Securing the Web with Cisco Web Security Appliance (SWSA)

Description

Le cours Sécurisation du Web avec l'appliance de sécurité Web Cisco (SWSA) v3.0 vous montre comment implémenter, utiliser et entretenir l'appliance de sécurité Web Cisco® (WSA), optimisé par Cisco Talos, pour fournir une protection avancée des e-mails professionnels et un contrôle contre menaces de sécurité Web. Grâce à une combinaison d'instructions d'experts et de travaux pratiques, 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, à utiliser les fonctionnalités anti-malware de la solution, à mettre en œuvre sécurité des données et prévention des pertes de données, effectuez l'administration de la solution Cisco WSA, etc.

Contenu du cours
Décrire Cisco WSA

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

Déploiement de services proxy

- Mode direct explicite vs mode transparent
- Redirection du trafic en mode transparent
- Protocole de contrôle du cache Web
- Flux amont et aval du protocole de communication Web Cache (WCCP)
- Contournement de proxy
- Mise en cache du proxy
- Fichiers de configuration automatique du proxy (PAC)
- Proxy FTP
- Proxy Socket Secure (SOCKS)
- Journal d'accès proxy et en-têtes HTTP
- Personnalisation des notifications d'erreur avec les pages de notification de l'utilisateur final (EUN)

Utilisation de l'authentification

- Protocoles d'authentification
- Domaines d'authentification
- Suivi des informations d'identification de l'utilisateur
- Mode proxy explicite (avant) et transparent
- Contournement de l'authentification avec des agents problématiques

- Rapports et authentification
- Nouvelle authentification
- Authentification proxy FTP
- Dépannage de la jonction de domaines et test de l'authentification
- Intégration avec Cisco Identity Services Engine (ISE)

Création de stratégies de déchiffrement pour contrôler le trafic HTTPS

- Présentation de l'inspection TLS (Transport Layer Security) / SSL (Secure Sockets Layer)
- Présentation du certificat
- Présentation 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 journaux d'accès

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

- Présentation des politiques d'accès
- Groupes de stratégies d'accès
- Aperçu des profils d'identification
- Profils d'identification et authentification
- Ordonnance de traitement des politiques d'accès et des profils d'identification
- Autres types de politiques
- Exemples de journaux d'accès
- Balises de décision ACL et groupes de stratégies
- Application des stratégies 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 politiques
- Filtrage de la réputation des fichiers et analyse des fichiers
- Cisco Advanced Malware Protection
- 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

- Sécurité des données

- Solution de sécurité des données Cisco
- Définitions des politiques de sécurité des données
- Journaux de sécurité des données

Administration et dépannage

- Surveillez l'appliance de sécurité Web Cisco
- Rapports Cisco WSA
- Surveillance de l'activité du système via des journaux
- Tâches d'administration système
- Dépannage
- Interface de ligne de commande

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 (Open Virtualization Format) de Cisco Web Security Appliance
- Mappage des ports de machine virtuelle (VM) de l'appliance de sécurité Web Cisco aux réseaux corrects
- Connexion à l'appliance virtuelle Cisco Web Security
- Activation du moniteur de trafic de couche 4 (L4TM)
- Accès et exécution de l'assistant de configuration du système
- Reconnexion à l'appliance de sécurité Web Cisco
- 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

Lab / Exercices

- Configurer l'appliance de sécurité Web Cisco
- Déployer des services proxy
- Configurer l'authentification proxy
- Configurer l'inspection HTTPS
- Créer et appliquer une politique d'utilisation acceptable basée sur l'heure / la date
- Configurer la protection avancée contre les logiciels malveillants
- Configurer les exceptions d'en-tête de référent
- Utiliser des flux de sécurité tiers et un flux externe MS Office 365
- Valider un certificat intermédiaire
- Afficher Reporting Services et le suivi Web
- Effectuer une mise à niveau centralisée du logiciel Cisco AsyncOS à l'aide de Cisco SMA

Documentation

- Support de cours numérique inclus

Examen

- Ce cours prépare à la certification 300-725 SWSA Securing the Web with Cisco Web Security Appliance. Si vous souhaitez passer cet examen, merci de contacter notre secrétariat qui vous communiquera son

prix et s’occupera de toutes les démarches administratives nécessaires pour vous.

Profils des participants

- Architectes de sécurité
- Concepteurs de systèmes
- Ingénieurs d'exploitation
- Gestionnaires de réseau
- Intégrateurs et partenaires Cisco

Connaissances Préalables

- Services TCP / IP
- Certification de l'industrie pertinente (ISC2), CompTIA Security +, EC-Council, Global Information Assurance Certification (GIAC), ISACA

Objectifs

- Décrire Cisco WSA
- Déployer des services proxy
- Utiliser l'authentification
- Décrire les politiques 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
- Se défendre contre les logiciels malveillants
- Décrire la sécurité et la prévention des pertes de données
- Effectuer l'administration et le dépannage

Niveau
Intermédiaire
Prix de l'inscription en Virtuel (CHF)
2200
Durée (Nombre de Jours)
2
Reference
CIS-SWSA