Développez vos talents
Certifiez vos compétences

Cisco - Offre officielle certifiante

# Securing Networks with Cisco Firepower Next-Generation Firewall

5 jours (35h00) | ★★★★½ 4,6/5 | SSNGFW | Certification 300-710 (non incluse) | Évaluation qualitative de fin de stage | Formation délivrée en présentiel ou distanciel [1]

Formations Informatique › Réseaux et Télécoms › Cisco - Offre officielle certifiante

## À l'issue de ce stage vous serez capable de :

- Implémenter Cisco Firepower Next-Generation Firewall (NGFW) pour fournir une protection avancée contre les menaces avant, pendant et après les attaques
- Acquérir des compétences de pointe pour des responsabilités très exigeantes axées sur la sécurité
- Décrire les concepts-clés des technologies Next-Generation Intrusion Prevention System (NGIPS), NGFW et du système de défense contre les menaces Cisco Firepower, et identifier les scénarios de déploiement
- Effectuer les tâches initiales de configuration et d'installation des dispositifs de défense contre les menaces de Cisco Firepower
- Gérer le trafic et mettre en oeuvre la qualité de service (QoS) en utilisant Cisco Firepower Threat Defense
- Mettre en oeuvre la NAT en utilisant Cisco Firepower Threat Defense (FTD)
- Effectuer une découverte initiale du réseau, en utilisant Cisco Firepower pour identifier les hôtes, les applications et les services
- Décrire le comportement, l'utilisation et la procédure de mise en oeuvre des politiques de contrôle d'accès
- Connaître les concepts et les procédures de mise en oeuvre des caractéristiques du renseignement de sécurité.

## Niveau requis

Avoir des connaissances de base sur les concepts de pare-feu et d'IPS et comprendre les techniques de mise en réseau TCP/IP et d'architecture réseau. De plus, il est recommandé d'avoir suivi les cours CCNA "Cisco Solutions - Implementing and administering" et SCOR "Cisco Security Core Technologies - Implementing and operating", ou avoir les connaissances équivalentes. Afin d'obtenir la certification CCNP Security, il faut avoir passé l'examen Core 350-701 et l'examen 300-710.

**(1) Modalité et moyens pédagogique :**

Formation délivrée en présentiel ou distanciel * (e-learning, classe virtuelle, présentiel à distance). Le formateur alterne entre méthodes ** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation). La validation des acquis peut se faire via des études de cas, des quiz et/ou une certification.

Les moyens pédagogiques mis en oeuvre (variables suivant les formations) sont : ordinateurs Mac ou PC (sauf pour les 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.

* Nous consulter pour la faisabilité en distanciel. ** Ratio variable selon le cours suivi.

## Public concerné

Administrateurs de la sécurité, conseillers en sécurité, administrateurs réseau, ingénieurs système, personnel de soutien technique, partenaires de distribution et revendeurs et/ou professionnels techniques souhaitant savoir déployer et gérer un Cisco Firepower NGIPS et NGFW dans leur environnement réseau.

## 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

### Aperçu de Cisco Firepower Threat Defense (FTD)

- Examen de la technologie des pare-feux et IPS
- Caractéristiques et composants de Firepower Threat Defense
- Examen des plateformes de Firepower
- Cas d'utilisation de la mise en oeuvre de Cisco Firepower

### Configuration du dispositif Cisco Firepower NGFW

- Enregistrement des dispositifs à Firepower Threat Defense
- FXOS et Firepower Device Manager
- Configuration initiale de l'appareil
- Gestion des dispositifs de NGFW
- Examen
  - Des politiques du centre de gestion de Firepower
  - Des objets
  - De la configuration du système et de la surveillance de la santé
- Gestion des appareils
- Examen de la haute disponibilité de Firepower
- Configuration de la haute disponibilité
- Migration de Cisco ASA
  - Vers Firepower
  - Vers Firepower Threat Defense

### Contrôle du trafic de Cisco Firepower NGFW

- Traitement des paquets de Firepower Threat Defense
- Mise en oeuvre de la QoS
- Contournement de la circulation

### Traduction d'adresses Cisco Firepower NGFW

- Principes de base du NAT
- Implémentation de NAT
- Exemples de règles NAT

### Découverte de Cisco Firepower

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

### Mise en oeuvre des politiques de contrôle d'accès

- Examen des politiques de contrôle d'accès
- Examen des règles de la politique de contrôle d'accès et des mesures par défaut
- Mise en oeuvre d'une inspection plus poussée
- Examen des événements de connexion
- Politique de contrôle d'accès des paramètres avancés
- Considérations relatives à la politique de contrôle d'accès
- Mise en oeuvre d'une politique de contrôle d'accès

### Security Intelligence

- Examen de Security Intelligence
- Examen des objets de Security Intelligence
- Déploiement, enregistrement et mise en oeuvre de Security Intelligence

### Contrôle des fichiers et protection avancée contre les logiciels malveillants

- Examens
  - Des logiciels malveillants et de la politique des fichiers
  - De la protection avancée contre les logiciels malveillants

## Systèmes Next-Generation de prévention des intrusions

- Examens
  - De la prévention des intrusions
  - et des règles de Snort
  - Des variables et des ensembles de variables
  - Des politiques d'intrusion

### VPN de site à site

- Examen d'IPSec
- Configuration VPN de site à site
- Dépannage VPN de site à site
- Mise en place d'un VPN de site à site

### VPN d'accès à distance

- Examen du VPN d'accès à distance
- Examen de la cryptographie à clé publique et des certificats
- Inscription au certificat d'examen
- Configuration du VPN d'accès à distance
- Mise en oeuvre d'un VPN d'accès à distance

### Décryptage SSL

- Examen du décryptage SSL
- Configuration des politiques SSL
- Bonnes pratiques et surveillance du décryptage SSL

### Techniques d'analyse détaillée

- Examens
  - De l'analyse des événements
  - Des types d'événements
  - Des données contextuelles
  - Des outils d'analyse
- Analyse de la menace

### Administration du système

- Gestion des mises à jour
- Examen des caractéristiques de la gestion
- des comptes utilisateurs
- Configuration des comptes utilisateurs
- Administration du système

### Dépannage de Cisco Firepower

- Examen des erreurs de configuration courantes
- Gestion des commandes de dépannage
- Dépannage de Firepower

### 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

## Modalités d'évaluation des acquis

L'évaluation des acquis se fait :

- En cours de formation, par des études de cas ou des travaux pratiques
- Et, en fin de formation, par un questionnaire d'auto-évaluation ou une certification (M2i ou éditeur)

## Les + de la formation

Le support de cours et les labs sont en anglais.