Fundamentals of Cisco Firewall Threat Defense and Intrusion Prevention

Durée: 5 Jours **Réf de cours: SFWIPF** **Version: 1.0**

Résumé:

Cette formation permet aux participants d'acquérir les compétences et connaissances nécessaires pour mettre en œuvre et configurer Cisco Secure Firewall Threat Defense pour un déploiement en tant que pare-feu de nouvelle génération à la périphérie de l'internet. Les participants comprendront l'architecture et le déploiement de Cisco Secure Firewall, la configuration de base, le traitement des paquets et les options avancées, ainsi que le dépannage de l'administration de Cisco Secure Firewall.
Cette formation vous prépare à la certification CCNP Security, qui requiert la réussite de l'examen de base 350-701 Implementing and Operating Cisco Security Core Technologies (SCOR) et d'un examen tel que l'examen de concentration 300-710 Securing Networks with Cisco Firepower (SNCF).
Cette formation vaut 40 crédits de formation continue (CE) pour la recertification.
Mise à jour : 25.09.2023

Public visé:

Cette formation s'adresse aux Ingénieurs en sécurité des réseaux et aux Administrateurs

Objectifs pédagogiques:

- A l'issue de la formation, les participants seront capables de :
- Décrire la défense contre les menaces de Cisco Secure Firewall
- Décrire les options de déploiement de Cisco Secure Firewall Threat Defense
- Décrire les options de gestion de Cisco Secure Firewall Threat Defense
- Configurer les paramètres initiaux de base de Cisco Secure Firewall Threat Defense
- Configurer la haute disponibilité sur Cisco Secure Firewall Threat Defense
- Configurer la traduction d'adresses réseau de base sur Cisco Secure Firewall Threat Defense
- Décrire les politiques de Cisco Secure Firewall Threat Defense et expliquer comment les différentes politiques influencent le traitement des paquets par l'appareil.
- Configurer la politique de découverte sur Cisco Secure Firewall Threat Defense
- Configurer et expliquer les règles de préfiltre et de tunnel dans la politique de préfiltre
- Configurer une politique de contrôle d'accès sur Cisco Secure Firewall Threat Defense

Pré-requis:

Les participants doivent remplir les conditions préalables suivantes :

- TCP/IP
- Protocoles de routage de base
- Concepts de pare-feu, de VPN et d'IPS
- CCNA - Mettre en oeuvre et administrer des solutions réseaux Cisco
- SCOR - Mettre en oeuvre et gérer les solutions de sécurité Cisco

Test et certification

Recommandé comme préparation à l'examen suivant :

- 300-710 - Securing Networks with Cisco Firewall (Sécurisation des réseaux avec les pare-feu Cisco)

Les sujets de l'examen sont actuellement répartis sur deux cours SSNGFW et SSFIPS, qui sont remplacés par SFWIPF et SFWIPA.

Contenu:

Présentation de Cisco Secure Firewall Threat Defense

Description des options de déploiement de Cisco Secure Firewall Threat Defense

Description des options de gestion de Cisco Secure Firewall Threat Defense

Configuration des paramètres réseau de base sur Cisco Secure Firewall Threat Defense

Configuration de la haute disponibilité sur Cisco Secure Firewall Threat Defense

Configuration de la NAT automatique sur Cisco Secure Firewall Threat Defense

Description du traitement des paquets et des politiques sur Cisco Secure Firewall Threat Defense

Configuration de la politique de découverte sur Cisco Secure Firewall Threat Defense

Configuration de la politique de préfiltrage sur Cisco Secure Firewall Threat Defense

Configuration de la politique de contrôle d'accès sur Cisco Secure Firewall Threat Defense

Configuration de la Security Intelligence sur Cisco Secure Firewall Threat Defense

Configuration de la politique de fichiers sur Cisco Secure Firewall Threat Defense

Configuration de la politique d'intrusion sur Cisco Secure Firewall Threat Defense

Exécution d'une analyse de base des menaces sur le centre de gestion de Cisco Secure Firewall

Gestion du système de défense contre les menaces de Cisco Secure Firewall

Dépannage du flux de trafic de base

Gestionnaire de périphériques Cisco Secure Firewall Threat Defense

Travaux pratiques :

- Lab1 : Effectuer la configuration initiale du dispositif
- Lab2 : Configurer la haute disponibilité
- Lab3 : Configurer la traduction d'adresses réseau
- Lab4 : Configuration de la découverte du réseau
- Lab5 : Configuration du préfiltre et de la politique de contrôle d'accès
- Lab6 : Configurer l'intelligence de sécurité
- Lab7 : Mise en œuvre du contrôle des fichiers et de la protection avancée contre les logiciels malveillants
- Lab 8 : Configurer Cisco Secure IPS
- Lab 9 : Analyse détaillée à l'aide du Centre de gestion des pare-feux
- Lab 10 : Gérer le système de défense contre les menaces de Cisco Secure Firewall
- Lab 11 : Principes de base du dépannage des pare-feux sécurisés
- Lab 12 : Configurer les périphériques gérés à l'aide de Cisco Secure Firewall Device Manager

Méthodes pédagogiques :

Support de cours officiel remis aux participants.
Les participants réalisent un test d'évaluation des connaissances en amont et en aval de la formation pour valider les connaissances acquises pendant la formation.

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :