# Formation Sécuriser les réseaux avec Cisco Firepower Next Generation Firewall

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

Cette formation permet aux participants d'acquérir les compétences et connaissances nécessaires pour déployer et utiliser le système de défense contre les menaces Cisco Firepower®. Les participants apprendront comment 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). Ils apprendront également comment mettre en oeuvre 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.
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.

| | |
|---|---|
| Référence | SSNGFW |
| Durée | 5 jours (35h) |
| Tarif | 4 290 €HT |
| Repas | 100 €HT(en option) |

## SESSIONS PROGRAMMÉES

### A DISTANCE (ENG)

- du 24 au 28 juin 2024
- du 29 juil. au 2 août 2024
- du 19 au 23 août 2024
- du 30 sept. au 4 octobre 2024
- du 28 oct. au 1er novembre 2024
- du 25 au 29 novembre 2024
- du 16 au 20 décembre 2024

VOIR TOUTES LES DATES

## 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 oeuvre la qualité de service (QoS) en utilisant Cisco FirepowerFirepower Threat Defense
| Décrire comment mettre en oeuvre 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 oeuvre des politiques de contrôle d'accès
| Décrire les concepts et les procédures de mise en oeuvre des dispositifs de renseignement de sécurité
| Décrire l'AMP Cisco pour les réseaux et les procédures de mise en oeuvre du contrôle des fichiers et de la protection avancée contre les logiciels malveillants
| Mettre en oeuvre et gérer les politiques d'intrusion
| Décrire les composantes et la configuration du VPN de site à sit, configurer un VPN SSL d'accès à distance qui utilise Cisco AnyConnect et les capacités de décryptage et l'utilisation du SSL

## Public

| professionnels qui doivent savoir comment déployer et gérer un Cisco Firepower NGIPS et NGFW dans leur environnement réseau.



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

## Prérequis

| Connaissance de TCP/IP et des protocoles de routage de base
| Etre à l'aise avec les concepts de pare-feu, de VPN et d'IPS Formations recommandées :

## Programme de la formation

**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 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
| 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

**Contrôle du trafic de Cisco Firepower NGFW**
| Traitement des paquets de Firepower Threat Defense
| Mise en oeuvre 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 oeuvre 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 oeuvre 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 oeuvre 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 oeuvre 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 oeuvre 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

## 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.

---

## Suivre cette formation à distance

Voici les prérequis techniques pour pouvoir suivre le cours à distance :

| Un ordinateur avec webcam, micro, haut-parleur et un navigateur (de préférence Chrome ou Firefox). Un casque n'est pas nécessaire suivant l'environnement.
| Une connexion Internet de type ADSL ou supérieure. Attention, une connexion Internet ne permettant pas, par exemple, de recevoir la télévision par Internet, ne sera pas suffisante, cela engendrera des déconnexions intempestives du stagiaire et dérangera toute la classe.
| Privilégier une connexion filaire plutôt que le Wifi.
| Avoir accès au poste depuis lequel vous suivrez le cours à distance au moins 2 jours avant la formation pour effectuer les tests de connexion préalables.
| Votre numéro de téléphone portable (pour l'envoi du mot de passe d'accès aux supports de cours et pour une messagerie


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

instantanée autre que celle intégrée à la classe virtuelle).
| Selon la formation, une configuration spécifique de votre machine peut être attendue, merci de nous contacter.
| Pour les formations incluant le passage d'une certification la dernière journée, un voucher vous est fourni pour passer l'examen en ligne.
| Pour les formations logiciel (Adobe, Microsoft Office...), il est nécessaire d'avoir le logiciel installé sur votre machine, nous ne fournissons pas de licence ou de version test.
| Horaires identiques au présentiel.

## 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.