Sécuriser les réseaux avec Cisco Firepower Next Generation Firewall

Formation Informatique / Réseaux et Sécurité / Cisco

Le cours Sécuriser les réseaux avec Cisco Firepower Next Generation Firewall (SSNGFW) v1.0 vous montre comment déployer et utiliser le système de défense contre les menaces Cisco Firepower®. Ce cours pratique vous donne les connaissances et les compétences nécessaires pour utiliser et configurer la technologie Cisco® Firepower Threat Defense, en commençant par l'installation et la configuration initiales des dispositifs et en incluant le routage, la haute disponibilité, la migration de l'ASA (Adaptive Security Appliance) vers Cisco Firepower Threat Defense, le contrôle du trafic et la translation d'adresses réseau (NAT). Vous apprendrez comment mettre en œuvre les fonctionnalités avancées du pare-feu de nouvelle génération (NGFW) et du système de prévention des intrusions de nouvelle génération (NGIPS), notamment l'intelligence réseau, la détection des types de fichiers, la détection des logiciels malveillants sur le réseau et l'inspection approfondie des paquets. Vous apprendrez également comment configurer le VPN de site à site, le VPN d'accès à distance et le décryptage SSL avant de passer à l'analyse détaillée, à l'administration du système et au dépannage.
Ce cours vous aide à vous préparer à l'examen, Sécuriser les réseaux avec la puissance de feu Cisco (300-710 SNCF), qui mène aux certifications CCNP Security et Cisco Certified Specialist - Network Security Firepower. L'examen 300-710 SNCF comporte également un deuxième cours de préparation, Sécuriser les réseaux avec Cisco Firepower Next-Generation IPS (SSFIPS). Vous pouvez suivre ces cours dans n'importe quel ordre.
Le suivi de cette formation permet de valider un total de 40 crédits dans le cadre du programme d'Education Continue Cisco (CCE) pour les professionnels qui souhaitent renouveler leur titre de certification.

OBJECTIFS

- Décrire les concepts clés des technologies NGIPS et NGFW et du système de défense contre les menaces de la puissance de feu Cisco et identifier les scénarios de déploiement
- Effectuer les tâches initiales de configuration et d'installation des dispositifs Firepower Threat Defense
- Décrire comment gérer le trafic et mettre en œuvre la qualité de service (QoS) en utilisant Cisco FirepowerFirepower Threat Defense
- Décrire comment mettre en œuvre la NAT en utilisant Cisco FirepowerFirepower Threat Defense
- Effectuer une première découverte du réseau, en utilisant Cisco FirepowerFirepower Threat Defense pour identifier les hôtes, les applications et les services
- Décrire le comportement, l'utilisation et la procédure de mise en œuvre des politiques de contrôle d'accès
- Décrire les concepts et les procédures de mise en œuvre des dispositifs de renseignement de sécurité
- Décrire l'AMP Cisco pour les réseaux et les procédures de mise en œuvre du contrôle des fichiers et de la protection avancée contre les logiciels malveillants
- Mettre en œuvre et gérer les politiques d'intrusion
- Décrire les composantes et la configuration du VPN de site à site
- Décrire et configurer un VPN SSL d'accès à distance qui utilise Cisco AnyConnect
- Décrire les capacités de décryptage et l'utilisation du SSL

PUBLIC

Ce cours est conçu pour les professionnels qui doivent savoir comment déployer et gérer un Cisco Firepower NGIPS et NGFW dans leur environnement réseau.

PRE-REQUIS

- Connaissance de TCP/IP et des protocoles de routage de base. Le suivi du cours CCNA est recommandé
- Etre à l'aise avec les concepts de pare-feu, de VPN et d'IPS - Le suivi des cours IINS or SFNDU est recommandé

PROGRAMME

Présenation de Cisco Firepower Threat Defense

- Découverte de la technologie des pare-feu et IPS
- Caractéristiques et composants de Firepower Threat Defense
- Etude des plates-formes de Firepower
- Cas d'utilisation de la mise en œuvre 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
- Présentation des politiques du Centre de gestion de Firepower
- Présentation des objets
- Présentation de la configuration du système et de la surveillance de la santé
- Gestion des appareils
- Présentation 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

A retenir

Durée : **5 jours** soit 35h.
Réf. **SSNGFW**

01 42 93 52 72

Dates des sessions

Paris
11/12/2023
12/02/2024
10/06/2024
14/10/2024
DISTANCE
09/10/2023

Cette formation est également proposée en formule INTRA-ENTREPRISE.

Inclus dans cette formation

Coaching Après-COURS

Pendant 30 jours, votre formateur sera disponible pour vous aider. CERTyou s'engage dans la réalisation de vos objectifs.

100% SATISFACTION GARANTIE

Votre garantie 100% SATISFACTION

Notre engagement 100% satisfaction

Sécuriser les réseaux avec Cisco Firepower Next Generation Firewall

Formation Informatique / Réseaux et Sécurité / Cisco

vous garantit la plus grande qualité de formation.

Contrôle du trafic de Cisco Firepower NGFW

- Traitement des paquets de Firepower Threat Defense
- Mise en œuvre de la QoS

Translation d'adresses Cisco Firepower NGFW

- Principes de base du NAT
- Implémentation de NAT
- Exemples de règles NAT
- Implémentation de NAT

Découverte de Cisco Firepower

- Présentation de la découverte du réseau
- Configuration de la découverte du réseau
- Mise en œuvre des politiques de contrôle d'accès
- Présentation des politiques de contrôle d'accès
- Présentation des règles de la politique de contrôle d'accès et des mesures par défaut
- Mise en œuvre d'une inspection plus poussée
- Présentation des événements de connexion
- Politique de contrôle d'accès Paramètres avancés
- Considérations relatives à la politique de contrôle d'accès
- Mise en œuvre d'une politique de contrôle d'accès

Security Intelligence

- Présentation de Security Intelligence
- Présentation des objets de Security Intelligence
- Déploiement et enregistrement de Security Intelligence
- Mise en œuvre de Security Intelligence

Contrôle des fichiers et protection avancée contre les logiciels malveillants

- Présentation des logiciels malveillants et de la politique des fichiers
- Présentation de la protection avancée contre les logiciels malveillants

Systèmes Next-Generation de prévention des intrusions

- Présentation de la prévention des intrusions et des règles de Snort
- Présentation des variables et des ensembles de variables
- Présentation des politiques d'intrusion

VPN site à site

- Présentation 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

- Présentation du VPN d'accès à distance
- Présentation de la cryptographie à clé publique et des certificats
- Inscription au certificat d'examen
- Configuration du VPN d'accès à distance
- Mise en œuvre d'un VPN d'accès à distance

Décryptage SSL

- Présentation du décryptage SSL
- Configuration des politiques SSL
- Best Practices et surveillance du décryptage SSL

Techniques d'analyse détaillée

- Présentation de l'analyse des événements
- Présentation des types d'événements
- Présentation des données contextuelles
- Présentation 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

Horaires, Planning et Déroulement de cette formation

Horaires

• Formation de 9h00 (9h30 le premier jour) à 17h30.
• Deux pauses de 15 minutes le matin et l'après-midi.
• 1 heure de pause déjeuner

DEROULEMENT

• Les horaires de fin de journée sont adaptés en fonction des horaires des trains ou des avions des différents participants.
• Une attestation de suivi de formation vous sera remise en fin de formation.
• Cette formation est organisée pour un maximum de 14 participants.

PROCHAINES FORMATIONS

Réussir la Certification Gestion de Projet PMP du PMI
Réussir la Certification PRINCE2 Foundation
Réussir les Certifications PRINCE2 Foundation et PRINCE2 Practitioner
Réussir la Certification ITIL Foundation
Réussir la Certification Agile certifié SCRUM Master
Réussir les Certifications TOGAF Certified et TOGAF Foundation

CERTyou est certifié Qualiopi

CERTyou a été reconnu par le BUREAU VERITAS pour la qualité de ces procédures et lui a décerné la certification Qualiopi Formation Professionnelle. La certification de services Qualiopi Formation Professionnelle répond aux exigences qualité décrites dans l'article 1 du décret n°2015-790 du 30 juin 2015.

Qualiopi processus certifié

RÉPUBLIQUE FRANÇAISE

La certification qualité a été délivrée au titre de la catégorie d'actions suivantes : **ACTIONS DE FORMATION**

Retrouvez cette formation sur notre site :
Sécuriser les réseaux avec Cisco Firepower Next Generation Firewall