Sécuriser le Web avec Cisco Web Security Appliance

Durée: 180 Jours **Réf de cours: SWSA** **Version: 3.1** **Méthodes d'apprentissage: E-learning**

Résumé:

Le cours "Sécuriser le Web avec Cisco Web Security Appliance (SWSA)" vous montre comment mettre en œuvre, utiliser et maintenir Cisco® Web Security Appliance (WSA), géré par Cisco Talos, pour fournir une protection avancée pour la messagerie d'entreprise et le contrôle contre les menaces de sécurité sur le Web.
Grâce à une combinaison de formation par des experts et de pratique, vous apprendrez à déployer des services proxy, à utiliser l'authentification, à mettre en œuvre des politiques pour contrôler le trafic et l'accès HTTPS, à mettre en œuvre des paramètres et des politiques de contrôle de l'utilisation, à utiliser les fonctions anti-malware de la solution, à mettre en œuvre la sécurité des données et la prévention des pertes de données, à effectuer l'administration de la solution Cisco WSA, et bien plus encore.

Ce cours vaut 16 crédits de formation continue (CE).
Mis à jour 27/02/2025

e-Learning

Interactive self-paced content that provides flexibility in terms of pace, place and time to suit individuals and organisations. These resources also consist of online books, educational podcasts and vodcasts, and video-based learning.

Public visé:

Ce cours s'adresse aux personnes concernées par le déploiement, l'installation et l'administration d'un dispositif de sécurité Web de Cisco.

Objectifs pédagogiques:

- A la fin de cette formation, les participants seront capables de.. :
- Décrire Cisco WSA
- Déployer des services proxy
- Utiliser l'authentification
- Décrire les politiques de décryptage pour contrôler le trafic HTTPS
- Comprendre les politiques d'accès au trafic différencié et les profils d'identification
- Appliquer les réglages de contrôle de l'utilisation autorisée
- Défendre contre les logiciels malveillants
- Décrire la sécurisation des données et la prévention des pertes de données
- Effectuer l'administration et le dépannage

Pré-requis:

Les participants doivent posséder les connaissances préalables suivantes :

- Services TCP/IP, y compris le système de noms de domaine (DNS), Secure Shell (SSH), FTP, Simple Network Management Protocol (SNMP), HTTP et HTTPS
- Routage IP
- CCNA - Mettre en oeuvre et administrer des solutions réseaux Cisco
- G013 - Formation CompTIA Security+

Test et certification

Cette formation prépare à l'examen :

300-725 - Securing the Web with Cisco Web Security Appliance

Après cette formation, nous vous conseillons le(s) module(s) suivant(s):

Les participants à la recherche d'une formation sur l'Email Security Appliance de Cisco devraient envisager :

- SESA - Securing your Email with Cisco Email Security Appliance

Contenu:

Présentation de Cisco WSA

- Cas d'utilisation
- Solution Cisco WSA
- Caractéristiques de Cisco WSA
- Architecture Cisco WSA
- Service Proxy
- Contrôle du trafic de couche 4 intégré
- Prévention de la perte de données
- Intelligence cognitive de Cisco
- Outils de gestion
- Cisco Advanced Web Security Reporting (AWSR) et intégration tierce
- Dispositif de gestion de la sécurité du contenu de Cisco (SMA)

Services Proxy

- Mode de transfert explicite vs. mode transparent
- Redirection du trafic en mode transparent
- Protocole de contrôle du cache Web
- Protocole de communication du cache Web
- WCCP Flux en amont et en aval
- Contournement de proxy
- Mise en cache du proxy
- Fichiers PAC (Proxy Auto-Config)
- Proxy FTP
- Proxy Socket Secure (SOCKS)
- Log d'accès au proxy et en-têtes HTTP
- Personnalisation des notifications d'erreur avec les pages de notification à l'utilisateur final (EUN)

Authentification Cisco WSA

- Protocoles d'authentification
- Domaines d'authentification
- Suivi des informations d'identification de l'utilisateur
- Mode proxy explicite (transfert) et transparent
- Contournement de l'authentification avec des agents problématiques
- Rapports et authentification
- Réauthentification
- Authentification par proxy FTP
- Dépannage de la jonction de domaines et de l'authentification de test
- Intégration avec Cisco Identity Services Engine (ISE)

Administration et dépannage

- Surveillance de l'appliance de sécurité Web de Cisco
- Rapports de l'appliance de sécurité Web de Cisco
- Surveillance de l'activité du système à l'aide des logs
- Tâches d'administration du système
- Dépannage
- Interface de ligne de commande

Politiques de décryptage

- Inspection de Transport Layer Security (TLS)/Secure Sockets Layer (SSL) - Vue d'ensemble
- Vue d'ensemble des certificats
- Aperçu des politiques de décryptage HTTPS
- Activation de la fonction proxy HTTPS
- Balises de liste de contrôle d'accès (ACL) pour l'inspection HTTPS
- Exemples de logs d'accès

Politiques d`accès différencié au trafic et profils d`identification

- Aperçu des politiques d'accès
- Groupes de politiques d'accès
- Aperçu des profils d'identification
- Profils d'identification et authentification
- Ordre de traitement des politiques d'accès et des profils d'identification
- Autres types de politiques
- Exemples de logs d'accès
- Balises de décision ACL et groupes de règles
- Application des politiques d'utilisation autorisée basées sur le temps et le volume de trafic, et notifications à l'utilisateur final

Défendre contre les logiciels malveillants

- Filtres de réputation Web
- Analyse anti-programmes malveillants
- Analyse du trafic sortant
- Anti-logiciels malveillants et vérification de la réputation dans les politiques
- Filtrage de la réputation des fichiers et analyse des fichiers
- Protection avancée contre les logiciels malveillants de Cisco
- Fonctionnalités d'analyse et de réputation des fichiers
- Intégration avec Cisco Cognitive Intelligence

Paramètres de contrôle de l'utilisation autorisée

- Contrôle de l'utilisation du web
- Filtrage des URL
- Solutions pour les catégories d'URL
- Moteur d'analyse dynamique du contenu
- Visibilité et contrôle des applications web
- Limitation de la bande passante des contenus multimédias
- Contrôle d'accès aux logiciels en tant que service (SaaS)
- Filtrage des contenus pour adultes

Sécurité des données et prévention des pertes de données

- Sécurité des données
- Solution de sécurité des données de Cisco
- Définitions de la politique de sécurité des données
- Logs de sécurité des données

Exercices pratiques:

- Exercice 1 : Configurer le dispositif de sécurité Web de Cisco
- Exercice 2 : Configuration de l'authentification par serveur mandataire (Proxy)
- Exercice 3 : Configurer les services de rapport et le suivi sur le Web
- Exercice 4 : Configurer le Cisco Secure Email et le Web Manager pour le suivi et la création de rapports
- Exercice 5 : Configurer l'inspection HTTPS
- Exercice 6 : Créer et appliquer une politique d'utilisation autorisée basée sur la date et l'heure
- Exercice 7 : Configurer la protection avancée contre les logiciels malveillants
- Exercice 8 : Configurer les Exceptions d'En-tête de Référence (Referrer Header Exceptions)
- Exercice 9 : Utiliser les flux de sécurité tiers et le flux externe de MS Office 365
- Exercice 10 : Valider un certificat intermédiaire

Méthodes pédagogiques :

Un support de cours officiel sera fourni aux participants.