

Fortigate I

Descripción del Curso

En este curso de 2 días, aprenderás como usar las características básicas de UTM de Fortigate. Con laboratorios interactivos, explorarás como hacer políticas de Firewall, VPNs básicas, detección de Virus, Filtro de Web, Control de aplicaciones autenticación de usuarios y más.

Estos fundamentos administrativos te proveerán con una sólida comprensión de cómo integrar seguridad básica a tu red.

Versiones de Producto

FortiGate 5.4

Agenda

1. Introducción a Fortinet UTM	7. VPNs de IPSec básicas
2. Logging y Monitoreo	8. Antivirus
3. Políticas de Firewall	9. Próxy Explícito
4. NAT	10. Web Filtering
5. Autenticación de Firewall	11. Control de Aplicaciones
6. VPNs de SSL	

Objetivos

Después de completar el curso, serás capaz de:

- Describir las capacidades UTM de Fortigate
- Neutralizar amenazas y abusos: virus, torrents y web sites inapropiados.
- Controlar el acceso a la red basado en los tipos de dispositivos.
- Autenticar usuarios a través de políticas de Firewall.
- Ofrecer una VPN de SSL para asegurar el acceso a tu red
- Establecer un túnel de VPN de IPSec entre dos dispositivos Fortigate.
- Comparar las VPNS de IPSec basadas en política contra las basadas en túnel.
- Aplicar port forwarding, source NAT, and destination NAT
- Interpretar entradas de log
- Generar Reportes
- Usar el GUI y el CLI para administración
- Implementar el modo de operación de Fortigate adecuado para cada caso.
- Implementar un proxy explícito con políticas de firewall, autenticación y caching.
- Simplificar el manejo de protocolos y control de aplicaciones.

Quién Debería de Asistir

Cualquiera que sea responsable de la administración del día a día de un dispositivo Fortigate. Debes de asistir a este curso antes de asistir al curso FortiGate II.

Prerrequisitos

Ninguna excepto experiencia en redes TCP/IP y comprensión básica de conceptos de Firewall.

Certificación

Este curso es parte de la preparación para el examen de certificación NSE 4