SÉCURISER LES EMAILS AVEC CISCO EMAIL SECURITY APPLIANCE

Cette formation permet aux participants d'acquérir les compétences et connaissances nécessaires pour installer, configurer et gérer Cisco Email Security Appliance dans un environnement d'entreprise de moyenne envergure. Les labs permettent de renforcer les connaissances et les connaissances de base sur le dépannage.

CODE DE LA FORMATION:
CS-SC-SESA

ÉDITEUR OU CONSTRUCTEUR:
CISCO

VERSION:
2.1

DURÉE:
5 JOURS

PRÉREQUIS:

- Avoir des connaissances sur les fondamentaux TCP/IP
- Avoir de l'expérience dans la messagerie Internet, incluant SMTP, les formats de messages Internet et les formats de messages MIME
- Le suivi du cours ICND2 est recommandé

PUBLIC:

Cette formation s'adresse aux responsables de la mise en œuvre de la messagerie tels que les gestionnaires de messagerie d'entreprise, les administrateurs systèmes, les designers de messagerie, les architectes ou gestionnaires réseaux.

OBJECTIFS:

- Installer et administrer Cisco Email Security Appliance
- Définir l'authentification des messages basés sur les domaines
- Décrire la fonction des filtres Web
- Comprendre et configurer le déclenchement des filtres
- Contrôler les domaines expéditeurs et destinataires
- Contrôler les Spam avec Cisco SensorBase et antispam
- Comprendre et configurer la protection avancée contre les logiciels malveillants avec Cisco SourceFire via « file reputation » et les services d’analyses
- Expliquer comment les résultats de la protection avancée contre les logiciels malveillants peuvent être appliqués au filtrage de contenu
- Utiliser les stratégies de messagerie
- Utiliser les filtres de contenus
- Décrire le filtrage d'URL
- Configurer le filtrage des messages pour détecter les attaques volumineuses de messages
- Prévenir la perte de données
- Utiliser LDAP
- Utiliser l'authentification et le cryptage
- Utiliser les filtres des messages
- Utiliser le système de Quarantaine et les méthodes de délivrance
- Créer un environnement en cluster
- Dépanner les Cisco ESA

CONTENU:

Rappels sur les Cisco ESA

- Rappels sur les Cisco SMA
- Définir la conversation SMTP
- Identifier les termes et définitions
- Examiner le Pipeline
- Définir les modèles Cisco ESA et la gestion des licences
- Installer et vérifier Cisco Email Security Appliance

Administration de Cisco ESA

- Configurer la localisation des messages et le reporting
- Configurer la centralisation et le reporting
- Configurer Cisco SMA pour la localisation et les messages de reporting
- Administrer Cisco ESA
- Gérer les fichiers journaux
- Créer et utiliser les comptes administrateurs

Contrôle des domaines expéditeurs et destinataires

- Configurer les auditeurs publics et privés
- 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
- 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 d'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

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

- Présenter les fonctionnalités LDAP
- Requête jeton et opérateurs
- Configurer et profils LDAP
- Configurer les “Call-Ahead” SMTP
- Etude de cas universitaire
- Utiliser les requêtes de groupe LDAP

Utilisation de l'Authentification et cryptage

- Configurer le service Cisco Registered Envelope
- Décrire TLS
- Utiliser SPF pour authentifier les emails

Utilisation des filtres de messages

- Identifier les filtres de messages
- Notions de base des expressions régulières
- Applications de filtres de messages

Utilisation du système de Quarantaine et méthodes de délivrance

- Vue d'ensemble de la Quarantaine
- Stratégie centralisée, Virus et déclenchement de la quarantaine
- Fixer les limites de la délivrance
- Créer les passerelles virtuelles
- Configurer les profils Bounce

Clustering

- Créer un environnement de cluster
- Joindre un cluster existant
- Gérer un environnement de cluster
- Administrer un cluster à partir d'une interface graphique de configuration

Dépannage

- Identifier les catégories des problèmes relatifs aux appliances
- Surveiller le système
- Diagnostiquer les problèmes
- Problèmes courants et solutions