DAWAN

Plan de la formation

www.dawan.fr

Formation Cisco Secure Firewall - Déploiement, administration et dépannage avec FMC

Durée :	5 jours (35 heures)
Tarif inter-entreprises :	3 775,00 € HT (Présentiel) 3 020,00 € HT (Distanciel)
Public :	Administrateurs et ingénieurs réseaux et sécurité - Intégrateurs de pare-feu Cisco Secure Firewall - Techniciens confirmés chargés de l'exploitation et du diagnostic des flux
Pré-requis :	Maîtriser l'adressage IP, le routage, les VLAN et les ACL au niveau CCNA - Comprendre le filtrage avec état, le NAT et les principes des VPN IPsec - Savoir diagnostiquer une connectivité réseau et lire une capture de paquets - Posséder une première expérience d'administration de pare-feu
Objectifs :	Déployer un pare-feu Cisco Secure Firewall Threat Defense administré par FMC - Configurer le routage, le NAT et les politiques de contrôle d'accès - Mettre en œuvre les protections IPS et analyser leurs événements - Configurer un VPN IPsec et vérifier un accès distant préparé - Mettre en place une paire de pare-feu à haute disponibilité - Diagnostiquer un flux bloqué et assurer les opérations courantes d'exploitation
Modalités pédagogiques, techniques et d'encadrement :	• Formation synchrone en présentiel et distanciel. • Méthodologie basée sur l'Active Learning : 75 % de pratique minimum. • Un PC par participant en présentiel, possibilité de mettre à disposition en bureau à distance un PC et l'environnement adéquat. • Un formateur expert.

Modalité d'évaluation :	• Définition des besoins et attentes des apprenants en amont de la formation. • Auto-positionnement à l'entrée et la sortie de la formation. • Suivi continu par les formateurs durant les ateliers pratiques. • Évaluation à chaud de l'adéquation au besoin professionnel des apprenants le dernier jour de formation.
Sanction :	Attestation de fin de formation mentionnant le résultat des acquis
Référence :	RéS103123-F
Note de satisfaction des participants :	Pas de données disponibles
Contacts :	commercial@dawan.fr - 09 72 37 73 73
Modalités d'accès :	Possibilité de faire un devis en ligne (www.dawan.fr, moncompteformation.gouv.fr, maformation.fr, etc.) ou en appelant au standard.
Délais d'accès :	Variable selon le type de financement.
Accessibilité :	Si vous êtes en situation de handicap, nous sommes en mesure de vous accueillir, n'hésitez pas à nous contacter à referenthandicap@dawan.fr, nous étudierons ensemble vos besoins

Préparer l’architecture Secure Firewall

Rôles de Threat Defense, Firewall Management Center et Device Manager
Modes de déploiement et choix d’une architecture routée
Interfaces d’administration, licences et compatibilité des versions
Enregistrement des équipements et cycle de déploiement des configurations

Atelier pratique : enregistrer un pare-feu dans FMC et vérifier la connectivité d’administration

Configurer les réseaux et la traduction d’adresses

Interfaces, zones de sécurité, sous-interfaces et objets réseau
Routes statiques et vérification des chemins aller et retour
NAT statique, PAT et priorités des règles de traduction
Publication d’un service et exceptions de NAT pour les VPN

Atelier pratique : donner accès à Internet à un réseau interne et publier un serveur de démonstration

Construire les politiques de contrôle d’accès

Traitement des paquets et articulation des différentes politiques
Règles de préfiltrage, contrôle d’accès et action par défaut
Filtrage par zones, réseaux, applications et catégories d’URL
Journalisation, ordre des règles et validation des changements

Atelier pratique : appliquer une matrice de flux entre réseau interne, DMZ et réseau externe

Activer et ajuster les protections

Security Intelligence, contrôle des fichiers et détection des menaces
Politiques IPS, moteur Snort et traitement des alertes
Choix des protections selon les services exposés et les risques
Principes du déchiffrement TLS, exceptions et limites de visibilité

Atelier pratique : activer une protection IPS, observer une alerte et justifier un ajustement de politique

Sécuriser les interconnexions VPN

VPN site à site : IKEv2, IPsec et paramètres de sécurité
Routage, exemptions NAT et filtrage du trafic chiffré
Principes de l’accès distant avec Cisco Secure Client
Authentification, certificats et contrôle des accès VPN

Atelier pratique : établir un tunnel IPsec et valider un profil d’accès distant préconfiguré

Mettre en œuvre la haute disponibilité

Prérequis et fonctionnement d’une paire active/passive Threat Defense
Interfaces de bascule, synchronisation et surveillance
Effets d’une bascule sur les sessions et les services
Procédure de vérification avant et après maintenance

Atelier pratique : configurer une paire, provoquer une panne et contrôler la reprise du trafic

Organiser l’exploitation et la maintenance

Health Monitor, événements de connexion et tableaux de bord
Comptes administratifs, rôles et export des journaux
Sauvegardes, restauration et préparation des mises à jour
Suivi des licences, des signatures et des changements de politique

Atelier pratique : produire un rapport d’exploitation et préparer une intervention avec retour arrière

Diagnostiquer les incidents de trafic

Méthode de recherche à partir d’une adresse, d’un port et d’un horaire
Captures, packet-tracer et analyse des décisions de traitement
Incidents de routage, NAT, contrôle d’accès, IPS et VPN
Validation du rétablissement et documentation de la cause

Atelier pratique : résoudre un incident combinant traduction d’adresses, règle de sécurité et tunnel VPN