SECURING THE WEB WITH CISCO WEB SECURITY APPLIANCE

Cette formation vous montre comment implémenter, utiliser et entretenir l'Appliance Cisco Web Security Applicance® (WSA), optimisé par Cisco Talos, pour fournir une protection avancée des emails professionnels et un contrôle contre les menaces de sécurité Web.

CURSUS:
CISCO

CODE DE LA FORMATION:
CS-SC-SWSA

ÉDITEUR OU CONSTRUCTEUR:
CISCO

VERSION:
3.0

DURÉE:
2 JOURS

PRÉREQUIS:

Les connaissances et compétences qu'un stagiaire doit posséder avant de suivre ce cours sont:

- Services TCP/IP, y compris les protocoles: DNS, SSH, FTP, SNMP, HTTP et HTTPS.
- Expérience avec le routage IP.

Pour bénéficier pleinement de ce cours, vous devez disposer de l'une/plusieurs des compétences suivantes:

- Certification Cisco (Cisco CCENT® ou supérieure).
- Certification pertinente telle que (ISC) 2, CompTIA Security +, EC-Council, Global Information Assurance Certification (GIAC) et ISACA.
- Lettre de suivis du cursus Cisco Networking Academy (CCNA® 1 et CCNA 2).
- Expertise Windows: Microsoft [spécialiste Microsoft, Microsoft Certified Solutions Associate (MCSA), Microsoft Certified Systems Engineer (MCSE)], CompTIA (A +, Network +, Server +).

PUBLIC:

Cette formation s'adresse aux:

- Ingénieurs Sécurité.
- Managers responsables de la sécurité web.
- Architecte Sécurité.
- Ingénieurs d'opération.
- Ingénieurs Réseau.
- Administrateurs Réseau.
- Techniciens Réseau ou Sécurité.
- Managers Réseau.
- Designers System.
- Intégrateurs et partenaires Cisco

OBJECTIFS:

Après avoir suivi ce cours, vous devriez pouvoir:

- Décrire le Cisco WSA
- Déployer des services proxy
- Utiliser l'authentification

- Décrire les policies de déchiffrement pour contrôler le trafic HTTPS
- Comprendre les politiques d'accès au trafic différenciées et les profils d'identification
- Appliquer des paramètres de contrôle d'utilisation acceptables
- Se défendre contre les logiciels malveillants
- Décrire la sécurité et la prévention des pertes de données (DLP)
- Effectuer l'administration et le dépannage

CONTENU:

Décrire Cisco WSA

- Cas d'utilisation de la technologie
- Solution Cisco WSA
- Caractéristiques du Cisco WSA
- Architecture du Cisco WSA
- Service proxy
- Moniteur de trafic de la couche 4
- Prévention contre la perte de données (DLP)
- Cisco Cognitive Intelligence
- Outils de gestion
- Cisco Advanced Web Security Reporting (AWSR) et intégration tierce
- Appliance Cisco Content Security Management (SMA)

Déploiement des services proxy

- Mode Forward Explicite vs mode transparent
- Redirection du trafic en mode transparent
- Protocole de contrôle du cache Web
- Web Cache Communication Protocol (WCCP) Upstream and Downstream Flow
- Contournement du proxy
- Mise en cache du proxy
- Fichiers de configuration automatique du proxy (PAC)
- Proxy FTP
- Socket Secure (SOCKS) Proxy
- Journal d'accès proxy et en-têtes http
- Personnalisation des notifications d'erreur avec les pages de notification de l'utilisateur final

Utilisation de l'authentification

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

Création de policy de déchiffrement pour contrôler le trafic HTTPS

- Présentation de l'inspection TLS (Transport Layer Security) / SSL (Secure Sockets Layer)
- Présentation des certificats
- Présentation des policies de décryptage HTTPS
- Activation de la fonction proxy HTTPS
- Tags des listes de contrôle d'accès (ACL) pour l'inspection HTTPS

- Exemples de journaux d'accès

Comprendre les policies d'accès au trafic différenciées et les profils d'identification

- Présentation des policies d'accès
- Groupes de policies d'accès
- Aperçu des profils d'identification
- Profils d'identification et authentification
- Ordonnance de traitement des policies d'accès et des profils d'identification
- Autres types de policies
- Exemples de journaux d'accès
- Tags de décision ACL et groupes de policies
- Application des policies d'utilisation acceptable en fonction du temps et du volume de trafic et des notifications aux utilisateurs finaux

Défense contre les logiciels malveillants

- Filtres de réputation de sites Web
- Analyse anti-malware
- Analyse du trafic sortant
- Anti-Malware et réputation dans les policies
- Filtrage de la réputation des fichiers et analyse des fichiers
- Cisco Advanced Malware Protection (AMP)
- Fonctions de réputation et d'analyse de fichiers
- Intégration avec Cisco Cognitive Intelligence

Application des paramètres de contrôle d'utilisation acceptable

- Contrôle de l'utilisation du Web
- Filtrage d'URL
- Solutions de catégorie d'URL
- Moteur d'analyse de contenu dynamique
- Visibilité et contrôle des applications Web
- Application des limites de bande passante multimédia
- Contrôle d'accès logiciel en tant que service (SaaS)
- Filtrage du contenu pour adultes

Sécurité des données et prévention des pertes de données (DLP)

- Sécurité des données
- Solution Cisco Data Security
- Définitions des policies de sécurité des données
- Journaux de sécurité des données

Administration et dépannage

- Surveillez la Cisco Web Security Appliance
- Rapports du Cisco WSA
- Surveillance de l'activité du système via des journaux
- Tâches d'administration système
- Dépannage
- Interface en ligne de commande (CLI)

Les références

- Comparaison des modèles Cisco WSA
- Comparaison des modèles Cisco SMA
- Présentation de la connexion, de l'installation et de la configuration
- Déploiement du modèle OVF du Cisco WSA
- Mappage des ports de machine virtuelle de la Cisco Web Securitu Appliance aux réseaux corrects
- Connexion à l'Appliance virtuelle Cisco WSA

- Activation du moniteur de trafic de couche 4 (L4TM)
- Accès et exécution de l'assistant de configuration du système
- Reconnexion à la Cisco WSA
- Présentation de la haute disponibilité
- Redondance matérielle
- Présentation du protocole CARP (Common Address Redundancy Protocol)
- Configuration des groupes de basculement pour la haute disponibilité
- Comparaison des fonctionnalités entre les options de redirection du trafic
- Scénarios d'architecture lors du déploiement de Cisco AnyConnect® Secure Mobility

CERTIFICATION:

Cette formation prépare à l'examen Cisco 300-725 SWSA.