



ADMINISTRACIÓN DE FIREWALL CISCO **FIREPOWER THREAT DEFENSE**

Impartido por: **Capacitaciones GoCursos Spa**

Modalidad
Presencial/Elearning

Reunión con Relator
Costo 0

Incluye
Diploma y Certificado





Objetivo general

Este curso proporciona a los participantes las habilidades esenciales para administrar y configurar el firewall Cisco Firepower Threat Defense, mejorando así la seguridad de la red. Se enfoca en la implementación de políticas de seguridad efectivas y la gestión de amenazas avanzadas.



Objetivos específicos

- Comprender la arquitectura del firewall Cisco Firepower. Desarrollar habilidades para configurar políticas de seguridad. Aprender a gestionar y monitorear amenazas en tiempo real.



Modalidad

Presentamos todas las modalidades que ofrecemos a nuestros alumnos.



ONLINE

Clases asincrónicas, entregándote la libertad de estudiar en el momento y lugar que tú decidas.



ONLINE EN VIVO

Clases remotas en vivo, donde profesor y alumnos se conectan e interactúan en tiempo real, en una fecha y horario establecido



PRESENCIAL

Asiste físicamente a las clases, en nuestras salas o en las propias dependencias del cliente.

Temario del curso:

Módulo 1: Introducción a Cisco FTD y conceptos de seguridad

Duración: 2 horas

Contenidos:

Introducción al sistema Firepower Threat Defense (FTD)

Arquitectura de Cisco Secure Firewall

Diferencia entre FTD y ASA tradicional

Componentes: FMC (Firepower Management Center) vs. FDM (Device Manager)

Casos de uso típicos de FTD en entornos corporativos

Buenas prácticas de seguridad perimetral

Actividad práctica:

Dinámica grupal: Analizar el diagrama de red de una empresa ficticia y discutir cómo integrar FTD como solución perimetral. Uso de pizarra digital o papelógrafo para presentación.

Módulo 2: Configuración inicial de Cisco FTD y acceso a FDM

Duración: 2 horas

Contenidos:

Registro y licenciamiento del dispositivo FTD

Acceso y navegación en FDM (Firepower Device Manager)

Configuración básica de red (interfaces, rutas, hostname)

Configuración de acceso remoto (HTTPS/SSH)

Gestión de backups y snapshots

Introducción a NAT y zonas de seguridad

Actividad práctica:

Laboratorio: Configurar por primera vez un FTD con FDM en un entorno de laboratorio (virtual o físico), accediendo vía navegador y configurando interfaces.

Módulo 3: Políticas de acceso y reglas de firewall

Duración: 2 horas

Contenidos:

Fundamentos de políticas de acceso

Configuración de reglas de firewall (permitir, denegar, inspeccionar)

Objetos de red y servicios en políticas

Uso de zonas de seguridad en reglas

Análisis del flujo de tráfico y logging

Introducción a políticas de tiempo (time-based rules)

Actividad práctica:

Simulación interactiva: Cada estudiante debe crear un conjunto de reglas de firewall que permitan navegación web segura, pero bloqueen redes sociales.

Módulo 4: Configuración de NAT en Cisco FTD

Duración: 2 horas

Contenidos:

Introducción a NAT (estático, dinámico, PAT)

Políticas de NAT automáticas vs manuales

Traducción basada en objetos

Reglas de NAT según interfaz/zona

Resolución de conflictos entre reglas NAT y ACL

Pruebas de conectividad post-NAT

y mucho más...

Datos del Organismo Capacitador:

Nombre Empresa OTEC:	Capacitaciones GoCursos SPA
Rut:	77919346-2
Giro:	Servicio de Capacitaciones
Dirección	Irrazaval 690 Ñuñoa Santiago de Chile
Cuenta Bancaria	Cuenta Corriente 95466877 Banco Santander
Email:	contacto@gocursos.cl