Formation Fortinet NSE4

FORTINET NSE4

5 Jours

Description synthétique de la formation

FortiGate Security:

Dans ce cours de 3 jours, vous apprendrez à utiliser les fonctionnalités de base de FortiGate, y compris les profils de sécurité. Dans les laboratoires interactifs, vous explorerez les politiques de pare-feu, l'authentification des utilisateurs, le VPN SSL, le VPN IPsec commuté et comment protéger votre réseau à l'aide de profils de sécurité tels que IPS, antivirus, filtrage Web, contrôle des applications, etc. Ces principes de base de l'administration vous fourniront une solide compréhension de la mise en oeuvre de la sécurité réseau de base.

FortiGate Infrastructure:

Dans ce cours de 2 jours, vous apprendrez à utiliser la mise en réseau et la sécurité avancées du FortiGate. Les sujets incluent des fonctionnalités couramment appliquées dans des réseaux d'entreprise ou MSSP complexes ou plus grands, tels que le routage avancé, le mode transparent, l'infrastructure redondante, le VPN IPsec site à site, l'authentification unique, le proxy Web et les diagnostics.

Objectifs pédagogiques

FortiGate Security:

- Déployez le mode de fonctionnement approprié pour votre réseau.
- Utilisez l'interface graphique et l'interface de ligne de commande pour l'administration.
- Identifier les caractéristiques du tissu de sécurité Fortinet.
- Contrôlez l'accès réseau aux réseaux configurés à l'aide des politiques de pare-feu.
- Appliquez le transfert de port, le NAT source et le NAT destination.
- Authentifiez les utilisateurs à l'aide de stratégies de pare-feu.
- Comprendre les fonctions de chiffrement et les certificats.
- Inspectez le trafic sécurisé par SSL/TLS pour empêcher le chiffrement utilisé pour contourner les politiques de sécurité.
- Configurez des profils de sécurité pour neutraliser les menaces et les abus, y compris les virus, les torrents et les sites Web inappropriés.
- Appliquez des techniques de contrôle des applications pour surveiller et contrôler les applications réseau susceptibles d'utiliser des protocoles et des ports standard ou non standard.
- Combattez le piratage et le déni de service (DoS).
- Protégez-vous contre les fuites de données en identifiant les fichiers contenant des données sensibles et empêchez-les de quitter votre réseau privé.
- Offrez un VPN SSL pour un accès sécurisé à votre réseau privé.
- Implémentez un tunnel VPN IPsec commuté entre un FortiGate et un FortiClient.
- Collectez et interprétez les entrées de journal.

FortiGate Infrastructure:

- Analysez la table de routage d'un FortiGate.
- Acheminez les paquets à l'aide de routes basées sur des règles et statiques pour les déploiements multi-chemins et à charge équilibrée.
- Configurez le SD-WAN pour équilibrer efficacement la charge du trafic entre plusieurs liaisons WAN.
- Inspectez le trafic de manière transparente, transférez-le en tant que périphérique de niveau 2.
- Divisez FortiGate en deux appareils virtuels ou plus, chacun fonctionnant comme un FortiGate indépendant, en configurant des domaines virtuels (VDOM).
- Établissez un tunnel VPN IPsec entre deux appliances FortiGate.
- Comparez les VPN IPsec basés sur des politiques et basés sur des routes.
- Implémentez un VPN maillé ou partiellement redondant.
- Diagnostiquer les échanges IKE ayant échoué.
- Offrez un accès Fortinet Single Sign On (FSSO) aux services réseau, intégré à Microsoft Active Directory.
- Déployez des appareils FortiGate en tant que cluster HA pour une tolérance aux pannes et des performances élevées.
- Déployez un proxy implicite et explicite avec des politiques de pare-feu, d'authentification et de mise en cache.
- Diagnostiquer et corriger les problèmes courants.

Public Concerné

Ingénieurs, administrateurs et techniciens réseaux.

Pré-requis

Une compréhension des couches du modèle OSI
Une connaissance de base des protocoles Internet TCP/IP
Une connaissance des concepts d'un firewall d'entreprise

Contenu du cours détaillé

FortiGate Security:

Jour 1 :

- Introduction and Initial Configuration
- Firewall Policie
- Network Address Translatio
- Firewall Authentication

Jour 2 :

- Logging and Monitoring
- Certificate Operations
- Web Filtering
- Application Control

Jour 3 :

- Antivirus
- IPS and Denial of Service
- Security Fabric

FortiGate Infrastructure:

Jour 4 :

- FSSO
- Virutal
- ZTNA

Jour 5 :

- SSL VPN
- IPSEC VPN
- HA
- Diagnostics

Mode d'évaluation

- L'évaluation par le formateur oralement chaque jour et auto-évaluation formalisée sur le Moodle.

Certification visée (si applicable)

- Fortinet NSE4