FORTINET - NSE5 - FortiManager

Durée: 2 jours
Public cible: Professionnel TI

À qui s'adresse cette formation ?

Toute personne responsable de la gestion quotidienne des politiques de sécurité FortiGate en utilisant la plateforme FortiManager

Objectifs de la formation

• Décrire les principales fonctionnalités et capacités de FortiManager • Déployer des domaines administratifs (ADOM) pour prendre en charge plusieurs clients sur un seul FortiManager • Restreindre l'accès simultané à ADOM en utilisant les espaces de travail et le mode de flux de travail • Utiliser des modèles de provisionnement pour les modifications au niveau de l'appareil sur de nombreux appareils • Identifier les états de synchronisation et gérer l'historique des révisions des dispositifs • Gérer les politiques de pare-feu sur plusieurs appareils FortiGate à l'aide de packages de politiques avec des objets partagés et dynamiques • Déployer des stratégies et des objets de l'ADOM global vers plusieurs ADOM • Comprendre l'intégration de Security Fabric avec FortiManager • Déployer le SD-WAN à l'aide de la gestion centralisée • Décrire les options de haute disponibilité (HA), de sauvegarde et de restauration pour FortiManager • Gérer le micrologiciel des appareils pris en charge de manière centralisée • Offrir un serveur de distribution FortiGuard local à vos appareils Fortinet • Diagnostiquer et résoudre les problèmes d'importation et d'installation

Description sommaire

Dans ce cours, vous apprendrez les bases de l'utilisation de FortiManager pour l'administration réseau centralisée de nombreux appareils FortiGate. Dans les laboratoires interactifs, vous explorerez les stratégies de déploiement, qui incluent plusieurs ADOM, enregistrement de périphérique, packages de stratégie, objets partagés, installation de modifications de configuration, provisionnement de FortiManager en tant que serveur de distribution FortiGuard locale et dépanner les fonctionnalités essentielles à l'utilisation quotidienne après déployer FortiManager.

Contenu du plan de cours

• Introduction et configuration initiale • Administration et gestion • Enregistrement de l'appareil • Configuration et installation au niveau du périphérique • Politique et objets • SD-WAN et Security Fabric • Diagnostics et dépannage • Configuration supplémentaire

Approche et méthode pédagogique

La formation privilégie une approche technico-pratique, alternant démonstrations et laboratoires sur la gestion centralisée des politiques de sécurité. Les participant.e.s travaillent sur des scénarios réalistes multi-équipements, afin de maîtriser le déploiement et la standardisation des configurations. L’animation met l’accent sur la résolution de problèmes et l’optimisation des pratiques, essentielles en environnement réel.

Recommandations

Bonnes connaissances de FortiOS / FortiGate et des politiques de sécurité réseau. Compréhension : concepts de gestion centralisée objets et politiques firewall Expérience en administration réseau multi-sites (atout)