Fundamentals of Cisco Firewall Threat Defense and Intrusion Prevention (SFWIPF)

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

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

Avec cette formation vous apprendrez à mettre en œuvre et configurer Cisco Secure Firewall Threat Defense pour un déploiement en tant que pare-feu de nouvelle génération à la périphérie d'internet. Vous découvrirez l'architecture et le déploiement de Cisco Secure Firewall, la configuration de base, le traitement des paquets et les options avancées, ainsi que le dépannage de l'administration de Cisco Secure Firewall.

PARTICIPANTS
Ingénieurs en sécurité des réseaux. Administrateurs.

PRÉREQUIS
Compréhension des réseaux TCP/IP et des protocoles de routage de base, ainsi que des concepts de pare-feu, de VPN 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.

OBJECTIFS PÉDAGOGIQUES

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

Décrire la défense contre les menaces de Cisco Secure Firewall

Décrire les options de déploiement de Cisco Secure Firewall Threat Defense

Décrire les options de gestion de Cisco Secure Firewall Threat Defense

Configurer les paramètres initiaux de base de Cisco Secure Firewall Threat Defense

Configurer la haute disponibilité sur Cisco Secure Firewall Threat Defense

Configurer la traduction d'adresses réseau de base sur Cisco Secure Firewall Threat Defense

Décrire les politiques de Cisco Secure Firewall Threat Defense

Expliquer comment les différentes politiques influencent le traitement des paquets par l'appareil

Configurer la politique de découverte sur Cisco Secure Firewall Threat Defense

Configurer et expliquer les règles de préfiltre et de tunnel dans la politique de préfiltre

Configurer une politique de contrôle d'accès sur Cisco Secure Firewall Threat Defense

Configurer l'intelligence de sécurité sur Cisco Secure Firewall Threat Defense

Configurer la politique de fichiers sur Cisco Secure Firewall Threat Defense

Configurer la politique d'intrusion sur Cisco Secure Firewall Threat Defense

Effectuer une analyse de base des menaces à l'aide du Cisco Secure Firewall Management Center

Effectuer des tâches de gestion et d'administration système de base sur Cisco Secure Firewall Threat Defense

Effectuer un dépannage de base du flux de trafic sur Cisco Secure Firewall Threat Defense

Gérer Cisco Secure Firewall Threat Defense avec Cisco Secure Firewall Threat Defense Manager

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 d'un examen de concentration tel que l'examen de concentration 300-710 Securing Networks with Cisco Firepower (SNCF).

LE PROGRAMME

dernière mise à jour : 06/2024

1) Programme officiel

- Présentation de Cisco Secure Firewall Threat Defense.
- Décrire des options de déploiement de Cisco Secure Firewall Threat Defense.
- Décrire des options de gestion de Cisco Secure Firewall Threat Defense.
- Configurer des paramètres réseau de base sur Cisco Secure Firewall Threat Defense.

- Configurer la haute disponibilité sur Cisco Secure Firewall Threat Defense.
- Configurer la NAT automatique sur Cisco Secure Firewall Threat Defense.
- Décrire le traitement des paquets et des politiques sur Cisco Secure Firewall Threat Defense.
- Configurer la politique de découverte sur Cisco Secure Firewall Threat Defense.
- Configurer la politique de préfiltrage sur Cisco Secure Firewall Threat Defense.
- Configurer la politique de contrôle d'accès sur Cisco Secure Firewall Threat Defense.
- Configurer Security Intelligence sur Cisco Secure Firewall Threat Defense.
- Configurer la politique de fichiers sur Cisco Secure Firewall Threat Defense.
- Configurer la politique d'intrusion sur Cisco Secure Firewall Threat Defense.
- Exécuter une analyse de base des menaces sur le centre de gestion de Cisco Secure Firewall.
- Gérer le système de défense contre les menaces de Cisco Secure Firewall.
- Dépanner un du flux de trafic de base.
- Gérer les périphériques Cisco Secure Firewall Threat Defense.

2) Travaux pratiques officiels

- Effectuer la configuration initiale de l'appareil.
- Configurer la haute disponibilité.
- Configurer la traduction d'adresses de réseau.
- Configurer la découverte du réseau.
- Configurer le préfiltre et la politique de contrôle d'accès.
- Configurer l'intelligence sécuritaire.
- Mettre en œuvre le contrôle des fichiers et la protection avancée contre les logiciels malveillants.
- Configurer Cisco Secure IPS.
- Analyser en détail à l'aide du centre de gestion des pare-feu (Firewall Management Center).
- Gérer le système de défense contre les menaces de Cisco Secure Firewall.
- Principes de base du dépannage des pare-feux sécurisés.
- Configurer les périphériques gérés à l'aide de Cisco Secure Firewall Device Manager.

LES DATES

CLASSE À DISTANCE
2024 : 23 sept., 16 déc.