Formation Cisco - Firewall ASA - Mise en oeuvre

Code : NET-CISCO-300 Durée : 3 jours (21 heures)

Public visé

Ingénieurs, techniciens et administrateurs réseaux et télécoms.

{{< formation-prerequis >}}

Objectifs pédagogiques

À l'issue de cette formation, vous serez capable de :

- Reconnaître et analyser les fonctionnalités du firewall Cisco ASA (équipement vital de protection des réseaux)
- Installer et configurer des firewalls Cisco ASA (pour mettre en place des architectures sécurisées)

Programme

Jour 1

Introduction aux Cisco ASA (Adaptative Security Appliance)

- Présentation des ASA et de leurs spécificités
- Cisco Security Appliance Device Manager (ASDM)
- Gestion des licences

Connexion et gestion de base

- Le processus de démarrage (boot)
- Gestion via l'interface CLI
- Gestion via l'interface GUI ASDM - Naviguer dans l'interface
- Gérer les mises à jour
- Configurer les :
- Niveaux de sécurité, les paramètres de connectivité de base
- Interfaces VLAN, la route par défaut et le serveur DHCP intégré

Exemple de travaux pratiques (à titre indicatif)

- Prise en main de l'environnement de lab

Jour 2

Intégration au réseau

- Translation d'adresses sur l'appliance
- Configurer les objets de :
- NAT (auto)
- NAT (manuel)
- Source NAT
- Destination NAT
- La table de connexions
- Configurer et vérifier les :
- ACL
- Groupes d'objets
- Serveurs publics
- Configurer le routage sur l'appliance
- Routage statique
- Dynamique
- EIGRP

Exemples de travaux pratiques (à titre indicatif)

- Administration et intégration dans le réseau
- Mise en oeuvre de NAT et des ACL

Les règles de filtrage

- Vue d'ensemble de MPF (Modular Policy Framework)
- Configurer des règles de couches 3 et 4
- Vue d'ensemble pour les couches 5 à 7
- Configurer l'inspection
- HTTP
- FTP
- Des autres applications

Exemple de travaux pratiques (à titre indicatif)

- Mise en oeuvre de l'inspection des applications

Jour 3

Les composants ASA pour réaliser un VPN

- Définition de VPN, types et composants
- Notions de profils (tunnel groups), politiques de groupes et d'utilisateurs
- Configurer la relation entre ASA et autorité de certification, obtention d'un certificat

Exemple de travaux pratiques (à titre indicatif)

- Configuration d'une autorité de certification puis installation de certificats sur l'ASA

VPN mode sans client

- Introduction à la solution sans client VPN SSL, cas d'usage et méthodes d'accès aux ressources

- SSL et TLS, établissement de la session, gestion des clés et authentification du serveur et du client
- Personnalisation du portail d'accès, signets
- Déploiement sur l'appliance

Exemple de travaux pratiques (à titre indicatif)

- Configuration VPN poste à site via WebVPN

Jour 4

VPN AnyConnect, le tunnel complet

- Les fondements, l'authentification, l'affectation d'adresses, la notion de partage de tunnel (Split tunneling)
- Configurer un pool d'adresses IP, identity NAT, les politiques de groupes et les profils de connexion
- Surveiller le VPN côté client et côté serveur
- Scénarios d'authentification externe, mise à profit de LDAP / AD
- Tunnel IPsec, IKEv1 et IKEv2
- Support d'IKEv2 par AnyConnect
- Configurer un tunnel IPsec avec AnyConnect

Exemple de travaux pratiques (à titre indicatif)

- Configuration d'un tunnel poste à site via VPN SSL, via VPN IPsec

Haute disponibilité et virtualisation

- Configurer EtherChannel, la redondance d'interfaces
- Configurer la haute disponibilité en mode actif / passif
- La notion de contexte, le mode contexte multiple et configurer des contextes de sécurité

Exemple de travaux pratiques (à titre indicatif)

- Mise en oeuvre de la haute disponibilité en mode actif / passif

Modalités d'évaluation des acquis

En cours de formation, par des études de cas ou des travaux pratiques. En fin de formation, par un questionnaire d'auto-évaluation.

{{< formation-require >}}

{{< formation-seealso >}}