SÉCURISER LE WEB AVEC CISCO WEB SECURITY APPLIANCE

CODE DE LA FORMATION:
CS-SC-SWSA

ÉDITEUR OU CONSTRUCTEUR:
CISCO

VERSION:
2.1

DURÉE:
2 JOURS

Cette formation permet d'acquérir les competences et connaissances nécessaires pour installer, configurer, gérer et dépanner la solution de sécurité Cisco Web Security Appliance (WSA) dans des entreprises de moyenne envergure.

PRÉREQUIS:

- Posséder de bonnes connaissances des services TCP/IP, tels que DNS, SSH, FTP, SNMP, http et HTTPS
- Le suivi du cours ICND2 est recommandé
- Avoir de bonnes connaissances du routage IP, de HTTP, de l'administration et du fonctionnement du serveur et du navigateur Web

PUBLIC:

Cette formation s'adresse aux personnes chargées du déploiement et de l'installation de Cisco Web Appliance.

OBJECTIFS:

- Décrire Cisco WSA
- Installer et vérifier WSA
- Déployer les services proxy pour WSA
- Utiliser l'authentification avec WSA
- Configurer les différentes stratégies de WSA
- Faire respecter l'utilisation normale de l'accès internet via WSA
- Se défendre contre les malware
- Configurer la sécurité des données
- Décrire Cisco CWS (Cloud Web Security)
- Utiliser le client Cisco AnyConnect secure mobility
- Améliorer l'administration et le dépannage de WSA

CONTENU:

Rappels sur le système

- Etudes de cas clients
- Modèles Cisco Web Security Appliance et architecture

Installation et vérification de Cisco Web Security Appliance

- Rappels sur Cisco Security Management Appliance
- Installer et vérifier le matériel Cisco Web Security Appliance
- Installer et vérifier Cisco Web Security virtual appliance pour VMware
- Démarrer l'assistant installation

- Configurer L4TM

Configuration du connecteur Virtual Web Security Appliance vers Cisco CWS

- Rappels sur la Cisco CWS
- Se connecter à CWS via Cloud Web Security Connector

Déploiement des services Proxy

- Les différents modes Proxy
- Rappels sur les fichiers PAC
- Configurer et gérer les services Proxy
- Déployer le proxy FTP natif
- Lire les journaux d'accès Proxy et les entêtes http

Utiliser l'authentification

- Configurer NTLM et l'authentification Proxy
- Identifier les paramètres d'authentification et les « realms »
- Décrire l'authentification LDAP et l'autorisation
- Dépanner les domaines joints et tester l'authentification

Configuration des stratégies

- Configurer les stratégies d'accès et les identités
- Configurer les exceptions d'authentification
- Rappels sur les tags des journaux d'accès

Garantir un usage normal et sécuriser l'accès internet

- Filtrer l'accès en fonctions des catégories URL
- Configurer la reconnaissance et le contrôle des applications
- Décrire le contrôle d'accès SaaS
- Utiliser l'inspection HTTPS
- Configurer les paramètres proxy HTTPS

Garantir un usage normal et sécuriser l'accès internet – Sujets avancés

- Configurer la reconnaissance et le contrôle des applications – Sujets avancés
- Décrire le contrôle d'accès SaaS – Sujets avancés
- Configurer les contrôles d'utilisation du Web et les catégories URL
- Vue journalisation et reporting

Se défendre contre les Malware

- Décrire et configurer WBRS
- Décrire et configurer le scan anti-malware
- Décrire et configurer la protection avancée contre les malware
- Interpréter les balises ACL contre les malware

Configuration de la sécurité des données

- Configurer la sécurité des données
- Configurer le DLP (Data Loss Prevention)

- Décrire les journaux de sécurité d'accès et de données

Description CWS

- Fonctionnalités de CWS
- Expliquer les modèles de Cloud Cisco attachés
- Utilisation du client Cisco AnyConnect Secure Mobility
- Décrire Cisco AnyConnect Web security
- Intégrer le client Cisco AnyConnect Secure Mobility

Amélioration de l'administration et du dépannage

- Décrire l'administration des rapports
- Surveiller Cisco Web Security Appliance
- Configurer la journalisation W3C
- Améliorer les autres tâches administratives
- Décrire la redondance Hardware
- Dépanner Cisco Web Security Appliance

CERTIFICATION:

Cette formation Cisco prépare à l'examen *WSFE 700-281*.