CISCO : Sécurisation des e-mails avec Cisco Email Security Appliance

Référence : **SESA** Durée : **4 jours** Certification : **300-720**

CONNAISSANCES PREALABLES

• Certification Cisco (certification Cisco CCENT® ou supérieure). • Certification de l'industrie pertinente, telle que (ISC) 2, CompTIA Security +, EC-Council, Global Information Assurance Certification (GIAC) et ISACA. • Expérience avec le routage IP. • Expertise Windows : Microsoft [spécialiste Microsoft, Microsoft Certified Solutions Associate (MCSA), Microsoft Certified Systems Engineer (MCSE)], CompTIA (A +, Network +, Server +). • Lettre d'achèvement de Cisco Networking Academy (CCNA® 1 et CCNA 2). • Services TCP / IP, y compris DNS (Domain Name System), Secure Shell (SSH), FTP, SNMP (Simple Network Management Protocol), HTTP et HTTPS.

PROFIL DES STAGIAIRES

• Administrateurs de sécurité. • Administrateurs réseau. • Architectes de sécurité. • Concepteurs de systèmes. • Gestionnaires de réseau. • Ingénieurs d'exploitation. • Ingénieurs réseau. • Ingénieurs sécurité. • Intégrateurs et partenaires Cisco. • Techniciens réseau ou sécurité.

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

Décrire l'appliance de sécurité de messagerie Cisco

- Présentation de l'appliance de sécurité de messagerie Cisco
- Cas d'utilisation de la technologie
- Fiche technique de l'appliance de sécurité de messagerie Cisco
- Présentation de SMTP
- Présentation du pipeline de messagerie
- Scénarios d'installation

- Configuration initiale de Cisco Email Security Appliance
- Centraliser les services sur une appliance de gestion de la sécurité du contenu Cisco (SMA)
- Notes de version pour AsyncOS 11.x

Administration de Cisco Email Security Appliance

- Distribution des tâches administratives
- L'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
- Utilisation de Email Security Monitor
- Messages de suivi
- Enregistrement

Contrôle des domaines expéditeur et destinataire

- Auditeurs publics et privés
- Configuration de la passerelle pour recevoir des e-mails
- Présentation de la table d'accès à l'hôte
- Présentation de la table d'accès des destinataires
- Configuration des fonctionnalités de routage et de livraison

Contrôle du spam avec Talos SenderBase et Anti-Spam

- Présentation de SenderBase
- Anti-spam
- Gérer Graymail
- Protection contre les URL malveillantes ou indésirables
- Filtrage de la réputation des fichiers et analyse des fichiers
- Vérification du rebond

Utilisation de filtres antivirus et anti-épidémies

- Présentation de l'analyse antivirus
- Filtrage antivirus Sophos
- Filtrage antivirus McAfee
- Configuration de l'appliance pour rechercher les virus
- Filtres anti-épidémies
- Fonctionnement de la fonction Filtres anti-épidémies
- Gestion des filtres d'épidémie

Utilisation des stratégies de messagerie

- Présentation de Email Security Manager
- Présentation des stratégies de messagerie
- Gestion différente des messages entrants et sortants
- Faire correspondre les utilisateurs à une stratégie de messagerie
- Éclatement de message
- Configuration des politiques de messagerie

Utilisation de filtres de contenu

- Présentation des filtres de contenu
- Conditions de filtrage du contenu
- Actions de filtrage de contenu
- Filtrer les messages en fonction du contenu
- Présentation des ressources textuelles
- Utilisation et test des 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 appliquer des stratégies de messagerie

- Présentation des filtres de messages
- Composants d'un filtre de messages
- Traitement du filtre des messages
- Règles de filtrage des messages
- Actions de filtrage des messages
- Numérisation des pièces jointes
- Exemples de filtres de messages d'analyse des pièces jointes
- Utilisation de la CLI pour gérer les filtres de messages
- Exemples de filtres de messages
- Configuration du comportement de scan

Prévenir la perte de données

- Présentation du processus de numérisation DLP (Data Loss Prevention)
- Configuration de la prévention de la perte de données
- Stratégies de prévention de la perte de données
- Actions de message
- Mise à jour du moteur DLP et des classificateurs de correspondance de contenu

Utilisation de LDAP

- Présentation de LDAP
- Travailler avec LDAP
- Utilisation de requêtes LDAP
- Authentification des utilisateurs finaux de la quarantaine de spam
- Configuration de l'authentification LDAP externe pour les utilisateurs
- Test des serveurs et des requêtes
- Utilisation de LDAP pour la prévention des attaques de récolte d'annuaire
- Requêtes de consolidation d'alias de quarantaine de spam
- Validation des destinataires à l'aide d'un serveur SMTP

Authentification de session SMTP

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

Authentification par courriel

- Présentation de l'authentification des e-mails
- Configuration de la signature DomainKeys et DomainKeys Identified Mail (DKIM)
- Vérification des messages entrants à l'aide de DKIM

- Vérification des messages entrants à l'aide de DKIM
- Vérification des rapports et de la conformité de l'authentification des messages basée sur le domaine (DMARC)
- Détection des e-mails falsifiés

Cryptage des e-mails

- Vue d'ensemble de Cisco Email Encryption
- Chiffrement des messages
- Détermination des messages à chiffrer
- Insertion d'en-têtes de chiffrement 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 de TLS sur la table d'accès à l'hôte d'un auditeur (HAT)
- Activation de TLS et de la vérification des certificats à la livraison
- Services de sécurité S / MIME (Secure Internet Multipurpose Internet Extensions)

Utilisation des quarantaines système et des méthodes de livraison

- Décrire les quarantaines
- Spam Quarantine
- Configuration de la quarantaine de spam centralisée
- Utilisation de listes fiables et de listes de blocage pour contrôler la remise des e-mails en fonction de l'expéditeur
- Configuration des fonctionnalités de gestion du spam pour les utilisateurs finaux
- Gestion des messages dans la quarantaine de spam
- Stratégie, virus et quarantaines d'épidémies
- Gestion des quarantaines de stratégie, de virus et d'épidémie
- Utilisation des messages dans les quarantaines de stratégie, de virus ou d'épidémie
- Modes 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
- Gérer les clusters
- Communication de cluster
- Chargement d'une configuration dans des appliances en cluster
- Les 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'écouteur
- Dépannage de la remise des e-mails
- Dépannage des performances
- Problèmes d'apparence et de rendu de l'interface Web
- Répondre aux alertes
- Dépannage 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)