Securing Data Center Networks and VPNs with Cisco Firewall Threat Defence

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

Résumé:

La formation **Securing Data Center Networks and VPNs avec Cisco Secure Firewall Threat Defense** vous apprend comment déployer le système Cisco Secure Firewall Threat Defense et ses fonctionnalités en tant que pare-feu de data center ou en tant que pare-feu de périphérie d'Internet avec support VPN.
Vous apprendrez 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.
Vous apprendrez 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 vous 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 vous permet également d'obtenir 40 crédits de formation continue (CE) en vue d'une recertification.

Mise à jour : 27.0.2024

Public visé:

Intégrateurs de systèmes Administrateurs systèmes Administrateurs réseaux Architectes de solutions

Objectifs pédagogiques:

- À l'issue de la formation, les participants seront capables de :
- 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 de niveau expert
- Cette formation vous permet d'obtenir 40 crédits CE pour la recertification

Pré-requis:

Les participants doivent remplir les conditions préalables suivantes :

- Connaissance du protocole de contrôle de transmission/protocole Internet (TCP/IP)
- Connaissance de base des protocoles de routage
- Avoir les connaissances équivalentes de la formation Securing Internet Edge with Cisco Secure Firewall Threat Defense
- Ces compétences peuvent être trouvées dans les cours Cisco suivants :
- Implementing and Administering Cisco Solutions v2.0
- Securing Internet Edge with Cisco Secure Firewall Threat Defense 1.0
- SFWIPF - Fundamentals of Cisco Firewall Threat Defense and Intrusion Prevention

Test et certification

Recommandé comme préparation à la certification suivant :

300-710 - Securing Networks with Cisco Firewall (Sécuriser les 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.

Spécialiste certifié Cisco - Sécurité des réseaux Firepower

Contenu:

- Présentation de Cisco Secure Firewall Threat Defense
- Description des options de déploiement avancées sur Cisco Secure Firewall Threat Defense
- Configuration des paramètres avancés des appareils sur Cisco Secure Firewall Threat Defense
- Configuration du routage dynamique sur Cisco Secure Firewall Threat Defense
- Configuration de la NAT avancée sur Cisco Secure Firewall Threat Defense
- Configuration de la politique SSL sur Cisco Secure Firewall Threat Defense
- Déploiement de l'accès à distance VPN sur Cisco Secure Firewall Threat Defense
- Déploiement des politiques basées sur l'identité sur Cisco Secure Firewall Threat Defense
- Déploiement d'un VPN site à site sur Cisco Secure Firewall Threat Defense
- Configuration des règles Snort et des politiques d'analyse du réseau
- Description de la gestion avancée des événements sur Cisco Secure Firewall Threat Defense
- Description des intégrations de Cisco Secure Firewall Threat Defense
- Dépannage des flux de trafic avancés sur Cisco Secure Firewall Threat Defense
- Automatisation de Cisco Secure Firewall Threat Defense
- Migration vers Cisco Secure Firewall Threat Defense

Méthodes pédagogiques :

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.

Un support de cours officiel sera remis aux stagiaires.

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