Fortinet, seguridad de redes

Curso práctico de 4 días - 28h
Ref.: TIR - Precio 2024: 1 950€ sin IVA

Este curso le enseñará a desplegar la solución de seguridad de Fortinet para proteger su red corporativa. Al finalizarlo, será capaz de instalarla y dominar los elementos esenciales de su configuración, incluidos el filtrado de aplicaciones, las VPN y la alta disponibilidad.

OBJETIVOS PEDAGÓGICOS

Al término de la formación, el alumno podrá:

Describir las características de FortiGate

Instalación y configuración del cortafuegos

Implantar una estrategia de filtrado de redes y aplicaciones

Implementación de una VPN SSL e IPSEC

Implementación de la alta disponibilidad de FortiGate

PROGRAMA

última actualización: 02/2024

1) Introducción

- Tecnologías y funciones de cortafuegos.
- La arquitectura. La familia de productos FORTINET.
- Componentes del aparato.

2) Configuración y administración

- Tareas administrativas.
- Modos CLI/GUI y FortiManager.
- El procedimiento de instalación.
- Familiarizarse con la interfaz.

Trabajo práctico : Instale y configure el cortafuegos.

3) Filtrado de redes y aplicaciones

- Política de control de acceso al cortafuegos. Filtrado de direcciones y puertos.
- Definición de una política de filtrado. Gestión de reglas.
- Filtrado de contenidos y detección de patrones.
- Filtrado de URL. Opciones avanzadas.
- Filtros antispam. Control del protocolo SMTP.
- Archivos adjuntos. Perfiles de protección. Antivirus. Bloqueo por extensión de archivo.

Trabajo práctico : Aplicación de una estrategia de filtrado de redes y aplicaciones.

4) NAT y enrutamiento

- Modos de funcionamiento NAT/Route/Transparent.
- Enrutamiento estático y enrutamiento dinámico.
- ¿Qué política de encaminamiento debe aplicarse?

Trabajo práctico : Configuración de una política de enrutamiento. Autenticación con AD o Radius.

PARTICIPANTES

Técnicos, administradores e ingenieros de sistemas/redes/seguridad.

REQUISITOS PREVIOS

Buenos conocimientos de TCP/IP. Conocimientos básicos de seguridad informática.

COMPETENCIAS DEL FORMADOR

Los expertos que imparten la formación son especialistas en las materias tratadas. Han sido validados por nuestros equipos pedagógicos, tanto en el plano de los conocimientos profesionales como en el de la pedagogía, para cada curso que imparten. Cuentan al menos con entre cinco y diez años de experiencia en su área y ocupan o han ocupado puestos de responsabilidad en empresas.

MODALIDADES DE EVALUACIÓN

El formador evalúa los progresos pedagógicos del participante a lo largo de toda la formación mediante preguntas de opción múltiple, escenificaciones de situaciones, trabajos prácticos, etc.
El participante también completará una prueba de posicionamiento previo y posterior para validar las competencias adquiridas.

MEDIOS PEDAGÓGICOS Y TÉCNICOS

• Los medios pedagógicos y los métodos de enseñanza utilizados son principalmente: ayudas audiovisuales, documentación y soporte de cursos, ejercicios prácticos de aplicación y ejercicios corregidos para los cursillos prácticos, estudios de casos o presentación de casos reales para los seminarios de formación.
• Al final de cada cursillo o seminario, ORSYS facilita a los participantes un cuestionario de evaluación del curso que analizarán luego nuestros equipos pedagógicos.
• Al final de la formación se entrega una hoja de presencia por cada media jornada de presencia, así como un certificado de fin de formación si el alumno ha asistido a la totalidad de la sesión.

MODALIDADES Y PLAZOS DE ACCESO

La inscripción debe estar finalizada 24 horas antes del inicio de la formación.

ACCESIBILIDAD DE LAS PERSONAS CON DISCAPACIDAD

¿Tiene alguna necesidad específica de accesibilidad? Póngase en contacto con la Sra. FOSSE, interlocutora sobre discapacidad, en la siguiente dirección psh-accueil@orsys.fr para estudiar de la mejor forma posible su solicitud y su viabilidad.

5) VLAN y dominios virtuales (VDOM)

- Recordatorio del concepto de VLAN. ¿Cuándo debe utilizarse?
- Administración y supervisión.
- Enrutamiento interVDOM.

Trabajo práctico : Instalación y configuración de VLAN y VDOM.

6) VPN con IPSEC

- Un recordatorio de IPSEC. VPN de sitio a sitio IPSEC.
- Modo interfaz y modo túnel.
- VPN IPSEC cliente-sitio.
- El cliente "FortiClient". Autenticación Xauth.
- Túneles con clave compartida.

Trabajo práctico : Configuración de un túnel IPSEC.

7) VPN con SSL

- Un recordatorio del protocolo SSL.
- Modo túnel y modo portal.
- Elige el modo adecuado.

Trabajo práctico : Configuración del túnel SSL en modo portal y túnel.

8) Alta disponibilidad

- Conceptos de alta disponibilidad.
- Modo activo-pasivo/activo-activo.
- Satisfacer las necesidades de la empresa.

Trabajo práctico : Implantación de la alta disponibilidad activa/pasiva del FGCP.

FECHAS

Contacto