverte du réseau

Implémentation des règles de contrôle d'accès (ACL)

- Etude des règles de contrôle d'accès
- Etude des règles de contrôle d'accès et de l'action par défaut
- Mise en œuvre d'une inspection supplémentaire
- Etude des événements de connexion
- Paramètres avancés des règles de contrôle d'accès
- Considérations relatives aux règles de contrôle d'accès
- Implémentation d'une règle de contrôle d'accès

La Security Inteligence

- Etude de la Security Inteligence
- Etude des objets de la Security Inteligence
- Déploiement et journalisation de la Security Intelligence
- Implémentation de la Security Inteligence

Contrôle des fichiers et protection avancée contre les logiciels malveillants (AMP)

- Etude des règles « Malware and File »

- Etude du AMP

Systèmes de prévention des intrusions de nouvelle génération (NGIPS)

- Etude du système de prévention d’intrusions et des règles Snort
- Etude des variables et des ensembles de variables
- Etude des règles de détection d'intrusion

VPN site-à-site

- Etude du protocole IPsec
- Configuration du VPN site-à-site
- Dépannage du VPN site-à-site
- Implémentation d'un VPN site-à site

VPN pour l'accès à distance

- Etude du VPN pour l’accès à distance
- Etude de la cryptographie à clé publique et des certificats
- Etude de l'inscription des certificats
- Configuration du VPN pour l'accès à distance
- Implémentation d'un VPN pour l'accès à distance

Déchiffrement SSL

- Etude du déchiffrement SSL
- Configuration des règles SSL
- Meilleures pratiques et gestion du déchiffrement SSL

Techniques d'analyse avancées

- Etude de l'analyse d’événements
- Etude des types d'événements
- Etude des données contextuelles
- Etude des outils d'analyse
- Analyse des menaces

L'administration du système

- Gestion des mises à jour
- Etude des fonctionnalités de gestion des comptes utilisateurs
- Configuration des comptes utilisateurs
- L'administration du système

Dépannage du Cisco Firepower

- Etude des erreurs de configuration courantes
- Etude des commandes de dépannage
- Dépannage du Firepower

CERTIFICATION:

Cette formation prépare à l'examen Cisco 300-710 SNCF