Securing networks with Cisco Firepower Next Generation Firewall (SSNGFW) v1.0

Cours officiel, préparation partielle à l'examen 300-710 SNCF

Cours Pratique de 5 jours - 35h
Réf : PPX - Prix 2024 : 4 490€ HT

Avec cette formation "Sécuriser les réseaux avec les firewalls de dernière génération Cisco Firepower", vous apprendrez à déployer et à utiliser le système Cisco Firepower® Threat Defense. Vous aborderez l'installation et la configuration initiales de l'appareil et y compris le routage, la haute disponibilité, la migration Cisco Adaptive Security Appliance (ASA) vers Cisco Firepower Threat Defense, le trafic contrôle et translation d'adresses réseau (NAT). Vous apprendrez à mettre en œuvre des fonctionnalités avancées de pare-feu de nouvelle génération, et bien plus encore.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

Décrire les concepts clés des technologies NGIPS et NGFW et du système de défense contre les menaces Cisco Firepower

Identifier les scénarios de déploiement

Effectuer les tâches initiales de configuration et d'installation du matériel 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 mettre en œuvre la NAT en utilisant Cisco Firepower Threat Defense

Effectuer une découverte initiale du réseau avec Cisco Firepower pour identifier les hôtes, les applications, etc.

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 des contrôles

Mettre en œuvre et gérer les stratégies d'intrusion

Décrire les composants et la configuration du VPN de site à site

Décrire et configurer un VPN SSL d'accès à distance qui utilise Cisco AnyConnect®

Décrire les capacités et l'utilisation du déchiffrement SSL

MÉTHODES PÉDAGOGIQUES

Animation de la formation en français. Support de cours officiel en anglais.

CERTIFICATION

Pour l'obtention de la certification Cisco Certified Network Professional Security (CCNP Security), la réussite de l'examen 350-701 SCOR est requise ainsi que la réussite de l'un des examens suivants (au choix) : 300-710 SNCF, 300-715 SISE, 300-720 SESA, 300-725 SWSA et 300-730 SVPN.

PARTICIPANTS

Administrateurs de sécurité, conseillers en sécurité, administrateurs réseau, ingénieurs système, personnel de soutien technique, intégrateurs et partenaires Cisco.

PRÉREQUIS

Compréhension technique de TCP/IP et de l'architecture réseau. Connaissance de base des concepts de pare-feu et d'IPS.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils sont agréés par l'éditeur et sont certifiés sur le cours. Ils ont aussi été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum trois à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Évaluation des compétences visées en amont de la formation.
Évaluation par le participant, à l'issue de la formation, des compétences acquises durant la formation.
Validation par le formateur des acquis du participant en précisant les outils utilisés : QCM, mises en situation…
À l'issue de chaque stage, ITTCERT fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques. Les participants réalisent aussi une évaluation officielle de l'éditeur.
Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le participant a bien assisté à la totalité de la session.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

Les ressources pédagogiques utilisées sont les supports et les travaux pratiques officiels de l'éditeur.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

LE PROGRAMME

dernière mise à jour : 12/2021

1) Présentation de Cisco Firepower Threat Defense

- Examen de la technologie pare-feu et IPS.
- Fonctionnalités et composants de Firepower Threat Defense.
- Examen des plateformes Firepower.
- Examen des licences de défense contre les menaces de Firepower.

Travaux pratiques : Cas d'utilisation de la mise en œuvre de Cisco FirePower

2) Configuration du périphérique Cisco Firepower NGFW

- Enregistrement du dispositif de défense contre les menaces Firepower.
- Gestionnaire de périphériques FXOS et Firepower.
- Configuration initiale de l'appareil.
- Gestion des appareils NGFW.
- Examen des stratégies du centre de gestion de Firepower.
- Examen des objets.
- Examen de la configuration du système et de la surveillance de l'état.
- Gestion d'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.

3) Contrôle du trafic Cisco Firepower NGFW

- Traitement des paquets de défense contre les menaces Firepower.
- Implémentation de la qualité de service.
- Contournement du trafic.

4) Traduction d'adresses Cisco Firepower NGFW

- Bases de NAT.
- Implémentation de la NAT.
- Exemples de règles de la NAT.

5) Découverte de Cisco Firepower

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

6) Implémentation des stratégies de contrôle d'accès

- Examen des stratégies 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 sur la stratégie de contrôle d'accès.
- Mise en œuvre d'une stratégie de contrôle d'accès.

7) Renseignement de sécurité

- Examen du renseignement de sécurité.
- Examen des objets de renseignement de sécurité.
- Déploiement et journalisation du renseignement de sécurité.
- Mise en œuvre du renseignement de sécurité.

8) Contrôle des fichiers et protection avancée contre les logiciels malveillants
- Examen des programmes malveillants et de la stratégie de fichiers.
- Examen de la protection avancée contre les logiciels malveillants.

9) Systèmes de prévention des intrusions de nouvelle génération
- Examen des règles de prévention des intrusions.
- Examen des variables et des ensembles de variables.
- Examen des stratégies d'intrusion.

10) VPN de site à site
- Examen d'IPsec.
- Configuration VPN de site à site.
- Dépannage VPN de site à site.
- Implémentation du VPN de site à site.

11) VPN d'accès à distance
- Examen du VPN d'accès à distance.
- Examen de la cryptographie et des certificats à clé publique.
- Examen de l'inscription au certificat.
- Configuration VPN d'accès à distance.
- Implémentation d'un VPN d'accès à distance.

12) Décryptage SSL
- Examen du décryptage SSL.
- Configuration des stratégies SSL.
- Meilleures pratiques et surveillance de décryptage SSL.

13) 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.

14) Administration du système
- Gestion des mises à jour.
- Examen des fonctionnalités de gestion des comptes d'utilisateurs.
- Configuration des comptes d'utilisateurs.
- Administration du système.

15) Dépannage de Cisco Firepower
- Examen des erreurs de configuration courantes.
- Examen des commandes de dépannage.
- Dépannage de Firepower.

16) Travaux pratiques officiels
- Exécuter la configuration initiale de l'appareil.
- Gérer les appareils.
- Configurer la haute disponibilité.
- Migrer de Cisco ASA vers Cisco Firepower Threat Defense.
- Mise en œuvre de la qualité de service.
- Implémenter le NAT.
- Configurer la découverte réseau.
- Mettre en œuvre une stratégie de contrôle d'accès.
- Mettre en œuvre du renseignement de sécurité.

- Implémenter du VPN de site à site.
- Implémenter un VPN d'accès à distance.
- Analyser les menaces.
- Gérer l'administration du système.
- Dépanner Firepower.

LES DATES

CLASSE À DISTANCE
2024 : 09 sept., 25 nov.