Securing Email with Cisco Email Security Appliance (SESA)

Durée : 03 jours.

Ref : CI- SESA

Formateur : Certifié

A qui s'adresse cette formation

- Aux administrateurs systèmes
- A tous les employés s'occupant de la messagerie (designers, architectes, gestionnaires réseaux...)

Certifications

Cette formation fait partie de la certification:

- Cisco Certified Network Professional Security (CCNP)

Pré-requis

Avant de suivre cette formation, le stagiaire doit posséder les connaissances suivantes:

-
- Posséder des compétences et connaissances sur les fondamentaux TCP/IP (comportant les modules suivants: l'adressage IP et le sous-réseau, le routage statique IP et DNS)
- Posséder des compétences sur la messagerie internet (comportant les modules suivants: SNMTP, les formats de messages Internet et les formats de messages MIME)
- Connaitre et savoir manipuler l'interface en ligne de commandes (CLI) ainsi que l'interface graphique utilisateur (GU)*
- Posséder des connaissances sur la sécurité des emails

Objectifs

A l'issue de la formation, le stagiaire sera en mesure de:

- Configurer et mettre en oeuvre l'application Cisco de sécurité des mails.
- Intégrer un service d'annuaire via LDAP
- Analyser et réaliser le dépannage des problèmes d'intégration de LDAP
- Utiliser les différents filtres afin de modifier de réorienter les emails
- Déployer en toute sécurité et réaliser le dépannage des filtres
- Configurer TLS et le GSD (Guaranteed Secure Delivery)
- Authentifier les emails à l'aide de DKIM et SPF

Contenu

Durant les 3 jours de formations, les modules suivants seront abordés:

Présentation de IronPort

- Présentation de la technologie et du produit
- Mettre en oeuvre et configurer IronPort

Organisation des mises en oeuvre

- Mettre en oeuvre et configurer le système
- Déterminer les expéditeurs ainsi que les groupes de destinataires

Paramétrer le public concerné

- Elaborer la stratégie de flux des messages
- Table d'accès des hôtes et des groupes de destinataires
- Routes SMTP
- Anti-Spam

Stopper les SPAMs à l'aide d'IronPorts

- Paramétrer et appliquer les "sender base reputation scores" ainsi que "content adpative scanning engine"
- Paramétrer et installer les Anti-Virus et Filtres
- Paramétrer l'activation d'un ou plusieures Anti-Virus
- Appliquer les filtres contre les virus pour une protection "Zerohour"
- Utilisation des stratégies

Concevoir des stratégies pour les mails des utilisateurs

- Déterminer les messages fractionnés
- Détailler la localisation centralisée (Rapports)
- Réaliser la localisation de messages

Elaborer et guider en quarantaines

- Consacrer des utilisateurs en quarantaine
- Attribuer des "bounce profiles"
- Elaborer des passerelles virtuelles

- Réaliser le filtrage de contenus

Détailler le scan des contenus

- Paramétrer la détection d'objet intégré
- Identifier les pièces jointes non protégées ou protégées par mot de passe
- Analyser des identifiants "intelligents"
- Crypter les messages

Le paramétrage d'une demande chiffrée

- Répondre avec le "Cisco Registered Envelope Service"
- Répondre avec un Serveur local de clés
- Dans une action de chiffrement lier une action de filtrage
- Paramétrer des demandes LDAP

Présentation de LDAP

- Jetons et opérateurs de demandes
- Paramétrer un profil LDAP ainsi que des "Call-Ahead" SMTP
- Appliquer les demandes groupées LDAP
- Routage LDAP et "masquerading"

Appliquer LDAP pour des demandes de routage des messages

- LDAP et"pipe-line"
- Paramétrer les demandes de routage
- Controler le routage LDAP
- Appliquer LDAP pour les requêtes déguisées
- Paramétrage du filtrage des messages

Présentation du filtrage des emails

- Overview
- Administrer le filtrage des messages
- Paramétrer TLS

Overview de TLS

- Paramétrer TLS
- Identification des emails

Résoudre les problèmes d'authentification

- Overview, signature et vérification DKIM
- Présentation de la technologie SPF et SIDF
- Vérification SPF

Analyser et séparer les problèmes

- Identification des outils de dépannage
- Administrer le système

Instruments pour le support

- Sauvegarder et restaurer le système
- Mettre à jour le logiciel