MAJ : le 19/08/2021

SSNGFW – Sécurisation des réseaux avec le pare-feu Cisco Firepower Next Generation

- Durée : 5 Jours (35h)
- Tarif en présentiel ou en classe à distance : 4 260 € HT
- Tarif en E-Learning: 1 000 € HT

A qui s'adresse ce cours ?

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

Pré-Requis

Pour profiter pleinement de ce cours, vous devez posséder les connaissances et compétences 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)

Moyens pédagogiques

Accueil des stagiaires dans une salle dédiée à la formation ou espace WebEx "Zoom, Teams....." en classe à distance
Modalité : Formation réalisée en présentiel ou à distance selon la formule retenue
Méthode : Un formateur expert, Labs à distance, Quiz en salle
Documentées : Support en anglais projeté et remis en PDF téléchargeable

Modalités de suivi et d'évaluation

Formulaires d'évaluations de la formation : pré-évaluation avant formation, évaluation de la satisfaction en fin de stage, évaluation des acquis à +90 jours
Feuille de présence émargée par demi-journée par les stagiaires et le formateur
Attestation de fin de formation
Analyse des attentes client

Accessibilité :
La formation est accessible aux personnes à mobilité réduite.
Une étude des conditions d'accès et des moyens de compensation sera réalisé en amont à l'inscription afin d'identifier plus précisément les conditions de réalisation et de faisabilité de la formation.
Vous pouvez trouver toutes les informations nécessaires sur notre site :
https://bigso.fr/accueil/formations/

Objectifs

A l'issue de la formation, vous serez capable de :

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
Effectuer 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

La sécurisation des réseaux avec le pare-feu Cisco Firepower nouvelle génération (SSNGFW) Le cours v1.0 vous montre comment déployer et utiliser le système Cisco Firepower Threat Defense. Ce cours pratique vous donne les connaissances et les compétences nécessaires pour utiliser et configurer la technologie Cisco Firepower Threat Defense, en commençant par l'installation et la configuration initiales des périphériques et en incluant le routage, la haute disponibilité, Cisco Adaptive Security Appliance (ASA) vers la migration de Cisco Firepower Threat Defense, le trafic contrôle et traduction d'adresses réseau (NAT). Vous apprendrez comment implémenter des fonctionnalités 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 de type de fichier, la détection de logiciels malveillants en réseau et l'inspection approfondie des paquets. Vous apprendrez également à configurer le VPN de site à site, le VPN d'accès à distance et le déchiffrement SSL avant de passer à l'analyse détaillée, à l'administration système.

Déroulement du cours

Présentation de Cisco Firepower Threat Defense

- Examen du pare-feu et de la technologie IPS
- Caractéristiques et composants de la défense contre les menaces de puissance de feu
- Examen des plates-formes de puissance de feu
- Examen des licences de défense contre les menaces de puissance de feu
- Cas d'utilisation d'implémentation de Cisco Firepower

Configuration du périphérique Cisco Firepower NGFW

- Enregistrement du dispositif de défense contre les menaces de puissance de feu
- FXOS et Firepower Device Manager
- Configuration initiale de l'appareil
- Gestion des appareils NGFW
- Examen des politiques du Firepower Management Center
- Examen des objets
- Examen de la configuration du système et de la surveillance de l'intégrité
- Gestion d'appareils
- Examen de la haute disponibilité de la puissance de feu
- Configuration de la haute disponibilité
- Migration de Cisco ASA vers Firepower
- Migration de Cisco ASA vers Firepower Threat Defense

Contrôle du trafic Cisco Firepower NGFW

- Traitement des paquets de défense contre les menaces de puissance de feu
- Implémentation de la QoS
- Contournement du trafic

Traduction d'adresse Cisco Firepower NGFW

- Notions de base NAT
- Implémentation de NAT
- Exemples de règles NAT
- Implémentation de NAT

Cisco Firepower Discovery

- Examen de la découverte du réseau
- Configuration de la découverte du réseau

Implémentation de stratégies de contrôle d'accès

- Examen des politiques de contrôle d'accès
- Examen des règles de stratégie de contrôle d'accès et de l'action par défaut
- Mise en œuvre d'une inspection supplémentaire
- Examen des événements de connexion
- Paramètres avancés de la stratégie de contrôle d'accès
- Considérations relatives à la politique de contrôle d'accès
- Implémentation d'une politique de contrôle d'accès

Intelligence de sécurité

- Examen des renseignements de sécurité
- Examen des objets de renseignement de sécurité
- Déploiement et journalisation de Security Intelligence
- Implémentation de Security Intelligence

Contrôle des fichiers et protection avancée contre les logiciels malveillants

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

Systèmes de prévention des intrusions de nouvelle génération

- Examen de la prévention des intrusions et des règles Snort
- Examen des variables et des ensembles de variables
- Examen des politiques d'intrusion

VPN de site à site

- Examen IPsec
- Configuration VPN de site à site
- Dépannage de VPN de site à site
- Implémentation 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
- Examen de l'inscription au certificat
- Configuration VPN d'accès à distance
- Implémentation d'un VPN d'accès à distance

Décryptage SSL

- Examen du déchiffrement SSL
- Configuration des politiques SSL
- Meilleures pratiques et surveillance du déchiffrement SSL

Techniques d'analyse détaillées

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

L’administration du système

Gérer les mises à jour
Examen des fonctionnalités de gestion des comptes d’utilisateurs
Configuration des comptes d’utilisateurs
L’administration du système

Dépannage de Cisco Firepower

Examen des erreurs de configuration courantes
Examen des commandes de dépannage
Dépannage de la puissance de feu

Aperçu du lab

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

ALLEZ PLUS LOIN

L’examen 300-710 SNCF certifie votre connaissance de Cisco Firepower Threat Defense et Firepower, y compris les configurations de politiques, les intégrations, les déploiements, la gestion et le dépannage.

Après avoir passé 300-710 SNCF :

Vous obtenez la certification Cisco Certified Specialist – Network Security Firepower. Vous aurez satisfait aux exigences de l’examen de concentration pour la nouvelle certification de sécurité CCNP. Pour compléter votre CCNP Sécurité, vous devez également réussir l’examen de mise en œuvre et d’exploitation des technologies de base de sécurité Cisco (350-701 SCOR) ou son équivalent.