

Cisco Firewall ASA, configuration et administration

Cours Pratique de 4 jours - 28h

Réf : CPF - Prix 2024 : 2 690CHF HT

Apprenez à déployer et à maintenir une solution de sécurité basée sur Cisco ASA. Vous verrez comment configurer les fonctions essentielles à l'aide d'une interface Web avec ASDM (Cisco Adaptive Security Device Manager) et en ligne de commande CLI, configurer les translations d'adresses dynamiques et statiques et les premières opérations de maintenance.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

Connaître les fonctionnalités du firewall Cisco ASA

Configurer un firewall ASA

Configurer les fonctions essentielles à l'aide de l'ASDM et du CLI

Configurer la stratégie d'accès basée sur les ACLs (Listes de contrôle d'accès)

Analyser et restreindre le flux (entrant et sortant)

Configurer un VPN pour les accès distants

Optimiser les règles de sécurité

LE PROGRAMME

dernière mise à jour : 05/2023

1) Introduction

- Les technologies et caractéristiques des firewalls.
- Présentation des firewalls. Terminologie et fonctionnalités.
- Exemples d'architecture. La gamme ASA.
- Le démarrage avec un ASA. L'interface utilisateur. Configuration du firewall.
- Paramétrage de NTP. Les niveaux de sécurité ASA.
- Configuration de Syslog.

Travaux pratiques : Configuration basique d'un ASA.

2) Traduction d'adresses et connexions

- NAT dynamique, PAT et NAT statique.
- La fonction TCP Intercept.
- Connexions, redirection de ports.
- Configuration DMZ.

Travaux pratiques : Configuration d'un ASA en PAT avec deux et trois interfaces. Publication d'un serveur Web.

3) ACL et Content Filtering

- Présentation des ACL.
- Configuration des ACL.
- Filtrage de code actif malicieux.
- Filtrage d'URL.
- Les groupes d'objets.

PARTICIPANTS

Responsables sécurité. Ingénieurs systèmes et réseaux. Architectes sécurité. Techniciens réseaux ou sécurité.

PRÉREQUIS

Bonnes connaissances en administration réseaux avec équipements Cisco et en sécurité informatique.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques...
Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

- Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
- À l'issue de chaque stage ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
- Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le stagiaire a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

- Présentation des groupes d'objets. Les usages.

- La configuration des groupes d'objets.

Travaux pratiques : Filtrage de trafic réseau HTTP et FTP. Création et utilisation de groupes d'objets dans les ACL.

4) Configuration AAA

- Présentation de Cisco Secure ACS.

- Installation de Cisco Secure ACS.

- Configurer l'authentification et l'autorisation.

- Téléchargement des ACL.

- Dépannage AAA.

Travaux pratiques : Installation de CSACS. Configuration d'ASA en AAA.

5) Routage et commutation

- Rappels sur les VLAN.

- Fonctionnalités supportées.

- Routage statique et dynamique.

- Le Multicast.

Travaux pratiques : Configuration d'ASA en multi-VLAN, de RIPv2 et d'OSPF.

6) VPN

- Mise en place des VPN.

- Configuration d'IPSec.

- Le client VPN Cisco.

- Configuration de l'accès distant avec Easy VPN.

- Configuration du serveur Easy VPN.

- Caractéristiques d'Easy VPN distant.

- Présentation et configuration du client.

- Présentation et configuration du WebVPN.

Travaux pratiques : Mise en place d'un VPN site-à-site, d'un accès distant VPN et du WebVPN.

7) Transparent firewall

- Transparent versus Routed firewall.

- Fonctionnalités non supportées.

- Configuration des adresses IP, des ACL et d'ARP.

- Maintenance et dépannage.

Travaux pratiques : Mise en place d'un firewall transparent.

8) Failover

- Présentation des modes de Failover. Configuration de Failover et de Lan Failover. Mise en place du Failover.

- Configuration de Failover.

- Configuration de Lan Failover.

- Mise en place du Failover en mode Active/Active.

Travaux pratiques : Mise en place d'un failover en mode Active/Standby, ainsi qu'en mode Active/Active.

9) Cisco Security Appliance Device Manager

- Utilisation de ASDM pour la configuration de ASA.

- Création de VPN site à site et d'accès distant VPN.

Travaux pratiques : Installation d'ASDM. Configuration de VPN.

10) Maintenance

- Configuration de l'accès.

- Niveaux de privilèges.

- Password Recovery.

- Gestion de l'IOS.
- Gestion de la configuration.
- Gestion des licences.

Travaux pratiques : Mise à jour de l'IOS. Sauvegarde de la configuration. Password Recovery.

LES DATES

CLASSE À DISTANCE

2024 : 03 déc.