Firewall Enterprise

Durée: 3 Jours Réf de cours: NSE7

Résumé:

Dans ce cours, vous apprendrez à mettre en œuvre et à gérer de manière centralisée une infrastructure de sécurité d'entreprise composée de plusieurs dispositifs FortiGate.
Ce cours suppose des connaissances avancées en matière de réseaux et une expérience pratique approfondie de FortiGate, FortiManager et FortiAnalyzer.
Mis à jour 16/01/2025

Public visé:

Ce cours est destiné aux professionnels des réseaux et de la sécurité impliqués dans la conception et l'administration d'une infrastructure de sécurité d'entreprise utilisant des dispositifs FortiGate.

Objectifs pédagogiques:

- Après avoir suivi ce cours, Les participants seront en mesure de:
- Intégrer FortiManager, FortiAnalyzer et plusieurs dispositifs FortiGate à l'aide de la Security Fabric de Fortinet
- Centraliser la gestion et la surveillance des événements de sécurité réseau
- Optimiser les ressources FortiGate
- Diagnostiquer et monitorer le traffic utilisateur en utilisant les outils de debug
- Corriger les problèmes avec le conserve mode, le cpu élevé, les policies firewall, les sessions helpers, les IPSEC, Fortiguard, l'inspection de contenu, le routage, et le HA
- Mettre en œuvre une solution de haute disponibilité sur FortiGate
- Déployer simultanément des tunnels IPsec vers plusieurs sites à l'aide de la console VPN du FortiManager
- Configurer ADVPN pour activer des tunnels VPN à la demande entre les sites
- Combiner OSPF et BGP pour acheminer le trafic de l'entreprise

Pré-requis:

Les participants doivent avoir une bonne compréhension des sujets abordés dans les cours suivants, ou avoir une expérience équivalente:

- FCP - FortiGate Security
- FCP - FortiGate Infrastructure

Il est également recommandé d'avoir une bonne compréhension des sujets abordés dans les cours suivants, ou d'avoir une expérience équivalente:

- FCP - FortiManager
- FCP - FortiAnalyzer

Test et certification

Contenu:

1. Introduction à l'architecture de la sécurité des réseaux
2. Accélération au niveau du matériel
3. Sécurité Fabric
4. Haute disponibilité
5. Gestion centralisée
6. OSPF
7. Passerelles frontalières (Border Gateway Protocol)
8. FortiGuard et profils de sécurité
9. Système de prévention des intrusions
10. VPN IPsec
11. VPN à découverte automatique

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