

# Fortinet NSE4

Código: FOR-010

**Propuesta de Valor:** SEGURIDAD INFORMÁTICA

**Duración:** 40 Horas Académicas



Los profesionales de NIVEL 4 (NSE 4) desarrollan el conocimiento necesario para administrar la configuración, el monitoreo y la operación del día a día de los dispositivos FortiGate para soportar las políticas de seguridad de la red corporativa. El programa abarca a Profesionales de IT, partners, empleados y estudiantes. Entrenar en Fortinet es invertir en su seguridad informática actual y futura con la mayor eficiencia costo - beneficio. ¡Convertite en un experto!

## AUDIENCIA

- Cualquier persona que sea responsable de la administración diaria de un dispositivo FortiGate, de su implementación y/o de definir la mejor solución de infraestructura. Se requieren conocimientos previos de Fortinet, preferentemente habiendo completado el curso de Fortinet Seguridad.

## PRE REQUISITOS

- Conocimiento de las siete capas del modelo de Interconexión de Sistemas Abiertos (OSI).
- Conocimientos de firewall en una red IPv4.
- Conocimientos de Fortigate, idealmente habiendo completado el curso de Seguridad Fortigate.

## OBJETIVOS

- Analizar las tablas de ruteo de Fortigate.
- Enrutar paquetes utilizando rutas basadas en políticas y rutas estáticas para implementaciones multirruta, e implementaciones con carga equilibrada.
- Configuración de la SD-WAN para balancear la carga de tráfico a través de múltiples vínculos WAN, en forma efectiva.
- Inspeccionar el tráfico en forma transparente, redireccionando como un conmutador de capa 2.
- Dividir FortiGate en dos o más dispositivos virtuales, cada uno operando como un FortiGate independiente, por medio de Dominios Virtuales VDOM.
- Establecer un túnel VPN IPsec entre dos dispositivos FortiGate.

- Comparar VPNs basadas en políticas (policy-based) contra VPN IPsec (route-based).
- Implementar una "mesh VPN" o una VPN parcialmente redundante.
- Ofrecer accesos Fortinet Single Sign On (FSSO) a los servicios de la red, integrándolos con los servicios de Microsoft Active Directory.

---

## CERTIFICACIÓN DISPONIBLE

- Certificación emitida por COGNOS.

---

## CONTENIDO

### 1. FORTIGATE SECURITY

- 1.1. INTRODUCCIÓN A FORTIGATE Y SECURITY FABRIC
- 1.2. POLÍTICAS DE FIREWALL
- 1.3. TRADUCCIÓN DE DIRECCIONES DE RED (NAT)
- 1.4. AUTENTICACIÓN DE FIREWALL
- 1.5. REGISTRO Y MONITOREO
- 1.6. OPERACIONES DE CERTIFICADO
- 1.7. FILTRADO WEB
- 1.8. CONTROL DE APLICACIONES
- 1.9. ANTIVIRUS
- 1.10. PREVENCIÓN DE INTRUSIONES Y DENEGACIÓN DE SERVICIO
- 1.11. VPN SSL
- 1.12. VPN DE DIAULUP IPSEC
- 1.13. PREVENCIÓN DE FUGAS DE DATOS (DLP)

### 2. FORTIGATE INFRAESTRUCTURA

- 2.1. ENRUTAMIENTO
- 2.2. WAN (SD-WAN) DEFINIDA POR SOFTWARE
- 2.3. DOMINIOS VIRTUALES
- 2.4. CONMUTACIÓN DE CAPA 2
- 2.5. VPN CON IPSEC SITIO A SITIO
- 2.6. SSO FORTINET
- 2.7. ALTA DISPONIBILIDAD
- 2.8. WEB PROXY
- 2.9. DIAGNÓSTICO

---

## BENEFICIOS

- Establecer conocimientos y habilidades en Infraestructura & Seguridad.