

CCNA Security



La Certificación CCNA de Seguridad satisface las necesidades de los profesionales de TI que son responsables de la seguridad de la red. Se confirman las habilidades de un técnico para la inserción laboral como, por ejemplo, los especialistas de la Red de Seguridad, Administradores de Seguridad, y de Ingenieros de Apoyo en Seguridad de Redes. Esta certificación valida las habilidades incluida la instalación, resolución de problemas y el control de dispositivos de red para mantener la integridad, confidencialidad y disponibilidad de datos y dispositivos y desarrolla la competencia en las tecnologías de Cisco que utiliza en su estructura de seguridad.

Los estudiantes al completar la formación de Cisco adquirirán una introducción a las tecnologías básicas de seguridad, así como la forma de elaborar las políticas de seguridad y mitigar los riesgos. Las organizaciones de TI que emplean CCNA titulares de Seguridad tendrá el personal de TI que puede desarrollar una infraestructura de seguridad, reconocer las amenazas y las vulnerabilidades a las redes, y mitigar las amenazas a la seguridad.

Este es el curso requiere tener la Certificación CNA / CNAP CCNA

La metodología docente es una combinación de cuatro elementos:

- **Aula-laboratorio** con profesorado altamente cualificado y certificado en la especialidad.
- **Guía de certificación** de gran calidad editada por Cisco Press.
- **Prácticas** reales.

Examen 640-553 IINS: Implementing Cisco IOS Network Security

Describe the security threats facing modern network infrastructures

Describe and list mitigation methods for common network attacks
Describe and list mitigation methods for Worm, Virus, and Trojan Horse attacks
Describe the Cisco Self Defending Network architecture

Secure Cisco routers

Secure Cisco routers using the SDM Security Audit feature
Use the One-Step Lockdown feature in SDM to secure a Cisco router
Secure administrative access to Cisco routers by setting strong encrypted passwords, exec timeout, login failure rate and using IOS login enhancements
Secure administrative access to Cisco routers by configuring multiple privilege levels
Secure administrative access to Cisco routers by configuring role based CLI
Secure the Cisco IOS image and configuration file

Implement AAA on Cisco routers using local router database and external ACS

Explain the functions and importance of AAA
Describe the features of TACACS+ and RADIUS AAA protocols
Configure AAA authentication
Configure AAA authorization
Configure AAA accounting

Mitigate threats to Cisco routers and networks using ACLs

Explain the functionality of standard, extended, and named IP ACLs used by routers to filter packets

Configure and verify IP ACLs to mitigate given threats (filter IP traffic destined for Telnet, SNMP, and DDoS attacks) in a network using CLI

Configure IP ACLs to prevent IP address spoofing using CLI
Discuss the caveats to be considered when building ACLs

Implement secure network management and reporting

Use CLI and SDM to configure SSH on Cisco routers to enable secured management access
Use CLI and SDM to configure Cisco routers to send Syslog messages to a Syslog server

Mitigate common Layer 2 attacks

Describe how to prevent layer 2 attacks by configuring basic Catalyst switch security features

Implement the Cisco IOS firewall feature set using SDM

Describe the operational strengths and weaknesses of the different firewall technologies
Explain stateful firewall operations and the function of the state table
Implement Zone Based Firewall using SDM

Implement the Cisco IOS IPS feature set using SDM

Define network based vs. host based intrusion detection and prevention
Explain IPS technologies, attack responses, and monitoring options
Enable and verify Cisco IOS IPS operations using SDM

Implement site-to-site VPNs on Cisco Routers using SDM

Explain the different methods used in cryptography
Explain IKE protocol functionality and phases
Describe the building blocks of IPSec and the security functions it provides
Configure and verify an IPSec site-to-site VPN with pre-shared key authentication using SDM