Curso de Fortinet

Código: FOR-001

Propuesta de Valor: SEGURIDAD INFORMÁTICA

Duración: 40 Horas

En este curso se aprenderá a utilizar las funciones básicas de Fortigate, incluyendo los perfiles de seguridad. Esto incluye la exploración de las políticas de firewall, la autenticación de usuarios, la configuración de la VPN con SSL, de una VPN dial-up con protocolo IPSEC, y cómo proteger todos estos componentes utilizando perfiles de seguridad, antivirus, filtros web, control de aplicaciones y más.

Los conceptos de administración que se brindan en el curso, permiten que el alumno un entendimiento profundo de cómo implementar seguridad perimetral en sus redes.

AUDIENCIA

- Ingenieros de Sistemas, Técnicos de Sistemas, Administradores de Red, Jefes de Sistema o Soporte, Estudiantes, Profesionales de carreras afines o personas con interés en temas informáticos, redes y sistemas.

PRE REQUISITOS

- No tiene prerequisitos previos

OBJETIVOS

Especializándote en ese curso aprenderás a:

- Describir las capacidades de un UTM FortiGate
- Comprender el concepto de las amenazas: virus, phishing, spam, torrents, y los sitios web inapropiados
- Proporcionar Control de acceso a la red basado en el tipo de dispositivo
- Establecer un túnel IPSec VPN entre dos dispositivos FortiGate (según disponibilidad de lab)
- Interpretar las entradas del registro (Logs y filtrado)
- Entender y como hacer un diagnostico (casos) y más

CERTIFICACIÓN DISPONIBLE

- Certificación emitida por COGNOS.

CONTENIDO

1. INTRODUCCIÓN A FORTINET

1.1. INTRODUCCIÓN A FORTIGATE
1.2. INTERFACES DE ADMINISTRACIÓN
1.3. DASHBOARD, GRÁFICAS
1.4. FORTIGUARD Y LICENCIAMIENTO
1.5. RESPALDOS DE CONFIGURACIÓN, NTOP, SETTINGS

2. CONFIGURACIÓN DE RED BÁSICA

2.1. CONFIGURACIÓN DE INTERFACES
2.2. DNS Y SNMP
2.3. USUARIOS Y GRUPOS
2.4. OTRAS OPCIONES

3. RUTEO

3.1. RUTAS ESTÁTICAS
3.2. POLICY ROUTING
3.3. RUTEO DINÁMICO
3.4. TABLA DE RUTEO

4. FIREWALL

4.1. FIREWALL EN FORTIGATE
4.2. OBJETOS DE FIREWALL
4.3. POLÍTICAS DE FIREWALL
4.4. NAT
4.5. TRAFFIC SHAPING

5. UTM

5.1. INTRODUCCIóN Y "PROTECTION PROFILES"
5.2. ANTIVIRUS
5.3. WEBFILTER
5.4. APPLICATION CONTROL
5.5. IPS
5.6. EMAIL FILTER
5.7. DLP
5.8. ENDPOINT CONTROL

6. USUARIOS Y VPN

6.1. USUARIOS Y GRUPOS
6.2. GRUPOS REMOTOS
6.3. IDENTITY BASED POLICY
6.4. VPN IPSEC
6.5. VPN SSL WEB Y PORTAL

7. WIRELESS CONTROLLER

7.1. CREACIÓN DE REDES INALÁMBRICAS (SSID)
7.2. PERFILES DE AP
7.3. MONITOREO

8. LOG Y REPORT Y HA

8.1. LOGUEO LOCAL Y REMOTO
8.2. AVISOS POR E-MAIL
8.3. REPORTES
8.4. ALTA DISPONIBILIDAD

9. CLI Y DIAGNÓSTICO

9.1. INTRODUCIÓN A CLI
9.2. COMANDOS DE DIAGNÓSTICOS
9.3. DEBUG DE PROCESOS

BENEFICIOS

- Al finalizar el curso, el estudiante estara capacitado para definir funciones de Fortigate y las politicas de seguridad en sus redes.