Fortigate Security - Infraestructura

Distintivo de nivel 1 Profesional certificado por Fortinet - Seguridad de redes

Curso práctico de 5 días - 35h
Ref.: FNA - Precio 2024: 2 820€ sin IVA

Este curso de formación sobre seguridad e infraestructura FortiGate le proporcionará todos los conocimientos relativos a la gestión unificada de amenazas (UTM) en una única plataforma. La parte "seguridad" le proporcionará conocimientos prácticos relativos a las reglas generales de gestión y a la protección contra el malware. La parte "infraestructura" le permitirá dominar las funciones de arquitectura avanzada de FortiGate.

PARTICIPANTES

Ingenieros/administradores y técnicos de red y cualquier persona implicada en el diseño de arquitecturas de red y seguridad basadas en hardware FortiGate.

REQUISITOS PREVIOS

Conocimientos básicos de seguridad informática y buenos conocimientos de TCP/IP.

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.

OBJETIVOS PEDAGÓGICOS

Al término de la formación, el alumno podrá:

Despliegue el modo operativo adecuado para su red (proxy, flujo, NGFW, etc.)

Utilice interfaces gráficas y CLI para la administración

Controlar el acceso a las redes configuradas mediante políticas de cortafuegos

Aplicar reenvío de puertos, traducción de direcciones de red (NAT) de origen y NAT de destino.

Autenticar usuarios mediante políticas de cortafuegos

Comprender las funciones de cifrado y los certificados

Descifrar el tráfico seguro SSL/TLS para que pueda ser inspeccionado

Configurar perfiles de seguridad para neutralizar amenazas y abusos

Aplicar técnicas de control de aplicaciones de red

Utilizar protocolos y puertos estándar o no estándar

Lucha contra la piratería informática y los ataques de denegación de servicio (DoS)

Recopilación e interpretación de los elementos recogidos en los periódicos

Identificar las características del tejido de seguridad de Fortinet

Análisis de una tabla de enrutamiento FortiGate

Enrutamiento de paquetes mediante rutas estáticas y basadas en reglas

Despliegue de rutas múltiples con equilibrio de carga

Dividir FortiGate en dos o más dispositivos virtuales

Configuración de dominios virtuales (VDOM)

Comprender los principios fundamentales y las ventajas de utilizar la ZTNA

Ofrezca una VPN SSL para un acceso seguro a su red privada

Establecimiento de un túnel VPN IPsec entre dos dispositivos FortiGate

Implantación de una VPN mallada o parcialmente redundante

Diagnosticar intercambios IKE fallidos

Ofrecer acceso de inicio de sesión único (FSSO) a los servicios de red respaldando el acceso a Microsoft Active Directory (AD).

Implementación de dispositivos FortiGate en un clúster de alta disponibilidad

Mejorar la tolerancia a fallos y ofrecer un alto rendimiento

Despliegue de la interfaz virtual SD-WAN

Implementar una distribución dinámica de flujos basada en el rendimiento medido en las interfaces miembro

MÉTODOS PEDAGÓGICOS

Una mezcla equilibrada de presentaciones, talleres y situaciones reales.

Trabajo práctico individual y en grupo, reflexión colectiva. Los ejercicios prácticos se realizan sobre la versión de FortiOS requerida para la certificación Fortinet.

CERTIFICACIÓN

Este curso está diseñado para los candidatos que deseen realizar el examen Fortinet NSE4 - FortiOS. Es el primer paso en el proceso de certificación NSE 5 - FortiGate Network Security Professional, y permite a los candidatos realizar un examen de acreditación (core), que debe combinarse con una optativa y la realización de un segundo examen, FortiManager (ref. FNB) o FortiAnalyzer (ref.FND).
La superación de ambos exámenes permite la validación del certificado Fortinet NSE5.

PROGRAMA

última actualización: 02/2024

1) Seguridad - Introducción y ajustes iniciales

- Funcionalidad de alto nivel.
- Decisiones iniciales.
- Administración básica.
- Mantenimiento básico.

2) Seguridad - Política de cortafuegos

- Configuración de la política.
- Gestión de políticas.
- Buenas prácticas y resolución de problemas.

3) Seguridad - Traducción de direcciones de red

- Introducción.
- NAT basado en políticas frente a NAT central.
- Buenas prácticas y resolución de problemas.

4) Seguridad - Autenticación de cortafuegos

- Métodos de autenticación del cortafuegos.
- Grupos de usuarios.
- Reglas de cortafuegos con autenticación.

5) Seguridad - Registro y supervisión

- Conocimientos básicos de prensa.
- Registro local o remoto.
- Configuración de registros, búsqueda en registros.
- Protección de los datos de registro.

6) Seguridad - Operaciones con certificados

- Autenticar y proteger datos mediante certificados.
- Inspecciona las cifras.

7) Seguridad - Filtrado web

- Métodos de inspección.
- Conceptos básicos del filtrado web.
- Funciones adicionales de filtrado web basado en proxy.
- Filtrado de vídeo.
- Buenas prácticas y resolución de problemas.

8) Seguridad - Control de aplicaciones

- Fundamentos del control de aplicaciones.
- Configuración del control de aplicaciones.
- Registro y supervisión de eventos de control de aplicaciones.

9) Seguridad - Antivirus

- Fundamentos.
- Modos de análisis.
- Configuración antivirus.

10) Seguridad - Prevención de intrusiones
- El sistema de prevención de intrusiones.
- Denegación de servicio.

11) Seguridad - Tejido de seguridad
- Noción de tejido de seguridad.
- Despliegue.
- Estire el tejido de seguridad.
- Sistema de clasificación de tejidos de seguridad y vista topológica.

12) Infraestructura - Enrutamiento
- Enrutamiento en FortiGate.
- Supervisión de rutas y atributos de rutas.
- Reparto equitativo de la carga de costes.
- Prueba de Reverse Path Forwarding (RPF), para combatir la suplantación de direcciones.
- Sondas de salud de enlaces y conmutación de rutas.
- Diagnóstico.

13) Infraestructura - Dominios virtuales
- Conceptos de VDOM.
- Administradores de VDOM.
- Configuración VDOM.
- Enlaces inter-VOM.
- Buenas prácticas y resolución de problemas.

14) Infraestructura - Fortinet Single Sign-On
- Función y despliegue.
- FSSO con Active Directory.
- Ajustes y solución de problemas.

15) Infraestructura - Acceso a la red de confianza cero (ZTNA)
- Introducción.
- Compare la ZTNA con las VPN IPsec y SSL.

16) Infraestructura - SSL VPN
- Modos de despliegue.
- Configuración.
- Supervisión y resolución de problemas.

17) Infraestructura - VPN IPsec
- Introducción.
- Configuración.
- Reglas de enrutamiento y cortafuegos.
- VPN redundantes, VPN de malla.
- Monitorización, registro.

18) Infraestructura - Alta disponibilidad
- Modos de funcionamiento activo/pasivo frente a activo/activo.
- Sincronización de clústeres HA.
- Conmutación de HA.

19) Infraestructura - SD-WAN
- Motivación, distribución dinámica de flujos.
- Implantación.
- Sondas de rendimiento.

- Reglas SD-WAN.

20) Infraestructura - Diagnóstico
- Información general.
- Depuración de flujos.
- Procesador y memoria.
- Firmware y hardware.

FECHAS

Contacto