

Certifiante Sessions garanties disponibles

Formation FortiWeb Administrator, préparation à l'examen Fortinet NSE 5

Réf. SF34167

Maîtrisez le déploiement et la sécurisation d'applications web avec FortiWeb, du WAF aux API !

3 j
Durée

3 450 € HT
Inter / participant

1
Sessions à venir

Objectifs pédagogiques

- ✓ Expliquer le rôle d'un Web Application Firewall (WAF) et son intégration dans le réseau.
- ✓ Protéger les applications contre les attaques de DoS et de défiguration.
- ✓ Réaliser le déploiement initial et la configuration de base de FortiWeb.
- ✓ Déployer le chiffrement SSL/TLS (certificats, inspection et offloading).
- ✓ Mettre en œuvre FortiWeb dans une architecture load-balanç  e (serveurs virtuels/r  els, inspection, distribution de charge).
- ✓ Activer la protection des API et la mitigation des bots.
- ✓ Configurer les fonctions de s  curit   applicative : signatures, r  gles et s  curisation des sessions/cookies HTTP.
- ✓ Exploiter le machine learning de FortiWeb et effectuer un d  pannage de premier niveau.

Public vis   & pr  requis

Public vis   Administrateurs syst  mes et r  seaux, Ing  nieurs t  l  coms et r  seaux

Pr  requis Connaissances   quivalentes au contenu de FortiGate Administrator (ou exp  rience comparable). Compr  hension du protocole HTTP et bases en HTML, JavaScript et langages dynamiques c  t   serveur (ex. PHP). Pour le passage de l'examen, il est recommand   : 3 ans d'exp  rience avec les r  seaux informatiques, 1 an d'exp  rience avec la s  curit   des r  seaux et minimum 6 mois d'exp  rience pratique avec FortiWeb.

Programme d  taill  

Introduction

Pare-feu applicatif web (WAF) : principes et r  le dans l'architecture r  seau

Mise en route

D  ploiement initial et configuration de base

Conformit  

Mise en conformit   des applications web (PCI DSS)

Authentification et contr  le d'acc  s

Authentification des utilisateurs
Gestion des acc  s et des autorisations

S  curit   des applications web

Param  tres logiques et inspection des flux

Signatures et personnalisation
Gestion et sécurisation des sessions/cookies HTTP

DoS et défiguration

Protection contre les attaques par déni de service
Mécanismes de prévention de la défiguration

SSL/TLS et certificats

Gestion des certificats
Inspection SSL/TLS et offloading

Distribution applicative

Répartition de charge : serveurs virtuels et serveurs réels
Cache et compression
Routage, réécriture et redirection HTTP basés sur le contenu

Protection des API

Sécurisation des API
Atténuation des bots

Machine learning

Entraînement et configuration des fonctionnalités ML

Configuration complémentaire

Paramétrages additionnels et ajustements opérationnels

Dépannage

Méthodes et outils de diagnostic FortiWeb

Prochaines sessions

DATE	LIEU	STATUT
17/11/2026	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