

Certifiante Sessions garanties disponibles

Formation FortiMail Administrator, préparation à l'examen Fortinet NSE 6

Réf. SF34165

Maîtrisez la sécurisation des messageries professionnelles face aux menaces avancées !

3 j
Durée

3 450 € HT
Inter / participant

3
Sessions à venir

Objectifs pédagogiques

- ✓ Intégrer FortiMail dans une infrastructure de messagerie existante ou nouvelle, en utilisant les différents modes de déploiement disponibles
- ✓ Limiter et contrôler les connexions clients afin de prévenir les abus des serveurs de messagerie
- ✓ Comprendre l'architecture interne de FortiMail et le cheminement des emails à travers ses modules de sécurité
- ✓ Bloquer efficacement le spam et les menaces grâce aux moteurs d'analyse avancés et aux services FortiGuard
- ✓ Mettre en œuvre l'authentification et la gestion des utilisateurs via un annuaire LDAP
- ✓ Protéger l'organisation contre le phishing ciblé, les malwares inconnus et les fuites de données
- ✓ Sécuriser les échanges de messagerie à l'aide de protocoles et mécanismes avancés (SMTPS, SMTP sur TLS, chiffrement basé sur l'identité)
- ✓ Diagnostiquer et résoudre les problèmes courants liés à la messagerie et à FortiMail

Public visé & prérequis

Public visé Ingénieurs télécoms et réseaux, Responsables de la sécurité des systèmes d'information (RSSI)

Prérequis Il est nécessaire de disposer de connaissances équivalentes à celles abordées dans la formation FortiGate Administrator ou d'une expérience comparable. Une compréhension des technologies suivantes est également recommandée : SMTP, PKI, SSL/TLS et LDAP.

Programme détaillé

Concepts de la messagerie électronique

Principes fondamentaux, flux de messages, enjeux de sécurité

Configuration initiale

Mise en service, paramètres de base, intégration réseau

Contrôle d'accès et politiques

Règles de traitement des emails et politiques de sécurité

Authentification

Gestion des utilisateurs, intégration LDAP

Gestion des sessions

Contrôle des connexions et prévention des abus

Antivirus et antisпам

Mécanismes de détection et de blocage des menaces

Inspection du contenu

Filtrage avancé et prévention des pertes de données

Sécurisation des communications

Chiffrement, TLS et protection des échanges

Haute disponibilité

Mise en œuvre d'architectures redondantes

Mode serveur

Fonctionnement et cas d'usage

Mode transparent

Déploiement et scénarios d'intégration

Maintenance

Sauvegardes, mises à jour et exploitation courante

Dépannage

Analyse et résolution des incidents

Prochaines sessions

DATE	LIEU	STATUT
23/11/2026	à distance	Sur confirmation
03/05/2027	à distance	Sur confirmation
08/11/2027	à distance	Sur confirmation

Pourquoi choisir Sparks Formation ?

20 ans d'expertise IT, des formateurs experts et des sessions garanties contre l'annulation.

20 ans
d'expertise

1 068+
formations

11 178
apprenants formés/an

+67
Net Promoter Score

Avis des participants

Note moyenne des participants de la filière Cybersécurité et Protection des Données : 4,9/5 — 13 avis

William B. — Prévoir l'envoi à chaque participant du livre de CISS au moins un mois avant la formation.

Mickael L. — il est top Romain GARCIA

Ils nous font confiance

Cette année notre filière Sécurité Défensive & Architecture (Blue Team) a accompagné plus de 25 entreprises dont :

ADVENTIEL ALTEN SA AMCS TECHNOLOGIES ARPEGE BIRDZ CA-GIP CHAPSVISION CHELA + CONSORT FRANCE ECONOCOM SERVICES & SOLUTION +15 autres

Financement & certifications

Cette formation est éligible aux financements OPCO et FNE-Formation. Nos équipes vous accompagnent dans le montage de votre dossier.



Réservez votre place dès maintenant

20 ans d'expertise · 1 000+ formations · NPS +67 · réponse sous 24h ouvrées

0 805 950 800

demande@sparks-formation.com