Security

Securing the Web with Cisco Web Security Appliance

SWSA

Version : 3.0
2 Jours

Objectifs

A l'issue de ce cours, le stagiaire sera en mesure d'atteindre ses 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 acceptables
- Se défendre contre les logiciels malveillants
- Décrire la sécurité et la prévention des pertes de données
- Effectuer l'administration et le dépannage

Public Concerné

- Architectes de sécurité
- Concepteurs de systèmes
- Administrateurs réseau
- Ingénieurs d'exploitation
- Gestionnaires de réseau, techniciens de réseau ou de sécurité, et ingénieurs et gestionnaires de sécurité responsables de la sécurité Web
- Intégrateurs et partenaires Cisco

Pré-requis

Avant de suivre ce cours, le stagiaire doit posséder les compétences techniques suivantes :

- Certification Cisco (certification CCENT ou supérieure)
- Certification de l'industrie pertinente [International Information System Security Certification Consortium ((ISC) 2), Computing Technology Industry Association (CompTIA) Security +, International Council of Electronic Commerce Consultants (EC-Council), Global Information Assurance Certification (GIAC), ISACA]
- Lettre d'achèvement de Cisco Networking Academy (CCNA 1 et CCNA 2)

Pour plus d'informations : info@learneo.com ou 01 53 20 37 00

- Expertise Windows: Microsoft [spécialiste Microsoft, Microsoft Certified Solutions Associate (MCSA), Microsoft Certified Solutions Expert (MCSE)], CompTIA (A +, Network +, Server +)

Le stagiaire doit posséder les compétences et les connaissances suivantes avant de suivre ce cours :

- Services TCP / IP, y compris DNS (Domain Name System), Secure Shell (SSH), FTP, SNMP (Simple Network Management Protocol), HTTP et HTTPS
- Routage IP

Plan du cours détaillé

1. Décrire Cisco WSA
   - 1.1. Cas d'utilisation de la technologie
   - 1.2. Solution Cisco WSA
   - 1.3. Caractéristiques de Cisco WSA
   - 1.4. Architecture de Cisco WSA
   - 1.5. Service proxy
   - 1.6. Moniteur de trafic de couche 4 intégré
   - 1.7. Prévention contre la perte de données
   - 1.8. Cisco Cognitive Intelligence
   - 1.9. Outils de gestion
   - 1.10. Cisco Advanced Web Security Reporting (AWSR) et intégration tierce
   - 1.11. Appliance de gestion de la sécurité du contenu Cisco (SMA)

2. Déploiement de services proxy
   - 2.1. Mode direct explicite vs mode transparent
   - 2.2. Redirection du trafic en mode transparent
   - 2.3. Protocole de contrôle du cache Web
   - 2.4. Flux amont et aval du protocole de communication Web Cache (WCCP)
   - 2.5. Contournement de proxy
   - 2.6. Mise en cache du proxy
   - 2.7. Fichiers de configuration automatique du proxy (PAC)
   - 2.8. Proxy FTP
   - 2.9. Proxy Socket Secure (SOCKS)
   - 2.10. Journal d'accès proxy et en-têtes HTTP
   - 2.11. Personnalisation des notifications d'erreur avec les pages de notification de l'utilisateur final (EUN)

3. Utilisation de l'authentification
   - 3.1. Protocoles d'authentification
   - 3.2. Domaines d'authentification
   - 3.3. Suivi des informations d'identification de l'utilisateur
   - 3.4. Mode proxy explicite (avant) et transparent

3.5. Contournement de l'authentification avec des agents problématiques
3.6. Rapports et authentification
3.7. Nouvelle authentification
3.8. Authentification proxy FTP
3.9. Dépannage de la jonction de domaines et test de l'authentification
3.10. Intégration avec Cisco Identity Services Engine (ISE)

4. Création de stratégies de déchiffrement pour contrôler le trafic HTTPS
   4.1. Présentation de l'inspection TLS (Transport Layer Security) / SSL (Secure Sockets Layer)
   4.2. Présentation du certificat
   4.3. Présentation des politiques de décryptage HTTPS
   4.4. Activation de la fonction proxy HTTPS
   4.5. Balises de liste de contrôle d'accès (ACL) pour l'inspection HTTPS
   4.6. Exemples de journaux d'accès

5. Comprendre les politiques d'accès au trafic différenciées et les profils d'identification
   5.1. Présentation des politiques d'accès
   5.2. Groupes de stratégies d'accès
   5.3. Aperçu des profils d'identification
   5.4. Profils d'identification et authentification
   5.5. Ordonnance de traitement des politiques d'accès et des profils d'identification
   5.6. Autres types de politiques
   5.7. Exemples de journaux d'accès
   5.8. Balises de décision ACL et groupes de stratégies
   5.9. Application des stratégies d'utilisation acceptable en fonction du temps et du volume de trafic et des notifications aux utilisateurs finaux

6. Défense contre les logiciels malveillants
   6.1. Filtres de réputation de sites Web
   6.2. Analyse anti-malware
   6.3. Analyse du trafic sortant
   6.4. Anti-Malware et réputation dans les politiques
   6.5. Filtrage de la réputation des fichiers et analyse des fichiers
   6.6. Cisco Advanced Malware Protection
   6.7. Fonctions de réputation et d'analyse de fichiers
   6.8. Intégration avec Cisco Cognitive Intelligence

7. Application des paramètres de contrôle d'utilisation acceptable
   7.1. Contrôle de l'utilisation du Web
   7.2. Filtrage d'URL
   7.3. Solutions de catégorie d'URL
   7.4. Moteur d'analyse de contenu dynamique
   7.5. Visibilité et contrôle des applications Web
   7.6. Application des limites de bande passante multimédia

7.7. Contrôle d'accès logiciel en tant que service (SaaS)
7.8. Filtrage du contenu pour adultes

8. Sécurité des données et prévention des pertes de données
   8.1. Sécurité des données
   8.2. Solution de sécurité des données Cisco
   8.3. Définitions des politiques de sécurité des données
   8.4. Journaux de sécurité des données

9. Administration et dépannage
   9.1. Surveillez l'appliance de sécurité Web Cisco
   9.2. Rapports Cisco WSA
   9.3. Surveillance de l'activité du système via des journaux
   9.4. Tâches d'administration système
   9.5. Dépannage
   9.6. Interface de ligne de commande

Laboratoire

- 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