SLS LATAM®

cisco Partner

TEMARIO SFWIPF

FUNDAMENTALS OF CISCO FIREWALL THREAT DEFENSE AND INTRUSION PREVENTION v1.0 (SFWIPF)

El curso Fundamentals of Cisco Firewall Threat Defense and Intrusion Prevention (SFWIPF) te enseña a implementar y configurar Cisco Secure Firewall Threat Defense para su despliegue como firewall de Next Generation en el perímetro de internet.

---

40 CLC | Duración 40 horas | 40 CE

¿CÓMO TE BENEFICIARÁ?

Este curso te prepara para la certificación CCNP Security, que requiere aprobar el examen central 350-701 SCOR y un examen de concentración como el 300-710 SNCF.

Aprenderás a implementar, configurar y administrar Cisco Secure Firewall Threat Defense, incluyendo la configuración de políticas, el análisis de amenazas y la gestión con Cisco Secure Firewall Management Center.

¿QUIÉN DEBERÍA INSCRIBIRSE?

Dirigido a ingenieros de seguridad de red y administradores que buscan aprender a implementar, configurar y gestionar Cisco Secure Firewall Threat Defense para proteger redes empresariales contra amenazas.

DETALLES DEL CURSO

Después de tomar este curso, deberías ser capaz de:

- Describir Cisco Secure Firewall Threat Defense.
- Explicar las opciones de implementación de Cisco Secure Firewall Threat Defense.
- Describir las opciones de administración para Cisco Secure Firewall Threat Defense.
- Configurar ajustes iniciales básicos en Cisco Secure Firewall Threat Defense.
- Configurar alta disponibilidad en Cisco Secure Firewall Threat Defense.
- Configurar NAT básico en Cisco Secure Firewall Threat Defense.

DETALLES DEL CURSO

Después de tomar este curso, deberías ser capaz de:

- Explicar las políticas de Cisco Secure Firewall Threat Defense y su impacto en el procesamiento de paquetes.
- Configurar la política de descubrimiento en Cisco Secure Firewall Threat Defense.
- Configurar y explicar reglas de prefiltro y túnel en la política de prefiltro.
- Configurar una política de control de acceso en Cisco Secure Firewall Threat Defense.
- Configurar inteligencia de seguridad en Cisco Secure Firewall Threat Defense.
- Configurar una política de archivos en Cisco Secure Firewall Threat Defense.
- Configurar la política de intrusión en Cisco Secure Firewall Threat Defense.
- Realizar análisis básico de amenazas con Cisco Secure Firewall Management Center.
- Ejecutar tareas básicas de administración del sistema en Cisco Secure Firewall Threat Defense.
- Solucionar problemas básicos de flujo de tráfico en Cisco Secure Firewall Threat Defense.
- Gestionar Cisco Secure Firewall Threat Defense con Cisco Secure Firewall Threat Defense Manager.

CONOCIMIENTOS RECOMENDADOS

La base de conocimientos y habilidades que se espera tengas antes de asistir a esta capacitación son:

- TCP/IP.
- Protocolos básicos de ruteo.
- Conceptos de Firewall, VPN e IPS.

CONTENIDO

- Introducción a Cisco Secure Firewall Threat Defense.
- Descripción de las opciones de implementación de Cisco Secure Firewall Threat Defense.
- Descripción de las opciones de gestión de Cisco Secure Firewall Threat Defense.
- Configuración de los ajustes básicos de red en Cisco Secure Firewall Threat Defense.
- Configuración de alta disponibilidad en Cisco Secure Firewall Threat Defense.
- Configuración de Auto NAT en Cisco Secure Firewall Threat Defense.
- Descripción del procesamiento de paquetes y políticas en Cisco Secure Firewall Threat Defense.
- Configuración de la política de descubrimiento en Cisco Secure Firewall Threat Defense.
- Configuración de la política de prefiltrado en Cisco Secure Firewall Threat Defense.
- Configuración de la política de control de acceso en Cisco Secure Firewall Threat Defense.
- Configuración de inteligencia de seguridad en Cisco Secure Firewall Threat Defense.
- Configuración de la política de archivos en Cisco Secure Firewall Threat Defense.
- Configuración de la política de intrusión en Cisco Secure Firewall Threat Defense.
- Realización de análisis básico de amenazas en Cisco Secure Firewall Management Center.
- Gestión del sistema Cisco Secure Firewall Threat Defense.
- Solución de problemas básicos de flujo de tráfico.
- Cisco Secure Firewall Threat Defense Device Manager.

ESQUEMA DE LABORATORIOS

- Realizar la configuración inicial del dispositivo.
- Configurar alta disponibilidad.
- Configurar traducción de direcciones de red (NAT).
- Configurar descubrimiento de red.
- Configurar políticas de prefiltrado y control de acceso.
- Configurar inteligencia de seguridad.
- Implementar control de archivos y protección avanzada contra malware.
- Configurar Cisco Secure IPS.
- Análisis detallado utilizando el Firewall Management Center.
- Gestionar el sistema Cisco Secure Firewall Threat Defense.
- Fundamentos de resolución de problemas de Secure Firewall.
- Configurar dispositivos gestionados utilizando Cisco Secure Firewall Device Manager.