

Fortinet - Email Security FortiMail

Durée: 3 Jours **Réf de cours: ESF** **Méthodes d'apprentissage: Classe à distance**

Résumé:

Dans ce cours, vous analyserez les défis auxquels sont confrontés les administrateurs en matière de sécurité de la messagerie et vous apprendrez où et comment déployer, gérer et dépanner FortiMail afin de protéger votre réseau contre les menaces véhiculées par la messagerie.

Vous explorerez également le rôle du FortiMail en tant que solution spécifique, et la manière dont ses fonctionnalités offrent à la fois des performances élevées et une sécurité approfondie pour les communications critiques de l'entreprise.

Mis à jour 30/01/2025

Classe à Distance - site Client

Cette formation peut être suivie à distance en synchrone depuis n'importe quel site pourvu d'une connexion internet (2 Mb/s en symétrique recommandés). Le programme (théorie et pratique) suit le même déroulé pédagogique qu'en présentiel. La solution technologique adoptée permet aux apprenants à distance de suivre les présentations faites au tableau, de voir et d'entendre l'instructeur et les participants en temps réel, mais également d'échanger avec eux.

Public visé:

Ce cours s'adresse aux professionnels de la sécurité impliqués dans la gestion, la configuration, l'administration et la surveillance de FortiMail dans les déploiements de messageries de petites et moyennes entreprises.

Objectifs pédagogiques:

- A l'issue de cette formation, les participants seront en mesure de :
- Positionner FortiMail dans une infrastructure de messagerie existante ou nouvelle en utilisant l'un des différents modes de déploiement
- Comprendre l'architecture du système FortiMail : comment le courrier électronique circule à travers ses modules, comment il applique un routage intelligent et des politiques au courrier électronique, et comment il peut protéger la réputation inestimable de votre agent de transfert de messages (MTA)
- Utiliser votre serveur LDAP existant pour gérer et authentifier les utilisateurs
- Sécuriser la transmission du courrier électronique à l'aide des meilleures technologies, telles que SMTPS SMTP over TLS et le cryptage basé sur l'identité (IBE)
- Limiter les connexions clients pour bloquer les abus MTA
- Bloquer le spam à l'aide de techniques sophistiquées, telles que l'inspection approfondie des en-têtes, l'épidémie de spam, l'heuristique et le service FortiGuard Antispam
- Éliminer le spear phishing et les virus de type « zero-day »
- Intégrer FortiMail avec FortiSandbox pour une protection avancée contre les menaces (ATP)
- Prévenir les fuites accidentelles ou intentionnelles de données confidentielles et réglementées
- Archivage des courriels pour assurer la conformité
- Déployer une infrastructure à haute disponibilité (HA) et redondante pour une disponibilité maximale de la messagerie critique
- Diagnostiquer les problèmes courants liés à la messagerie et à FortiMail.
- NOTE : Ce cours couvre en profondeur les modes passerelle et serveur. Ce cours couvre également le mode transparent. Cependant, si vous avez besoin d'un cours détaillé sur l'utilisation du mode transparent dans des réseaux d'entreprises, vous devez commander une formation personnalisée.

Pré-requis:

Les participants doivent avoir une bonne compréhension des sujets couverts par le cours FCP - FortiGate Administrator, ou

Test et certification

■

avoir une expérience équivalente.

Il est également recommandé de connaître les sujets suivants :

- SMTP
- PKI
- SSL/TLS
- LDAP

Contenu:

- Concepts de l'email
- Configuration de base
- Contrôle d'accès et politiques
- Authentification
- Gestion des sessions
- Antivirus et antispam
- Inspection du contenu
- Sécurisation des communications
- Haute disponibilité
- Mode serveur
- Mode transparent
- Maintenance
- Dépannage

Méthodes pédagogiques :

Un support de cours officiel sera fourni aux participants.

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