FortiGate Security

Durée : 3 Jours

Public visé

Les professionnels du réseau et de la sécurité impliqués dans la gestion, la configuration, l'administration et la surveillance des dispositifs FortiGate utilisés pour sécuriser les réseaux de leurs organisations. Les participants doivent avoir une compréhension approfondie de tous les sujets abordés dans le cours sur la sécurité FortiGate avant de suivre le cours sur l'infrastructure FortiGate.

Objectifs

Après avoir suivi ce cours, vous devriez être capable de :

• Déployer le mode de fonctionnement approprié pour votre réseau.

• Utiliser l'interface graphique (GUI) et la ligne de commande (CLI) pour l'administration.

• Identifier les caractéristiques du tissu de sécurité Fortinet.

• Contrôler l'accès au réseau des réseaux configurés à l'aide de politiques de pare-feu.

• Appliquer le transfert de port, le NAT source et le NAT de destination.

• Authentifier les utilisateurs à l'aide des politiques de pare-feu.

• Comprendre les fonctions de chiffrement et les certificats.

• Inspecter le trafic sécurisé par SSL/TLS pour empêcher l'utilisation du chiffrement pour contourner les politiques de sécurité.

• Configurer des profils de sécurité pour neutraliser les menaces et les abus, y compris les virus, les torrents et les sites web inappropriés.

• Appliquer des techniques de contrôle des applications pour surveiller et contrôler les applications réseau qui pourraient utiliser des protocoles et ports standards ou non standards.

• Combattre le piratage et les attaques par déni de service (DoS).

• Défendre contre les fuites de données en identifiant les fichiers contenant des données sensibles et les bloquer pour qu'ils ne quittent pas votre réseau privé.

• Offrir un VPN SSL pour un accès sécurisé à votre réseau privé.

• Mettre en œuvre un tunnel VPN IPsec dial-up entre FortiGate et FortiClient.

• Collecter et interpréter les entrées de journalisation.

Pré-requis

Connaissance des protocoles réseau
Compréhension de base des concepts de pare-feu

Contenu

Le plan de la formation est comme suit :

• Introduction à FortiGate et au tissu de sécurité
• Politiques de pare-feu
• Traduction d'adresses réseau (NAT)
• Authentification par pare-feu
• Journalisation et surveillance
• Gestion des certificats
• Filtrage web
• Contrôle des applications
• Antivirus
• Prévention des intrusions et déni de service
• VPN SSL
• VPN IPsec dial-up
• Prévention des fuites de données (DLP)