+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 06/09/2024

S'inscrire

Formation Fortimail de Fortinet

(EDU-NSE6)

3 jours (21 heures)

Présentation

FortiMail pour protéger votre réseau contre les cybermenaces déjà identifiées et à utiliser FortiSandbox pour détecter et bloquer les cybermenaces émergentes. En laboratoire interactif, vous comprendrez en détail tout l'intérêt de FortiMail. Vous découvrirez des fonctionnalités allant encore bien au-delà du filtrage e-mail FortiGate.

FortiMail offre des performances élevées et une protection de pointe permettant de sécuriser les communications sensiblesde votre entreprise. Vous analyserez les défis auxquels sont confrontés les administrateurs et opérateurs de petites entreprises, en matière de sécurisation des e-mails. Vous découvrirez de quelle manière déployer FortiMail. Vous apprendrez à gérer cette solution et à la dépanner en cas de problème.

Notre formation FortiMail, vous enseignera la dernière version du programme à savoir Fortimail 7.6

Objectifs

- Positionner FortiMail dans une infrastructure de messagerie existante ou en cours de création, via les différents modes de déploiement flexibles proposés.
- Comprendre l'architecture système de FortiMail : circulation des e-mails à travers les modules, application des règles et d'un routage intelligent au courrier électronique et protection de la réputation de votre agent de transfert de messages (MTA)
- Utiliser votre serveur LDAP existant pour gérer et authentifier les utilisateurs.
- Sécuriser la transmission d'e-mails à l'aide de technologies de pointe : SMTPS, SMTP sur TLS et chiffrement basé sur l'identité.
- Limiter les connexions clients pour bloquer les abus de MTA
- bloquer les spams à l'aide de techniques sophistiquées telles que l'inspection approfondie des en-têtes, le recensement des épidémies de spam, l'heuristique et le service Antispam FortiGuard.
- Éliminer les pratiques d'hameçonnage (phishing) et les virus 0-day.
- Intégrer FortiMail à FortiSandbox pour une protection avancée contre les menaces

- Prévenir les fuites accidentelles ou intentionnelles de données confidentielles et réglementées
- Archiver les e-mails à des fins de conformité
- Déployer une infrastructure haute disponibilité (HA) et redondante pour assurer une disponibilité maximale des e-mails importants.
- Diagnostiquer les problèmes courants relatifs aux e-mails et à FortiMail

Public visé

Professionnels des réseaux et de la sécurité chargés de l'administration et l'assistance FortiMail

Prérequis

- Compréhension de base des concepts de mise en réseau TCP/IP et de sécurité des réseaux.
- La connaissance des éléments suivants est recommandée :
- Protocole SMTP (Simple Mail Transfer Protocol),infrastructure à clés publiques,
  - Sécurité de la couche de transport, Sécurité de la couche de transport,
  - Protocole RADIUS
  - Protocole LDAP

Prérequis techniques

- Vous devez avoir 2 disques durs virtuels pour faire fonctionner Fortimail VM

Programme

1. Concepts relatifs aux e-mails 2. Configuration de base 3. Contrôle et règles d'accès 4. Authentification 5. Gestion des sessions 6. Inspection des antivirus et du contenu 7. Antispam 8. Sécurisation des communications 9. Haute disponibilité 10.Mode serveur 11.Mode transparent 12.Maintenance et Dépannage

Certification

Ce cours vous prépare à l'examen de spécialiste FortiMail 7.2. Il fait également partie des cours préparant l'examen de certification NSE 6.

Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d’auto-évaluation nous permettant d’apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce

questionnaire nous permet également d’anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l’acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.