

## Formation CISCO SFWIPA, Sécuriser les réseaux avec les IPS de dernière génération Cisco Firepower

### Présentation

Cette formation prépare à la/aux certifications Cisco Certified Network Professional Security (CCNP SECURITY)

Durée : 35,00 heures (5 jours)

Tarif INTRA : Nous consulter

### Objectifs de la formation

A l'issue de la formation, vous serez en mesure 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 événements 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

## Prérequis

- Les connaissances et les compétences que vous êtes censé posséder avant de participer à cette formation sont les suivantes :
- Connaissance du protocole de contrôle de transmission/protocole Internet (TCP/IP)
- Connaissance de base des protocoles de routage
- Familiarité avec le contenu expliqué dans la formation Securing Internet Edge avec Cisco Secure Firewall Threat Defense

Ces compétences peuvent être trouvées dans les offres de formation Cisco suivantes :

- Mettre en œuvre et administrer les solutions Cisco
- SWIFT

## Public

- Installateurs de systèmes
- Intégrateurs de systèmes
- Administrateurs de systèmes
- Administrateurs de réseaux
- Concepteurs de solutions

## Programme de la formation

- 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 événements 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

## Organisation

### Formateur

Les formateurs de Docaposte Institute sont des experts de leur domaine, disposant d'une expérience terrain qu'ils enrichissent continuellement. Leurs connaissances techniques et pédagogiques sont rigoureusement validées en amont par nos référents internes. Riches de leur expérience sur le sujet, ils sauront accompagner vos collaborateurs dans leur montée en compétences.

### Moyens pédagogiques et techniques

- Alternance d'apports théoriques et de mises en pratique contextualisées.
- Progression pédagogique structurée, de la compréhension à la mise en œuvre opérationnelle.

- Pédagogie immersive favorisant une mise en application immédiate des compétences.
- Formation interactive et participative s'appuyant sur des ateliers pratiques, études de cas et échanges collectifs (+ 60 % du temps de formation.)
- Séquences pédagogiques rythmées et évaluations formatives régulières pour renforcer l'ancrage des apprentissages.
- Supports de cours, ressources documentaires et références mis à disposition par le formateur

## **Dispositif de suivi de l'exécution et de l'évaluation des résultats de la formation**

### **En amont de la formation** *(évaluation en ligne dans l'extranet apprenant)*

- Recueil des besoins et des attentes des participants.
- Auto-positionnement permettant d'évaluer le niveau initial des apprenants.

### **Tout au long de la formation**

- Évaluations continues réalisées par le formateur à travers des questions orales, exercices, QCM, études de cas et mises en situation pratiques.

### **À l'issue de la formation** *(évaluations en ligne dans l'extranet apprenant)*

- Auto-positionnement afin de mesurer l'acquisition des compétences visées.
- Validation de l'acquisition des compétences par le formateur
- Questionnaire de satisfaction « à chaud » à l'issue de la formation
- Questionnaire de satisfaction "à froid", 45 jours après la formation afin d'évaluer l'ancrage des acquis et leur mise en application en situation professionnelle.

## **Accessibilité**

Nos formations peuvent être adaptées à certaines conditions de handicap. Nous contacter pour toute information et demande spécifique.