Sécuriser les emails avec Cisco Email Security Appliance (SESA)

Assurer la sécurité des échanges par mail avec une appliance

Présentiel ou en classe à distance

Durée : 4 jours (28 h)

Réf. : CS86

Prix inter : 3.580,00 € HT

Destiné à protéger l'entreprise ou l'organisation de menaces pouvant être véhiculées par les emails, l'Appliance Cisco Email Security scrute l'intégralité des contenus qui transitent par la messagerie. Qu'il s'agisse de messages expédiés ou reçus, le dispositif réagit dès lors qu'il identifie du contenu assimilé à du spam, du phishing ou contenant un malware ou un virus en le plaçant automatiquement en quarantaine. Disposant de tout un arsenal technologique dédié à la sécurité des échanges par email, la solution peut être paramétrée très finement. Les administrateurs de la solution participants à cette formation de 4 jours apprendront à configurer les différents outils proposés avec l'Appliance.
Cette formation prépare à la certification Cisco Certified Network Professional Security (CCNP Security) et Cisco Certified Specialist - Email Content Security.

Les objectifs de la formation

- Apprendre à configurer et à mettre en oeuvre l'application Cisco de sécurité des mails
- Pouvoir intégrer un service d'annuaire via LDAP
- Être capable d'analyser et de réaliser le dépannage des problèmes d'intégration de LDAP
- Savoir utiliser les différents filtres afin de modifier et de réorienter les emails
- Comprendre comment déployer en toute sécurité et réaliser le dépannage des filtres
- Apprendre à configurer TLS et le GSD (Guaranteed Secure Delivery)
- Pouvoir authentifier les emails à l'aide de DKIM et SPF
- Se préparer à passer l'examen Securing Email with Cisco Email Security Appliance (300-720 SESA)

A qui s'adresse cette formation ?

Pour qui

- Administrateurs systèmes
- Toute personne s'occupant de la messagerie (designers, architectes, gestionnaires réseaux...)

Prérequis

- Posséder des compétences et connaissances sur les fondamentaux TCP/IP (l'adressage IP et le sous-réseau, le routage statique IP et DNS)
- Posséder des compétences sur la messagerie internet (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

Programme

1 - Présentation de IronPort

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

2 - Organisation des mises en oeuvre

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

3 - Paramétrer le public concerné

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

4 - 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 plusieurs Anti-Virus
- Appliquer les filtres contre les virus pour une protection "Zerohour"
- Utilisation des stratégies

5 - Concevoir des stratégies pour les mails des utilisateurs

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

6 - Élaborer et guider en quarantaines

- Consacrer des utilisateurs en quarantaine
- Attribuer des "bounce profiles"
- Élaborer des passerelles virtuelles
- Réaliser le filtrage de contenus

7 - 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

8 - 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

9 - 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"

10 - Appliquer LDAP pour des demandes de routage des messages

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

11 - Présentation du filtrage des emails

- Overview
- Administrer le filtrage des messages
- Paramétrer TLS

12 - Overview de TLS

- Paramétrer TLS
- Identification des emails

13 - Résoudre les problèmes d'authentification

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

14 - Analyser et séparer les problèmes

- Identification des outils de dépannage
- Administrer le système

15 - Instruments pour le support

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

Evaluation

- Cette formation fait l'objet d'une évaluation formative.

Les points forts de la formation

- La formation intègre de nombreux travaux pratiques qui favorisent une assimilation rapide et durable des thématiques abordées en cours.
- Les retours d'expérience de consultants-formateurs spécialistes de la technologie.
- La qualité d'une formation officielle Cisco (support de cours numérique en anglais).