Cisco - Offre officielle certifiante

Cisco Firewall Threat Defense - Advanced Techniques and Intrusion Prevention

5 jours (35h00) | ★★★★½ 4,6/5 | SFWIPA | Certification 300-710 (non incluse) | Évaluation qualitative de fin de stage | Formation délivrée en présentiel ou distanciel

Contenu mis à jour le 13/10/2023. Document téléchargé le 23/09/2024.

Objectifs de formation

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

- Décrire Cisco Secure Firewall Threat Defense
- Décrire les options de déploiement avancées de Cisco Secure Firewall Threat Defense
- Décrire les paramètres avancés de l'appareil Cisco Secure Firewall Threat Defense
- Configurer le routage dynamique sur Cisco Secure Firewall Threat Defense
- Configurer la traduction d'adresse réseau avancée sur Cisco Secure Firewall Threat Defense
- Configurer la politique de décryptage SSL sur Cisco Secure Firewall Threat Defense
- Déployer le VPN d'accès à distance sur Cisco Secure Firewall Threat Defense
- Déployer des politiques basées sur l'identité sur Cisco Secure Firewall Threat Defense
- Déployer un VPN IPsec de site à site sur Cisco Secure Firewall Threat Defense
- Déployer des paramètres de contrôle d'accès avancés sur Cisco Secure Firewall Threat Defense
- Décrire la gestion avancée des évènements sur Cisco Secure Firewall Threat Defense
- Décrire les intégrations disponibles avec Cisco Secure Firewall Threat Defense
- Dépanner le flux de trafic à l'aide des options avancées de Cisco Secure Firewall Threat Defense
- Décrire les avantages de l'automatisation de la configuration et des opérations de Cisco Secure Firewall Threat Defense
- Décrire la migration de la configuration vers Cisco Secure Firewall Threat Defense.

Modalités, méthodes et moyens pédagogiques

Formation délivrée en présentiel ou distanciel* (blended-learning, e-learning, classe virtuelle, présentiel à distance).

Le formateur alterne entre méthode** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

Variables suivant les formations, les moyens pédagogiques mis en oeuvre sont :

- Ordinateurs Mac ou PC (sauf pour certains cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel)
- Environnements de formation installés sur les postes de travail ou en ligne
- Supports de cours et exercices

En cas de formation intra sur site externe à M2i, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatiques...) au bon déroulement de l'action de formation visée conformément aux prérequis indiqués dans le programme de formation communiqué.

* *nous consulter pour la faisabilité en distanciel*

** *ratio variable selon le cours suivi*

Prérequis

Avoir suivi les cours CCNA "Cisco Solutions - Implementing and administering" et SFWIPF "Cisco Firewall Threat Defense - Fundamentals and Intrusion Prevention", ou avoir les connaissances équivalentes. Connaître le protocole de contrôle de transmission/protocole Internet (TCP/IP) et avoir des connaissances de base des protocoles de routage.

Public concerné

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

Cette formation :

- Est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par M2i Formation
- Bénéficie d'un suivi de son exécution par une feuille de présence émargée par demi-journée par les stagiaires et le formateur.

Programme

Présentation de Cisco Secure Firewall Threat Defense

Description des options de déploiement avancées sur Cisco Secure Firewall Threat Defense

Configuration des paramètres avancés des périphériques sur Cisco Secure Firewall Threat Defense

Configuration du routage dynamique sur Cisco Secure Firewall Threat Defense

Configuration de la NAT avancée sur Cisco Secure Firewall Threat Defense

Configuration de la politique SSL sur Cisco Secure Firewall Threat Defense

Déploiement d'un accès à distance VPN sur Cisco Secure Firewall Threat Defense

Déploiement de politiques basées sur l'identité sur Cisco Secure Firewall Threat Defense

Déploiement d'un VPN site à site sur Cisco Secure Firewall Threat Defense

Configuration des règles Snort et des politiques d'analyse du réseau

Description de la gestion avancée des évènements sur Cisco Secure Firewall Threat Defense

Description des intégrations sur Cisco Secure Firewall Threat Defense

Dépannage des flux de trafic avancés sur Cisco Secure Firewall Threat Defense

Automatisation de Cisco Secure Firewall Threat Defense

Migration vers Cisco Secure Firewall Threat Defense

Labs

- *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*

Certification (en option)

- Prévoir l'achat de la certification en supplément
- Le passage de l'examen se fera (ultérieurement) dans un centre agréé Pearson Vue
- L'examen (en anglais) s'effectue en ligne, et durera en moyenne 1h30

Le contenu de ce programme peut faire l'objet d'adaptation selon les niveaux, prérequis et besoins des apprenants.

Modalités d’évaluation des acquis

- En cours de formation, par des évaluations formatives, à travers des travaux pratiques réalisés sur les labs (à l'issue de chaque module)
- Et/ou, en fin de formation, par une certification (proposée en option)

Les + de la formation

Le support de cours et les labs sont en anglais.

Accessibilité de la formation

Le groupe M2i s'engage pour faciliter l'accessibilité de ses formations. Les détails de l'accueil des personnes en situation de handicap sont consultables sur la page Accueil et Handicap.

Modalités et délais d’accès à la formation

Les formations M2i sont disponibles selon les modalités proposées sur la page programme.
Les inscriptions sont possibles jusqu'à 48 heures ouvrées avant le début de la formation.
Dans le cas d'une formation financée par le CPF, ce délai est porté à 11 jours ouvrés.