

SECURING NETWORKS WITH CISCO FIREPOWER NEXT-GENERATION IPS

Cette formation vous apprend comment déployer et utiliser le Cisco Firepower® Next-Generation Intrusion Prevention System (NGIPS).

PRÉREQUIS:

Pour bénéficier pleinement de ce cours, vous devez disposer de:

- Très bonnes connaissances de la pile TCP/IP ainsi que des protocoles de routage de base.
- Familiarité avec les concepts relatifs aux systèmes de prévention/détection des intrusions (IPS/IDS).

Le suivi des cours CCNA et SFNDU est fortement recommandé.

PUBLIC:

Cette formation s'adresse aux:

- Administrateurs sécurité.
- Administrateurs réseau.
- Intégrateurs et partenaires Cisco
- Consultants en sécurité.
- Personnel de support technique
- Ingénieurs système.

OBJECTIFS:

Après avoir suivi ce cours, vous devriez pouvoir:

- Décrire les composants du Cisco Firepower Threat Defense et le processus d'enregistrement des périphériques gérés
- Détailler le contrôle de trafic sur le pare-feu nouvelle génération (NGFW) et configurer le système Cisco Firepower pour la découverte du réseau.
- Mettre en œuvre des politiques de contrôle d'accès et décrire les fonctionnalités avancées de la policy de contrôle d'accès
- Configurer les fonctionnalités « Security Intelligence » et la procédure de mise en œuvre de la protection avancée contre les logiciels malveillants (AMP) pour les réseaux pour le contrôle des fichiers et la protection avancée contre les logiciels malveillants
- Mettre en œuvre et gérer des règles d'intrusion et d'analyse de réseau pour l'inspection NGIPS
- Décrire et démontrer les techniques d'analyse détaillées et les fonctionnalités de génération de rapports fournies par Cisco Firepower Management Center (FMC)
- Intégrez Cisco Firepower Management Center à une destination de journalisation externe
- Décrire et démontrer les options d'alerte externes disponibles pour Cisco Firepower Management Center et configurer une stratégie de corrélation
- Décrire les principales fonctionnalités de mise à jour logicielle et de gestion des comptes utilisateurs de Cisco Firepower Management Center
- Identifiez les paramètres souvent mal configurés dans Cisco Firepower Management Center et utilisez les commandes

CURSUS:
CISCO

CODE DE LA FORMATION:
CS-SC-SSFIPS

**ÉDITEUR OU
CONSTRUCTEUR:**
CISCO

VERSION:
4.0

DURÉE:
5 JOURS

de base pour dépanner un périphérique Cisco Firepower Threat Defense

CONTENU:

- Présentation du Cisco Firepower Threat Defense (FTD)
- Configuration du Cisco Firepower NGFW.
- Contrôle du trafic sur le Cisco Firepower NGFW
- Cisco Firepower Discovery
- Implémentation des politiques de contrôle d'accès
- Security Intelligence
- Contrôle des fichiers et protection avancée contre les logiciels malveillants (AMP)
- Systèmes de prévention des intrusions de nouvelle génération
- Politiques d'analyse de réseau
- Techniques d'analyse détaillées
- Intégration de la plate-forme Cisco Firepower
- Règles d'alerte et de corrélation
- L'administration du système
- Dépannage de Cisco Firepower

CERTIFICATION:

Cette formation prépare à l'examen Cisco 300-710 SNCF