CISCO : Sécuriser les emails avec Cisco Email Security Appliance

Référence : **SESA** Durée : **3 jours** Certification : **300-720**

CONNAISSANCES PREALABLES

• Il est recommandé d'avoir suivi le cours CCNA - CISCO : Mettre en œuvre et administrer des solutions réseaux.

PROFIL DES STAGIAIRES

• Responsables de la mise en oeuvre de la messagerie tels que les gestionnaires de messagerie d'entreprise, les administrateurs systèmes, les designers de messagerie, les architectes ou gestionnaires réseaux.

OBJECTIFS

• Décrire et administrer l'appliance Cisco Email Security (ESA). • Contrôler les domaines expéditeur et destinataire. • Contrôler le spam avec Talos SenderBase et anti-spam. • Utiliser des filtres anti-virus et anti-épidémies. • Utiliser les politiques de messagerie. • Utiliser des filtres de contenu. • Utiliser des filtres de message pour appliquer les stratégies de messagerie. • Prévenir la perte de données. • Effectuer des requêtes LDAP. • Authentifier les sessions SMTP (Simple Mail Transfer Protocol). • Authentifier le courrier électronique. • Crypter le courrier électronique. • Utiliser les méthodes de mise en quarantaine et de remise du système. • Effectuer une gestion centralisée à l'aide de clusters. • Tester et dépanner.

CERTIFICATION PREPAREE

Securing Email with Cisco Email Security (SESA). Cette formation vous aide à vous préparer l'examen 300-720 SESA, qui mène aux certifications CCNP® Security et Certified Specialist - Email Content Security.

METHODES PEDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

Consultant-Formateur expert Security Cisco

METHODE D'EVALUATION DES ACQUIS

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation de fin de stage adressée avec la facture

CONTENU DU COURS

Rappels sur les Cisco ESA - Email Security Appliance

- Présentation de l'appliance Cisco Email Security
- Cas d'utilisation de la technologie
- Fiche technique de Cisco Email Security Appliance
- Présentation de SMTP
- Présentation du pipeline de messagerie
- Scénarios d'installation
- Configuration initiale de l'appliance Cisco Email Security
- Centralisation des services sur un dispositif SMA (Cisco Content Security Management Appliance)
- Notes de publication pour AsyncOS 11.x

Administration de Cisco ESA

- 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 réseau avancée

- Utiliser Email Security Monitor
- Suivi des messages
- Logging

Contrôle des domaines expéditeurs et destinataires

- Configurer les auditeurs publics et privés
- Configurer la passerelle pour recevoir un courrier électronique
- Décrire les Tables d'accès des hôtes (HAT)
- Décrire les Tables d'accès des destinataires (RAT)
- Décrire les méthodes d'authentification des messages
- Définir l'authentification des messages basée sur les domaines
- Configuration des fonctionnalités de routage et de livraison
- Dépanner avec les journaux des mails

Contrôler les spams avec Cisco SensorBase et Antispam

- Décrire SensorBase
- Configurer et utiliser Antispam sur les Cisco ESA Mise en quarantaine des Spam
- Décrire Safelist et Blocklist
- Mise en quarantaine des spam sur Cisco SMA
- Configurer la vérification "Bounce"
- Décrire les filtres Web Reputation
- Définir le déclenchement des filtres

Utilisation de Antivirus, filtrage « Outbeak » des virus et protection avancée contre les logiciels malveillants

- Activer le déclenchement de l'antivirus
- Utiliser le déclenchement des filtres
- Utiliser la protection avancée contre les logiciels malveillants

Utilisation des stratégies de messagerie

- Vue d'ensemble de Email Security Manager
- Stratégies de messagerie basées sur l'utilisateur
- Fragmentation des messages

Utilisation des filtres de contenu

- Décrire le filtrage de contenu
- Décrire le filtrage de contenu de base
- Applications du filtrage de contenu
- Décrire et configurer le filtrage de messages

Utilisation de filtres de message pour appliquer les stratégies de messagerie

- Présentation des filtres de message et de leurs composants
- Traitement du filtre de message
- Règles de filtrage des messages
- Actions de filtrage des messages
- Numérisation de pièces jointes
- Exemples de filtres de messages d'analyse de pièces jointes
- Utilisation de la CLI pour gérer les filtres de messages
- Exemples de filtres de messages
- Configuration du comportement de numérisation

Prévention de la perte de données

- Identifier les problèmes de perte de données
- Choisir une solution Cisco DLP
- Mettre en œuvre la configuration DLP
- Décrire RSA Engine

Utilisation de LDAP

- Utiliser les requêtes LDAP
- Authentifier des utilisateurs finaux de la mise en quarantaine du courrier indésirable
- Configurer l'authentification LDAP externe pour les utilisateurs
- Tester des serveurs et des requêtes
- Utiliser LDAP pour la prévention des attaques d'exploration d'annuaire
- Requêtes de consolidation d'alias de quarantaine de spams
- Valider des destinataires à l'aide d'un serveur SMTP

Authentification de session SMTP

- Configuration de l'authentification AsyncOS pour SMTP
- Authentification des sessions SMTP à l'aide de certificats clients
- Vérification de la validité d'un certificat client
- Authentification d'un utilisateur à l'aide du répertoire LDAP
- Authentification de la connexion SMTP sur TLS (Transport Layer Security) à l'aide d'un certificat client
- Établissement d'une connexion TLS à partir de l'appliance
- Mise à jour d'une liste de certificats révoqués

Authentification par email

- Aperçu de l'authentification par courrier électronique
- Configuration de DomainKeys et de MailDKIM Identified de DomainKeys)
- Vérification des messages entrants à l'aide de DKIM
- Présentation du cadre de politique des expéditeurs (SPF) et vérification SIDF
- Vérification de la conformité et du rapport de conformité et d'authentification de message basée sur le domaine (DMARC)
- Détection de courriels forgés

Cryptage Email

- Présentation de Cisco Email Encryption
- Cryptage des messages
- Détermination des messages à chiffrer
- Insérer des en-têtes de chiffrement dans des messages
- Chiffrement de la communication avec d'autres agents de transfert de message (MTA)
- Travailler avec des certificats
- Gestion des listes d'autorités de certification
- Activation de TLS sur une table d'accès hôte (HAT) d'un auditeur
- Activation de la vérification TLS et du certificat à la livraison
- Services de sécurité S / MIME (Internet Mail Extensions) sécurisés / polyvalents

Utilisation de la quarantaine système et des méthodes de livraison

- Description des quarantaines
- Quarantaine du spam
- Configuration de la mise en quarantaine centralisée du courrier indésirable
- Utilisation de listes sécurisées et de listes de blocage pour contrôler la distribution des e-mails en fonction de l'expéditeur
- Configuration des fonctionnalités de gestion du spam pour les utilisateurs finaux
- Gestion des messages en quarantaine du courrier indésirable
- Mise en quarantaine des stratégies, des virus et des épidémies
- Gestion de la stratégie, des virus et des quarantaines épidémiques
- Utilisation de messages dans les stratégies, les virus ou les quarantaines épidémiques
- Méthodes de livraison

Gestion centralisée à l'aide de clusters

- Présentation de la gestion centralisée à l'aide de clusters
- Organisation du cluster
- Créer et rejoindre un cluster
- Gestion des clusters
- Communication de cluster
- Chargement d'une configuration dans des appliances en cluster
- Meilleures pratiques

Test et dépannage

- Débogage du flux de messagerie à l'aide de messages de test : trace
- Utilisation de l'écouteur pour tester l'appliance
- Dépannage du réseau
- Dépannage de l'auditeur
- Dépannage de la livraison par courrier électronique
- Dépannage des performances
- Problèmes d’apparence et de rendu de l’interface Web
- Répondre aux alertes
- Résolution des problèmes matériels
- Travailler avec le support technique

Les références

- Spécifications du modèle pour les grandes entreprises
- Spécifications de modèle pour les entreprises moyennes et les petites ou moyennes entreprises ou les succursales
- Spécifications du modèle d'appareil Cisco Email Security pour les appareils virtuels
- Forfaits et licences

Certification Cisco Securing Email with Cisco Email Security (SESA)

- Cette formation prépare au pssage de la certification Cisco Securing Email with Cisco Email Security (SESA)