Advanced Techniques for Cisco Firewall Threat Defense and Intrusion Prevention

Durée: 5 Jours Réf de cours: SFWIPA Version: 1.0 Méthodes d'apprentissage: Classe à distance

Résumé:

Cette formation permet aux participants d'acquérir les compétences et connaissances nécessaires sur la défense contre les menaces et la prévention des intrusions de Cisco Firewall, pour déployer et configurer un système de défense contre les menaces Cisco Secure Firewall et ses fonctions en tant que pare-feu de réseau de Data Center ou en tant que pare-feu de périphérie Internet avec prise en charge de réseaux privés virtuels (VPN). Ils apprendront à configurer les politiques basées sur l'identité, le décryptage SSL (Secure Sockets Layer), le VPN d'accès à distance et le VPN de site à site avant de passer à la configuration avancée du système de prévention des intrusions (IPS) et à la gestion des événements, aux intégrations avec d'autres systèmes et au dépannage avancé. Ils apprendront également à automatiser la configuration et les opérations du système Cisco Secure Firewall Threat Defense en utilisant la programmabilité et les interfaces de programmation d'applications (API) et à migrer la configuration des appliances de sécurité adaptatives (ASA) Cisco Secure Firewall.
Cette formation prépare à l'examen 300-710 Securing Networks with Cisco Firepower (SNCF). En cas de réussite, vous obtenez la certification Cisco Certified Specialist - Network Security Firepower et répondez aux exigences de l'examen de concentration pour la certification Cisco Certified Networking Professional (CCNP) Security.
Cette formation aidera les participants à :
Acquérir une connaissance avancée de la technologie Cisco Secure Firewall Threat Defense
Acquérir les compétences et les aptitudes nécessaires pour mettre en œuvre et gérer un système de défense contre les menaces Cisco Secure Firewall, quelle que soit la plate-forme.
Obtenir des informations détaillées sur la gestion des politiques, le flux de trafic à travers le système et l'architecture du système
Déployer et gérer de nombreuses fonctions avancées disponibles dans le système Cisco Secure Firewall Threat Defense
Acquérir des connaissances sur les protocoles, les solutions et les conceptions pour acquérir des rôles de centre de données de niveau professionnel et expert.
Cette formation vaut 40 crédits de formation continue (CE) pour la recertification.
Mise à jour ; 18.10.2024

Public visé:

Toute personne impliquée dans le déploiement et la maintenance d'une solution de défense contre les menaces Cisco Secure Firewall.

Objectifs pédagogiques:

- A l'issue de la formation, les participants seront capables 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

Pré-requis:

Les participants doivent remplir les conditions préalables suivantes :

- Connaissance du protocole de contrôle de transmission/protocole Internet (TCP/IP)

Test et certification

Recommandé comme préparation à l'examen suivant :

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

Les connaissances acquises dans les cours SFWIPF et SWIPA sont

- Connaissance de base des protocoles de routage
- Familiarité avec le contenu expliqué dans le cours Fundamentals of Cisco Firewall Threat Defense and Intrusion Prevention (Principes de base de la défense contre les menaces et de la prévention des intrusions).
- SFWIPF - Fundamentals of Cisco Firewall Threat Defense and Intrusion Prevention

requises pour cet examen.

Contenu:

Présentation de Cisco Secure Firewall Threat Defense

- Fonctionnalité du pare-feu
- Plate-forme Cisco Secure Firewall
- Cas d'utilisation
- Options de déploiement
- Options de gestion
- Paramètres de base du réseau
- Traitement des paquets
- Vue d'ensemble des politiques ACP et de préfiltrage
- Licence intelligente de Cisco Secure Firewall

Description des options de déploiement avancées de Cisco Secure Firewall Threat Defense

- Architecture de la défense contre les menaces de Cisco Secure Firewall
- FXOS et Secure Firewall Chassis Manager
- Déploiement multi-instances
- Déploiement en grappe
- Configuration du cluster

Configuration des paramètres avancés des périphériques sur Cisco Secure Firewall Threat Defense

- Mise en œuvre de la QoS
- Mise en œuvre des politiques de service
- Mise en œuvre des politiques FlexConfig
- Contournement du trafic

Configuration du routage dynamique sur Cisco Secure Firewall Threat Defense

- Présentation du routage dynamique
- Routage virtuel
- Configuration du routage dynamique

Configuration de la NAT avancée sur Cisco Secure Firewall Threat Defense

- Présentation de la traduction d'adresses réseau
- Mise en œuvre de règles NT avancées

Configuration de la politique SSL sur Cisco Secure Firewall Threat Defense

- Présentation du cryptage SSL
- Vue d'ensemble du décryptage SSL
- Configuration de la politique SSL
- Meilleures pratiques de la politique SSL

Déploiement d'un VPN d'accès à distance sur Cisco Secure Firewall Threat Defense

- Composants du VPN d'accès à distance
- Inscription au certificat numérique
- Configuration du VPN d'accès à distance
- Haute disponibilité du VPN d'accès à distance

Déploiement de politiques basées sur l'identité sur Cisco Secure Firewall Threat Defense

- Politiques basées sur l'identité
- Configuration du domaine
- Configuration de la source d'identité
- Configuration des politiques basées sur l'identité

Déploiement d'un VPN site à site sur Cisco Secure Firewall Threat Defense

- Composants du VPN site à site
- VPN site à site basé sur une politique et sur une route
- Configuration VPN point à point VTIs
- Configuration VPN Hub-and-Spoke avec Crypto Maps
- Haute disponibilité site à site

Configuration des règles Snort et des politiques d'analyse de réseau

- Règles Snort et politiques d'analyse du réseau
- Règles et actions Snort
- Recommandations pour les pare-feux sécurisés

Description de la gestion avancée des événements Défense contre les menaces de Cisco Secure Firewall

- Alertes
- Politiques de corrélation
- Enregistrement d'événements externes

Description des intégrations de Cisco Secure Firewall Threat Defense

- Intégration avec Cisco Identity Service Engine
- Intégration avec Cisco Network Analytics
- Intégration avec SecureX

Dépannage du flux de trafic avancé sur Cisco Secure Firewall Threat Defense

- Aperçu du flux de trafic
- Outils de dépannage
- Processus de dépannage
- Dépannage des performances

Automatisation de la défense contre les menaces de Cisco Secure Firewall

- Automatisation des opérations réseau
- Présentation de l'API du centre de gestion du pare-feu sécurisé de Cisco
- Présentation de l'API du Cisco Secure Firewall Device Manager

Migration vers Cisco Secure Firewall Threat Defense

- Options de migration
- Outil de migration
- Migration depuis Cisco Secure firewall ASA

Labs

- Configurer le pare-feu multi-instance à l'aide du gestionnaire de châssis Activité interactive
- Déployer les paramètres de connexion avancés
- Configurer le routage dynamique
- Configurer la politique SSL
- Configurer l'accès à distance VPN
- Configurer la politique basée sur l'identité
- Configurer le VPN site à site
- Personnaliser les politiques IPS et NAP
- Configurer les intégrations de défense contre les menaces de Cisco Secure Firewall
- Dépannage de Cisco Secure Firewall Threat Defense
- Automatisation de la défense contre les menaces de Cisco Secure Firewall
- Migration de la configuration de Cisco Secure Firewall ASA

Méthodes pédagogiques :

Support de cours officiel remis aux participants

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 :

• Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
• Votre place sera confirmée à la réception d'un devis ou """"booking form""""" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
• Attention, si cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés avant le début de la session pour vous inscrire via moncompteformation.gouv.fr.

Accueil des bénéficiaires :

• En cas de handicap : plus d'info sur globalknowledge.fr/handicap
• Le Règlement intérieur est disponible sur globalknowledge.fr/reglement