# Sécuriser les emails avec Cisco Email Security Appliance

**Durée: 4 Jours Réf de cours: SESA Version: 3.1 Méthodes d'apprentissage: Intra-entreprise & sur-mesure**

## Résumé:

Cette formation Cisco explique comment déployer et utiliser l'appliance Cisco® Email Security pour établir une protection de vos systèmes de messagerie contre le phishing, la messagerie commerciale et les ransomwares, et pour aider à rationaliser la stratégie de sécurité de la messagerie. Ce cours pratique vous fournit les connaissances et les compétences nécessaires pour mettre en œuvre, dépanner et administrer l'appliance Cisco Email Security, notamment des fonctionnalités clés telles que la protection avancée contre les programmes malveillants, le blocage du courrier indésirable, la protection anti-virus, le filtrage des épidémies (spams), le cryptage, la mise en quarantaine et la prévention des pertes des données.
Le suivi de cette formation permet de valider un total de 24 crédits dans le cadre du programme d'Education Continue Cisco (CCE) pour les professionnels qui souhaitent renouveler leur titre de certification.

## Public visé:

Cette formation s'adresse aux 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 pédagogiques:

- A l'issue de la formation, les participants seront capables de :
- Contrôler les domaines expéditeur et destinataire, le spam avec Talos SenderBase et anti-spam
- Utiliser des filtres anti-virus, anti-épidémies (anti-spams), les politiques de messagerie et les 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) et 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

## Pré-requis:

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 niveau de connaissances de la certification CCNA est recommandé.

- CCNA - Mettre en oeuvre et administrer des solutions réseaux Cisco

## Test et certification

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

Le suivi de cette formation permet de valider un total de 24 crédits dans le cadre du programme d'Education Continue Cisco (CCE) pour les professionnels qui souhaitent renouveler leur titre de certification.

## Contenu:

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)
- Configuration des fonctionnalités de routage et de livraison

Contrôler les spams avec Talos 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
- Manager Graymail
- Protéger contre les URL malveillantes et indésirables

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

- Activer le déclenchement de l'antivirus

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

- Présenter les fonctionnalités 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

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

- 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

- 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

- 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

## Méthodes pédagogiques :

Support de cours officiel Cisco remis aux participants, en anglais.
Les participants réalisent un test d'évaluation des connaissances en amont et en aval de la formation pour valider les connaissances acquises pendant la formation.

## Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

• Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
• Votre place sera confirmée à la réception d'un devis ou """"booking form"""" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
• Attention, si cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés avant le début de la session pour vous inscrire via moncompteformation.gouv.fr.

Accueil des bénéficiaires :

• En cas de handicap : plus d'info sur globalknowledge.fr/handicap
• Le Règlement intérieur est disponible sur globalknowledge.fr/reglement