Securing Email with Cisco Email Security Appliance (SESA)

Description

Cette formation vous enseigne comment déployer et utiliser Cisco® Email Security Appliance pour protéger vos systèmes de messagerie contre les menaces telles que le phishing, la compromission des e-mails professionnels et les ransomwares, tout en simplifiant la gestion des politiques de sécurité de la messagerie. Ce cours vous permettra de développer les compétences et les connaissances nécessaires pour déployer, dépanner et administrer Cisco Email Security Appliance, y compris des fonctionnalités telles que la protection avancée contre les logiciels malveillants, le blocage des spams, la protection antivirus, le cryptage, les quarantaines et la prévention des pertes de données.

Contenu du cours
Module 1 : Description du Cisco Email Security Appliance

- Présentation du Cisco Email Security Appliance
- Cas d'utilisation de la technologie
- Fiche technique du Cisco Email Security Appliance
- Aperçu du SMTP
- Vue d'ensemble de l'acheminement du courrier électronique
- Scénarios d'installation
- Configuration initiale du Cisco Email Security Appliance
- Centralisation des services sur un dispositif de gestion de la sécurité du contenu Cisco (SMA)
- Notes de mise à jour pour AsyncOS 11.x

Module 2 : Administration de Cisco Email Security Appliance

- Répartition des tâches administratives
- Administration du système
- Gestion et surveillance à l'aide de l'interface de ligne de commande (CLI)
- Autres tâches dans l'interface graphique
- Configuration avancée du réseau
- Utilisation de Email Security Monitor
- Suivi des messages
- Logging

Module 3 : Contrôle des domaines de l'expéditeur et du destinataire

- Auditeurs publics et privés
- Configuration du gateway pour la réception de courriers électroniques
- Aperçu du Host Access Table
- Aperçu du Recipient Access Table
- Configuration des fonctions de routage et de transmission

Module 4 : Contrôler le spam avec Talos SenderBase et Anti-Spam

- Aperçu de SenderBase
- Anti-Spam
- Gérer Graymail

- Protection contre les URL malveillants ou indésirables
- Filtrage de la réputation des fichiers et analyse des fichiers
- Vérification des rebonds (bounces)

Module 5 : Utilisation de filtres anti-virus et outbreaks

- Aperçu de l'analyse antivirus
- Filtrage anti-virus Sophos
- Filtrage anti-virus McAfee
- Configuration de l'appareil pour la recherche de virus
- Filtres d'outbreaks
- Fonctionnement du dispositif de filtrage des outbreaks
- Gestion des filtres d'outbreaks

Module 6 : Utilisation des politiques de courrier

- Aperçu du gestionnaire de sécurité du courrier électronique
- Aperçu des politiques en matière de courrier
- Traiter différemment les messages entrants et sortants
- Adaptation des utilisateurs à une politique du courrier
- Fractionnement des messages
- Configuration des politiques de courrier

Module 7 : Utilisation des filtres de contenu

- Aperçu des filtres de contenu
- Conditions de filtrage du contenu
- Actions de filtrage de contenu
- Filtrer les messages en fonction de leur contenu
- Aperçu des ressources textuelles
- Utiliser et tester les règles de filtrage des dictionnaires de contenu
- Comprendre les ressources textuelles
- Gestion des ressources textuelles
- Utilisation des ressources textuelles

Module 8 : Utilisation de filtres de messages pour faire appliquer les politiques en matière de courrier électronique

- Aperçu des filtres de messages
- Composantes d'un filtre de messages
- Traitement des filtres de messages
- Règles de filtrage des messages
- Actions de filtrage des messages
- Numérisation des pièces jointes
- Exemples de filtres de messages pour l'analyse des pièces jointes
- Utilisation de l'ICA (CLI) pour gérer les filtres de messages
- Exemples de filtres de messages
- Configuration du comportement de scan

Module 9 : Prévention de la perte de données

- Aperçu du processus d'analyse de la prévention des pertes de données (DLP)
- Mise en place de la prévention des pertes de données

- Politiques de prévention des pertes de données
- Message Actions
- Mise à jour du moteur DLP et des classificateurs de correspondance de contenu

Module 10 : Utilisation du LDAP

- Vue d'ensemble du LDAP
- Travailler avec le LDAP
- Utilisation des requêtes LDAP
- Authentification des utilisateurs finaux de la quarantaine anti-spam
- Configuration de l'authentification LDAP externe pour les utilisateurs
- Test des serveurs et des requêtes
- Utilisation du LDAP pour la prévention des attaques de répertoires
- Requêtes de consolidation d'alias de quarantaine pour les spams
- Validation des destinataires à l'aide d'un serveur SMTP

Module 11 : Authentification de la session SMTP

- Configuration d'AsyncOS pour l'authentification SMTP
- Authentification des sessions SMTP à l'aide de certificats de clients
- Vérification de la validité d'un certificat de client
- Authentification de l'utilisateur à l'aide du répertoire LDAP
- Authentification de la connexion SMTP par la couche de transport de sécurité (TLS) à l'aide d'un certificat de client
- Établissement d'une connexion TLS à partir de l'appareil
- Mise à jour d'une liste de certificats révoqués

Module 12 : Authentification de l'email

- Aperçu de l'authentification du courrier électronique
- Configuration des DomainKeys et signature du courrier identifié (DKIM)
- Vérification des messages entrants à l'aide de DKIM
- Aperçu du cadre de la politique d'envoi (SPF) et de la vérification du SIDF
- Rapport d'authentification de message par domaine et vérification de conformité (DMARC)
- Détection des faux courriers électroniques

Module 13 : Cryptage du courrier électronique

- Aperçu du cryptage du courrier électronique par Cisco
- Cryptage des messages
- Déterminer les messages à crypter
- Insertion d'en-têtes de cryptage dans les messages
- Cryptage des communications avec d'autres agents de transfert de messages (MTA)
- Travailler avec des certificats
- Gestion des listes d'autorités de certification
- Activation du TLS sur une table d'accès à l'hôte d'un auditeur (HAT)
- Permettre la vérification des TLS et des certificats à la livraison
- Services de sécurité S/MIME (Secure/Multipurpose Internet Mail Extensions)

Module 14 : Utilisation des systèmes de quarantaine et des méthodes de livraison

- Description des quarantaines
- Quarantaine pour les spams

- Mise en place de la quarantaine centralisée pour les spams
- Utilisation de listes de sécurité et de listes de blocage pour contrôler la distribution du courrier électronique en fonction de l'expéditeur
- Configuration des fonctionnalités de gestion des spams pour les utilisateurs finaux
- Gestion des messages dans le cadre de la quarantaine anti-spam
- Politique, virus et quarantaine
- Gestion des politiques, des virus et des quarantaines
- Travailler avec les messages dans les politiques, les virus ou les quarantaines
- Méthodes de livraison

Module 15 : Gestion centralisée à l'aide de clusters

- Aperçu de la gestion centralisée à l'aide des clusters
- Organisation du cluster
- Créer et rejoindre un cluster
- Gestion des clusters
- Communication des clusters
- Chargement d'une configuration dans les appareils en cluster
- Best Practices

Module 16 : Tests et dépannage

- Débogage du flux de courrier à l'aide de messages de test : Trace
- Utilisation de l'écouteur pour tester l'appareil
- Dépannage du réseau
- Dépannage de l'auditeur
- Dépannage de l'envoi de courriers électroniques
- Dépannage des performances
- Aspect de l'interface web et problèmes de rendu
- Répondre aux alertes
- Dépannage des problèmes de matériel
- Travailler avec le soutien technique

Module 17 : Références

- Modèle de spécifications pour les grandes entreprises
- Modèle de spécifications pour les entreprises de taille moyenne et les petites et moyennes entreprises ou succursales
- Spécifications du modèle Cisco Email Security Appliance pour les appareils virtuels
- Forfaits et licences

Lab / Exercices
Laboratoires officiels CISCO

- Vérifier et tester la configuration Cisco ESA
- Effectuer l'administration de base
- Malware avancé dans les pièces jointes (macro-détection)
- Protection contre les URL malveillants ou indésirables sous les URL raccourcis
- Protection contre les URL malveillantes ou indésirables dans les pièces jointes
- Gérer intelligemment les messages non scannables
- Exploiter les renseignements du cloud AMP grâce à l'amélioration de la pré-classification
- Intégrer Cisco ESA avec la console AMP
- Prévenir les menaces grâce à la protection antivirus

- Application de filtres de contenu et d'outbreaks
- Configurer la numérisation des pièces jointes
- Configurer la prévention des pertes de données sortantes
- Intégrer Cisco ESA avec LDAP et activer la requête d'acceptation LDAP
- Courrier identifié par des clés de domaine (DKIM)
- Cadre politique de l'expéditeur (SPF)
- Détection des faux courriers électroniques
- Configurer le Cisco SMA pour le suivi et les rapports

Documentation

- Support de cours numérique officiel CISCO

Examen

- Ce cours vous prépare à passer l'examen "Securing Email with Cisco Email Security Appliance (300-720 SESA)" qui mène aux certifications "CCNP® Security et Certified Specialist - Email Content Security"

Profils des participants

- Architectes sécurité
- Ingénieurs sécurité, opérationnel et réseau
- Administrateurs réseau et sécurité
- Techniciens de réseau ou de sécurité
- Gestionnaires de réseaux
- Concepteurs de systèmes

Connaissances Préalables

- Certification Cisco (certification Cisco CCENT® ou supérieure)
- Certifications industrielles pertinentes, telles que (ISC)2, CompTIA Security+, EC-Council, Global Information Assurance Certification (GIAC), et ISACA
- Attestation d'achèvement de la 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+)
- Les services TCP/IP, y compris le système de noms de domaine (DNS), Secure Shell (SSH), FTP, Simple Network Management Protocol (SNMP), HTTP et HTTPS
- Expérience en matière de routage IP

Objectifs

- Administrer le Cisco Email Security Appliance (ESA)
- Contrôler les domaines expéditeur et destinataire
- Contrôler le spam avec Talos SenderBase et l'anti-spam
- Utiliser des filtres anti-virus et outbreak
- Utiliser les politiques de mail
- Utiliser des filtres de contenu
- Utiliser des filtres de messages pour appliquer les politiques mail
- Prévenir la perte de données
- Effectuer des requêtes LDAP
- Authentifier les sessions SMTP
- Authentifier les e-mails
- Chiffrer les e-mails

- Utiliser des systèmes de quarantaine et des méthodes de diffusion
- Effectuer une gestion centralisée à l'aide de clusters
- Tester et dépanner

Niveau
Avancé
Prix de l'inscription en Virtuel (CHF)
3560
Durée (Nombre de Jours)
4
Reference
CIS-SESA