Formation Sécuriser les emails avec Cisco Email Security Appliance

Description de la formation Cisco Email Security Appliance

Cette **formation Cisco Email Security Appliance** vous explique comment déployer et utiliser l'appliance Cisco Email Security (ESA) pour établir une protection de vos systèmes de messagerie contre le phishing, la messagerie commerciale et les ransomwares, et pour aider à rationaliser la sécurité de messagerie et la gestion des politiques.

Ce cours pratique vous fournit les connaissances et les compétences nécessaires pour mettre en œuvre, dépanner et administrer l'appliance Cisco Email Security, notamment des fonctionnalités clés telles que la protection avancée contre les programmes malveillants, le blocage du courrier indésirable, la protection anti-virus, le filtrage des épidémies, le cryptage, la mise en quarantaine et les données et la prévention des pertes.

Objectifs

Objectifs opérationnels :

Savoir installer, configurer, administrer, dépanner et tester Cisco Email Security Appliance.

Objectifs pédagogiques :

Concrètement, à l'issue de cette **formation Cisco Email Security Appliance**, vous serez en mesure de :

- Décrire et administrer le Cisco Email Security Appliance (ESA)
- Contrôler les domaines expéditeurs et destinataire
- Contrôler le spam avec Talos SenderBase et l'anti-spam
- Utiliser des filtres anti-virus et out break
- 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 (Simple Mail Transfer Protocol)
- 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

À qui s'adresse cette formation ?

Public :

Ce cours Cisco Email Security Appliance s'adresse aux administrateurs systèmes ainsi qu'à tous les employés s'occupant de la messagerie (designers, architectes, gestionnaires réseaux...).

Prérequis :

Pour suivre cette formation Cisco Email Security Appliance, il est nécessaire de connaître au préalable 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. Il est également demandé d'avoir une expérience en matière de routage IP.

Contenu du cours Cisco Email Security Appliance

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

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

Contrôle des domaines de l'expéditeur et du destinataire

Auditeurs publics et privés

Configuration du gateway pour la réception de courriers électroniques

Aperçu de l'Host Access Table

Aperçu du Récipient Access Table

Configuration des fonctions de routage et de transmission

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)

Utilisation de filtres anti-virus et out breaks

Aperçu de l'analyse antivirus

Filtrage anti-virus Sophos

Filtrage anti-virus McAfee

Configuration de l'appareil pour la recherche de virus

Filtres d'out breaks

Fonctionnement du dispositif de filtrage des out breaks

Gestion des filtres d'out breaks

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

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

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

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

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

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

Authentification de l'email

Aperçu de l'authentification du courrier électronique

Configuration des Domain Keys 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

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)

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

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

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

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

Travaux Pratiques

Les travaux pratiques de cette formation Cisco vous inviteront à :

- 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'out breaks
- 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