Formation Sécuriser les réseaux avec les firewalls de dernière génération Cisco Firepower (SSNGFW)

N° ACTIVITÉ : 11 92 18558 92 | TÉLÉPHONE : 01 85 77 07 07 | E-MAIL : inscription@hubformation.com

Référence	CS131
Durée	5 jours (35h)
Tarif	4 290 €HT

Objectifs

| Décrire les concepts clés des technologies NGIPS et NGFW et du système de défense contre les menaces Cisco Firepower, et identifier les scénarios de déploiement
| Effectuer les tâches initiales de configuration et d'installation des dispositifs de défense contre les menaces de Cisco Firepower
| Décrire comment gérer le trafic et mettre en oeuvre la qualité de service (QoS) en utilisant Cisco Firepower Threat Defense
| Décrire comment mettre en oeuvre la NAT en utilisant Cisco Firepower Threat Defense
| Effectuer une découverte initiale du réseau, en utilisant Cisco Firepower pour identifier les hôtes, les applications et les services
| Décrire le comportement, l'utilisation et la procédure de mise en oeuvre des politiques de contrôle d'accès
| Décrire les concepts et les procédures de mise en oeuvre des caractéristiques du renseignement de sécurité
| Se préparer à l'examen Securing Networks with Cisco Firepower (300-710 SNCF)

PROCHAINES SESSIONS

Pour connaître les prochaines dates ou organiser un intra-entreprise, contactez-nous, nous vous répondrons sous 72 heures.

Public

| Administrateurs de la sécurité
| Conseillers en sécurité
| Administrateurs réseau
| Ingénieurs système
| Personnel de soutien technique
| Partenaires de distribution et revendeurs

Prérequis

| Compréhension technique de la mise en réseau TCP/IP et de l'architecture réseau
| Connaissance de base des concepts de pare-feu et d'IPS

Programme de la formation

Aperçu de Cisco Firepower Threat Defense
| Examen de la technologie des pares-feux et IPS
| Caractéristiques et composants de Firepower Threat Defense
| Examen des plates-formes de Firepower
| Cas d'utilisation de la mise en oeuvre de Cisco Firepower

Configuration du dispositif Cisco Firepower NGFW
| Enregistrement des dispositifs à Firepower Threat Defense
| FXOS et Firepower Device Manager
| Configuration initiale de l'appareil
| Gestion des dispositifs de NGFW
| Examen des politiques du Centre de gestion de Firepower
| Examen des objets
| Examen de la configuration du système et de la surveillance de la santé

| Gestion des appareils
| Examen de la haute disponibilité de Firepower
| Configuration de la haute disponibilité
| Migration de Cisco ASA vers Firepower
| Migration de Cisco ASA vers Firepower Threat Defense

Contrôle du trafic de Cisco Firepower NGFW
| Traitement des paquets de Firepower Threat Defense
| Mise en oeuvre de la QoS
| Contournement de la circulation

Traduction d'adresses Cisco Firepower NGFW
| Principes de base du NAT
| Implémentation de NAT
| Exemples de règles NAT
| Implémentation de NAT

Découverte de Cisco Firepower (Cisco Firepower Discovery
| Examen de la découverte du réseau
| Configuration de la découverte du réseau
| Mise en oeuvre des politiques de contrôle d'accès
| Examen des politiques de contrôle d'accès
| Examen des règles de la politique de contrôle d'accès et des mesures par défaut
| Mise en oeuvre d'une inspection plus poussée
| Examen des événements de connexion
| Politique de contrôle d'accès Paramètres avancés
| Considérations relatives à la politique de contrôle d'accès
| Mise en oeuvre d'une politique de contrôle d'accès

Security Intelligence
| Examen de Security Intelligence
| Examen des objets de Security Intelligence
| Déploiement et enregistrement de Security Intelligence
| Mise en oeuvre de Security Intelligence

Contrôle des fichiers et protection avancée contre les logiciels malveillants
| Examen des logiciels malveillants et de la politique des fichiers
| Examen de la protection avancée contre les logiciels malveillants

Systèmes Next-Generation de prévention des intrusions
| Examen de la prévention des intrusions et des règles de Snort
| Examen des variables et des ensembles de variables
| Examen des politiques d'intrusion

VPN de site à site
| Examen d'IPsec
| Configuration VPN de site à site
| Dépannage VPN de site à site
| Mise en place d'un VPN de site à site

VPN d'accès à distance
| Examen du VPN d'accès à distance
| Examen de la cryptographie à clé publique et des certificats
| Inscription au certificat d'examen
| Configuration du VPN d'accès à distance
| Mise en oeuvre d'un VPN d'accès à distance

Décryptage SSL
| Examen du décryptage SSL
| Configuration des politiques SSL
| Best Practices et surveillance du décryptage SSL

Techniques d'analyse détaillée
| Examen de l'analyse des événements
| Examen des types d'événements
| Examen des données contextuelles

HUB Formation - 1-7, Cours Valmy - 92923 Paris - La Defense
01 85 77 07 07 - www.hubformation.com - SIREN 525 287 785

| Examen des outils d'analyse
| Analyse de la menace

Administration du système
| Gestion des mises à jour
| Examen des caractéristiques de la gestion des comptes utilisateurs
| Configuration des comptes d'utilisateur
| Administration du système

Dépannage de Cisco Firepower
| Examen des erreurs de configuration courantes
| Examen des commandes de dépannage
| Dépannage de Firepower

Méthode pédagogique

Chaque participant travaille sur un poste informatique qui lui est dédié. Un support de cours lui est remis soit en début soit en fin de cours. La théorie est complétée par des cas pratiques ou exercices corrigés et discutés avec le formateur. Le formateur projette une présentation pour animer la formation et reste disponible pour répondre à toutes les questions.

Méthode d'évaluation

Tout au long de la formation, les exercices et mises en situation permettent de valider et contrôler les acquis du stagiaire. En fin de formation, le stagiaire complète un QCM d'auto-évaluation.

Accessibilité

Les sessions de formation se déroulent sur des sites différents selon les villes ou les dates, merci de nous contacter pour vérifier l'accessibilité aux personnes à mobilité réduite.
Pour tout besoin spécifique (vue, audition...), veuillez nous contacter au 01 85 77 07 07.