



C/ Hernán Ruiz, 6 - 29008 - Málaga
Tlfs.952 21 67 01 – 2 líneas / Fax: 952 22 89 10
e-mail: formacion@cenec.es
web: www.cenecmalaga.es

Fundamentals Network Security

Fundamentos de Network Security enseñara a los estudiantes a diseñar e implementar soluciones de seguridad que reducirán los riesgos de pérdida de datos y vulnerabilidades. Como otros cursos ofertados por Cisco Networking Academy, el foco de este curso combinara trabajos de laboratorios, explicaciones del instructor y estudio e-learning.

El curso dará una introducción de la seguridad en la red y procesos de seguridad sobre la red. Tomando especial énfasis en:

- Diseño y Manejo de políticas de seguridad
- Tecnologías , productos y soluciones de seguridad
- Diseño, instalación, configuración y mantenimiento de Firewall y Router seguros.
- Implementación de AAA usando Routers y Firewalls.
- Implementación de VPN usando Routers y Firewalls.

Este curso prepara a los estudiantes para tomar los exámenes SNP y SNPA para Cisco Firewall Specialist.

Contenidos:

Network Security I

- Module 1: Vulnerabilities, Threats, and Attacks
- Module 2: Security Planning and Policy
- Module 3: Security Devices
- Module 4: Trust and Identity Technology
- Module 5: Cisco Secure Access Control Server
- Module 6: Configure Trust and Identity at Layer 3
- Module 7: Configure Trust and Identity at Layer 2
- Module 8: Configure Filtering on a Router
- Module 9: Configure Filtering on a PIX Security Appliance
- Module 10: Configure Filtering on a Switch

Network Security II

- Module 1: Intrusion Detection and Prevention Technology
- Module 2: Configure Network Intrusion Detection and Prevention
- Module 3: Encryption and VPN Technology
- Module 4: Configure Site-to-Site VPN Using Pre-shared Keys
- Module 5: Configure Site-to-Site VPNs Using Digital Certificates
- Module 6: Configure Remote Access VPN
- Module 7: Secure Network Architecture and Management
- Module 8: PIX Security Appliance Contexts, Failover, and Management

El Sistema Educativo e-Learning

e-Learning es un nuevo y revolucionario paradigma del aprendizaje. Los contenidos de la formación que ha desarrollado Cisco para esta iniciativa están basados en este sistema. Al igual que otros conceptos como **e-Business** o **e-Service**, el e-Learning surge a raíz de aprovechar las posibilidades que ofrece la actual expansión de Internet. Es decir, el e-Learning es una forma de aprender basada en Internet.

Contenidos

Normalmente existen unos contenidos diseñados para que se puedan consultar mediante un navegador. Para su desarrollo se pueden utilizar todas aquellas tecnologías internet / intranet que permitan crear contenidos efectivos, que despierten el interés del alumno, que resulten amenos. Es muy habitual encontrar una gran variedad de elementos como texto, glosarios, imágenes en movimiento, un buen sistema de navegación, etc. Es muy importante que existan mecanismos de evaluación que permitan al alumno conocer su propio progreso y eventualmente, que informe al profesor / tutor sobre el proceso de aprendizaje del alumno.

Interactividad con otros participantes

Fundamentalmente el profesor / tutor y otros alumnos, aunque puede resultar interesante poder entrar en contacto con comunidades virtuales con intereses en temas afines. Esto se suele concretar en la posibilidad de comunicarse mediante e-mail o chats, añadiendo a los contenidos una parte de intercambio humano.

Acceso a información relevante

Un sistema e-Learning puede contar con páginas donde, mediante aportaciones de expertos, tutores u otros alumnos, se pueda complementar lo aprendido con noticias de última hora que permitan estar al día sobre lo aprendido.

Elementos añadidos

El paradigma e-Learning considera incluir en un sistema educativo cualquier elemento que beneficie el proceso formativo. En el caso concreto del "Networking Academies", el aprendizaje mediante el web se complementa con clases presenciales y prácticas en el laboratorio.

Exámenes CNAP-Network Security I

Module 1: Vulnerabilities, Threats, and Attacks	Examen duración 60mn entre 20 y 35 preguntas.
Module 2: Security Planning and Policy	Examen duración 60mn entre 20 y 35 preguntas.
Module 3: Security Devices	Examen duración 60mn entre 20 y 35 preguntas.
Module 4: Trust and Identity Technology	Examen duración 60mn entre 20 y 35 preguntas.
Module 5: Cisco Secure Access Control Server	Examen duración 60mn entre 20 y 35 preguntas.
Module 6: Configure Trust and Identity at Layer 3	Examen duración 60mn entre 20 y 35 preguntas.
Module 7: Configure Trust and Identity at Layer 2	Examen duración 60mn entre 20 y 35 preguntas.
Module 8: Configure Filtering on a Router	Examen duración 60mn entre 20 y 35 preguntas.
Module 9: Configure Filtering on a PIX Security Appliance	Examen duración 60mn entre 20 y 35 preguntas.
Module 10: Configure Filtering on a Switch	Examen duración 60mn entre 20 y 35 preguntas.

Examen final del capítulo 1 al capítulo 10 duración 2 horas entre 60 y 80 preguntas

Examen práctico duración 2 horas

Caso de Estudio durante el curso

Exámenes CNAP-Network Security II

Module 1: Intrusion Detection and Prevention Technology	Examen duración 60mn entre 20 y 35 preguntas.
Module 2: Configure Network Intrusion Detection and Prevention	Examen duración 60mn entre 20 y 35 preguntas.
Module 3: Encryption and VPN Technology	Examen duración 60mn entre 20 y 35 preguntas.
Module 4: Configure Site-to-Site VPN Using Pre-shared Keys	Examen duración 60mn entre 20 y 35 preguntas.
Module 5: Configure Site-to-Site VPNs Using Digital Certificates	Examen duración 60mn entre 20 y 35 preguntas.
Module 6: Configure Remote Access VPN	Examen duración 60mn entre 20 y 35 preguntas.
Module 7: Secure Network Architecture and Management	Examen duración 60mn entre 20 y 35 preguntas.
Module 8: PIX Security Appliance Contexts, Failover, and Management	Examen duración 60mn entre 20 y 35 preguntas.

Examen final del capítulo 1 al capítulo 8 duración 2 horas entre 60 y 80 preguntas

Examen práctico duración 2 horas

Caso de Estudio durante el curso

Preguntas Frecuentes

¿Para qué trabajo me habilita?

Habilita para desarrollar e implantar la seguridad en una red LAN conectada o no a una WAN como Internet.

¿Quiénes pueden acceder?

El desarrollo de la Certificación supone conocimientos previos y el CNAP CCNA o equivalente.

¿Cómo se cursa el curso?

Se cursa presencial con prácticas en routers y pix, con exámenes parciales y finales para evaluar conocimientos.

¿Se cuenta con materiales de estudio?

Cada alumno recibe en su primera clase un User ID y password que le permiten acceder, a través de Internet, a un sistema de administración de contenidos multimedia de última generación. Por medio de este sistema accede a los contenidos por Internet, apuntes y documentación en formato electrónico.

¿Hay exámenes?

FNS está dotado de un esquema de evaluaciones en Internet, con parciales por cada tema y de aprobación obligatoria un examen final práctico y otro teórico.

¿En qué idioma se desarrolla la Certificación?

En Inglés, material de estudio de la plataforma CNAP y exámenes. Las explicaciones del profesor y libro oficial en español.

¿Qué certificación se recibe?

Al finalizar el modulo se entregará el correspondiente certificado de aprobación de Cisco Networking Academy Program avalado por Cisco Systems. La Certificación obtenida es el CISCO CNAP FNS I y II. Es un excelente "puente" entre el CCNA y el CCNP.

**NUESTROS CURSOS SON EN DIAS LABORABLES Y SABADOS MAÑANAS.
FORMACIÓN DE CARÁCTER PRIVADO. INCLUYE CERTIFICACION DE MULTINACIONAL.**