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

Description

La formation Fundamentals of Cisco Firewall Threat Defense and Intrusion Prevention (SFWIPF) vous offre une maîtrise approfondie des techniques de protection contre les menaces modernes grâce à Cisco Secure Firewall. Ce cours vous accompagne dans la configuration et le déploiement de ce pare-feu de nouvelle génération, essentiel pour sécuriser les réseaux d'entreprise.

Ce programme est conçu pour fournir des compétences concrètes, permettant de configurer efficacement les politiques de sécurité, la gestion des paquets, et de réaliser des analyses de menaces en temps réel. Vous apprendrez également à mettre en œuvre des fonctionnalités avancées comme la haute disponibilité, la traduction d'adresses réseau (NAT), et la défense contre les intrusions.

Contenu du cours
Module 1 : Présentation de Cisco Secure Firewall Threat Defense

- Comprendre les fonctions principales de Cisco Secure Firewall Threat Defense
- Identifier les composants clés de la solution
- Décrire les options de déploiement de Cisco Secure Firewall Threat Defense

Module 2 : Configuration des paramètres réseau de base

- Configurer les interfaces réseau sur Cisco Secure Firewall Threat Defense
- Mettre en œuvre la traduction d'adresses réseau (NAT)
- Configurer la haute disponibilité (HA)

Module 3 : Gestion des politiques de sécurité

- Configurer les politiques de contrôle d'accès (ACL)
- Configurer les politiques de préfiltre et de tunnel VPN
- Gérer les règles de sécurité avec Cisco Secure Firewall Threat Defense

Module 4 : Sécurisation avancée avec Cisco Secure Firewall

- Configurer l'intelligence sécuritaire (Security Intelligence)

© Copyright ITTA – Tous les contenus sont protégés par le droit d'auteur.

- Configurer les politiques d'intrusion avec Cisco IPS
- Gérer les événements et les menaces avec Cisco Secure Firewall Management Center

Module 5 : Analyse des menaces et gestion avancée

- Exécuter des analyses de base sur les menaces réseau
- Mettre en œuvre des rapports de sécurité et d'événements
- Diagnostiquer et dépanner les problèmes de flux de trafic

Module 6 : Gestion du système et dépannage

- Gérer Cisco Secure Firewall Threat Defense avec Cisco Firewall Device Manager
- Assurer la maintenance du système avec les outils Cisco
- Dépanner les incidents réseau et de sécurité

Lab / Exercices

- 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

Documentation

- Support de cours numérique inclus

Examen

- Ce cours prépare à la certification CCNP Security. Pour l'obtenir il faudra passer et réussir deux examens : l'examen de base 350-701 Implementing and Operating Cisco Security Core Technologies (SCOR) et un examen de concentration 300-710 Securing Networks with Cisco Firepower (SNCF). Si vous souhaitez passer ces examens, merci de contacter notre secrétariat qui vous communiquera son prix et s’occupera de toutes les démarches administratives nécessaires pour vous.

Profils des participants

- Ingénieurs en sécurité réseau
- Administrateurs réseau
- Architectes réseau
- Consultants en sécurité informatique

Connaissances Préalables

- Maîtrise des concepts TCP/IP
- Compréhension des protocoles de routage de base
- Notions de pare-feu et de VPN

© Copyright ITTA – Tous les contenus sont protégés par le droit d’auteur.

- Connaissances des systèmes de prévention d'intrusion (IPS)

Objectifs

- Déployer Cisco Secure Firewall Threat Defense
- Configurer la haute disponibilité
- Mettre en œuvre la traduction d'adresses (NAT)
- Configurer les politiques de sécurité et de découverte
- Gérer Cisco Secure Firewall Management Center
- Diagnostiquer et résoudre les problèmes réseau

Description
Formation Fundamentals of Cisco Firewall Threat Defense and Intrusion Prevention (SFWIPF)
Niveau
Intermédiaire
Prix de l'inscription en Présentiel (CHF)
4350
Prix de l'inscription en Virtuel (CHF)
4350
Durée (Nombre de Jours)
5
Reference
SFWIPF

© Copyright ITTA – Tous les contenus sont protégés par le droit d’auteur.