Formation : Advanced Techniques for Cisco Firewall Threat Defense and Intrusion Prevention (SFWIPA)

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

Cours pratique - 5j - 35h00 - Réf. PPX
Prix : 4350 € H.T.

Nouvelle édition

Avec cette formation vous apprendrez à déployer et configurer Cisco Secure Firewall Threat Defense et ses fonctionnalités en tant que pare-feu de réseau de centre de données ou de périphérie Internet avec support VPN. Vous apprendrez également à configurer des politiques basées sur l'identité, le décryptage SSL, les VPN d'accès à distance et de site à site, ainsi que des fonctionnalités avancées comme l'IPS, la gestion des événements, les intégrations système, le dépannage avancé, l'automatisation via API, et la migration des configurations (ASA) Cisco Secure Firewall.

Objectifs pédagogiques

À l'issue de la formation, le participant sera en mesure de :

- Décrire Cisco Secure Firewall Threat Defense
- Décrire les options de déploiement avancées de Cisco Secure Firewall Threat Defense
- Configurer le routage dynamique sur Cisco Secure Firewall Threat Defense
- Configurer la traduction d'adresse réseau avancée (NAT)
- Configurer la politique de décryptage SSL
- Déployer un VPN IPsec de site à site et un VPN d'accès à distance
- Déployer des politiques basées sur l'identité
- Déployer des paramètres de contrôle d'accès avancés (ACP)
- Dépanner le flux de trafic à l'aide des options avancées
- Décrire la gestion avancée des événements sur Cisco Secure Firewall Threat Defense

Public concerné

Installateurs de systèmes, intégrateurs de systèmes, administrateurs de systèmes, administrateurs de réseaux et concepteurs de solutions.

PARTICIPANTS

Installateurs de systèmes, intégrateurs de systèmes, administrateurs de systèmes, administrateurs de réseaux et concepteurs de solutions.

PRÉREQUIS

Connaissance du protocole TCP/IP et des protocoles de routage. Familiarité avec le contenu de la formation "Securing Internet Edge avec Cisco Secure Firewall Threat Defense".

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 formation, 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.

Prérequis

Connaissance du protocole TCP/IP et des protocoles de routage. Familiarité avec le contenu de la formation "Securing Internet Edge avec Cisco Secure Firewall Threat Defense".

Méthodes et moyens pédagogiques

Méthodes pédagogiques

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

Modalités d'évaluation

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…

Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

Programme de la formation

1 Programme officiel

- Introduction à Cisco Secure Firewall Threat Defense.
- Décrire des options de déploiement avancées sur Cisco Secure Firewall Threat Defense.
- Configurer les paramètres avancés des périphériques sur Cisco Secure Firewall Threat Defense.
- Configurer le routage dynamique sur Cisco Secure Firewall Threat Defense.
- Configurer NAT avancée sur Cisco Secure Firewall Threat Defense.
- Configurer la politique SSL sur Cisco Secure Firewall Threat Defense.
- Déployer un accès à distance VPN sur Cisco Secure Firewall Threat Defense.
- Déployer des politiques basées sur l'identité sur Cisco Secure Firewall Threat Defense.
- Déployer un VPN site à site sur Cisco Secure Firewall Threat Defense.
- Configurer des règles Snort et des politiques d'analyse du réseau.
- Décrire la gestion avancée des événements sur Cisco Secure Firewall Threat Defense.
- Décrire des intégrations sur Cisco Secure Firewall Threat Defense.
- Dépanner des flux de trafic avancés sur Cisco Secure Firewall Threat Defense.
- Automatiser Cisco Secure Firewall Threat Defense.
- Migrer vers Cisco Secure Firewall Threat Defense

2 Travaux pratiques officiels

- Déployer des paramètres de connexion avancés.
- Configurer le routage dynamique.
- Configurer la politique SSL.
- Configurer le VPN d'accès à distance.
- Configurer le VPN site à site.
- Personnaliser les politiques IPS et NAP.
- Configurer les intégrations de défense contre les menaces de Cisco Secure Firewall.
- Dépanner Cisco Secure Firewall Threat Defense.
- Migrer la configuration de Cisco Secure Firewall ASA.

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.

Options

Certification : 330 € HT

Cette formation vous prépare à l'examen 300-710 Securing Networks with Cisco Firepower (SNCF). En cas de réussite, vous obtenez la certification "Cisco Certified Specialist - Network Security Firepower" et répondez aux exigences de l'examen de concentration pour la certification "Cisco Certified Networking Professional (CCNP) Security".

Comment passer votre examen ?

L'option de certification se présente sous la forme d'un voucher ou d'une convocation qui vous permettra de passer l'examen à l'issue de la formation.