



CCNA Security

Opportunity

The Internet is changing life as we know it – bringing new economic and social opportunities to communities throughout the world, and increasing the global demand for information and communication technology (ICT) skills. Security and risk management skills are among the most highly sought after skills in networking, and demand continues to grow. Organizations around the world are experiencing a shortage of qualified ICT candidates with the specialized knowledge and skills needed to administer devices and applications in a secure infrastructure, recognize network vulnerabilities, and mitigate security threats. In a recently commissioned study conducted by Forrester Consulting on behalf of Cisco, dedicated security roles are expected in 80 percent of the companies studied worldwide within five years.

Solution

The Cisco® Networking Academy® CCNA® Security course provides a next step for individuals who want to enhance their CCNA-level skill set and help meet the growing demand for network security professionals. The curriculum provides an introduction to the core security concepts and skills needed for the installation, troubleshooting, and monitoring of network devices to maintain the integrity, confidentiality, and availability of data and devices.

CCNA Security is a hands-on, career-oriented e-learning solution with an emphasis on practical experience to help students develop specialized security skills, along with critical thinking and

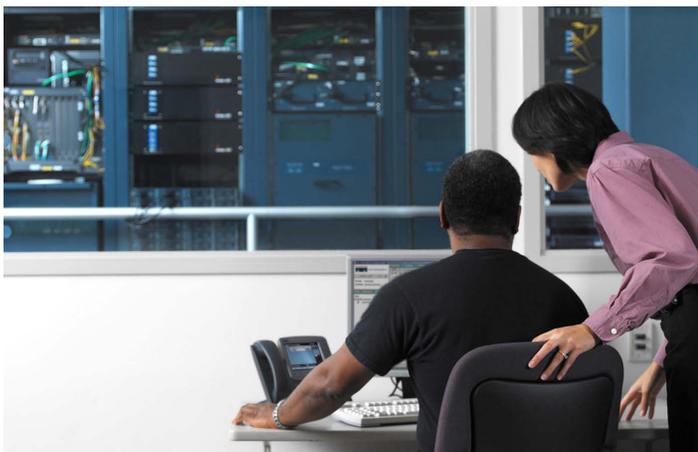
complex problem solving skills. The curriculum helps prepare students for entry-level security career opportunities and the globally recognized Cisco CCNA Security certification, which helps students differentiate themselves in the marketplace with specialist skills to advance their careers.

“80 percent of the companies studied worldwide expect to have a dedicated security role within five years.”
— Forrester Research

Features

CCNA Security provides an in-depth, theoretical, and hands-on introduction to network security, in a logical sequence driven by technologies. CCNA Security includes the following features:

- Students develop an in-depth, theoretical understanding of network security principles as well as the tools and configurations available.
- The courses emphasize the practical application of skills needed to design, implement, and support network security.
- Hands-on labs help students develop critical thinking and complex problem-solving skills.
- Packet Tracer simulation-based learning activities promote the exploration of networking security concepts and allow students to experiment with network behavior and ask “what if” questions.
- Innovative assessments provide immediate feedback to support the evaluation of knowledge and acquired skills.



Who Should Enroll	Prerequisites
<ul style="list-style-type: none"> • College and university-level students seeking career-oriented, entry-level security specialist skills • IT professionals wishing to broaden or add specialized skills to their technology expertise • Current CCNA certification holders who wish to build on their CCNA knowledge base 	<ul style="list-style-type: none"> • CCNA-level networking concepts and skills • Basic PC and Internet navigation skills ❖ Students can acquire the CCNA-level routing and switching skills needed for success in this course by completing CCNA Discovery or CCNA Exploration

1 Modern Network Security Threats
1.2 Viruses, Worms, and Trojan Horses
1.2.4 Mitigating Viruses, Worms, and Trojan Horses

CCNA Security
 Implementing Network Security

In the case of the SQL Slammer worm, malicious traffic normally is blocked by a firewall on the perimeter. However, most infections enter by way of back doors and do not pass through the firewall, therefore, to prevent the spreading of this worm it would be necessary to block this port on all devices throughout the internal network.

In some cases, the port on which the worm is spreading might be critical to business operation. For example, when SQL Slammer was propagating, some organizations could not block UDP port 1434 because it was required to access the SQL Server for legitimate business transactions. In such a situation, alternatives must be considered.

If the network devices using the service on the affected port are known, permitting selective access is an option. For example, if only a small number of clients are using SQL Server, one option is to open UDP port 1434 to critical devices only. Selective access is not guaranteed to solve the problem, but it certainly lowers the probability of infection.

The diagram illustrates a network topology for mitigating SQL Slammer worm. It shows a central Core network with two Layer 3 switches. The Core is connected to two ISPs (ISP A and ISP B) via Network-Enabled Routers. The Core also connects to a Data Center and two Workgroups (Workgroup 1 and Workgroup 2). Red arrows indicate traffic flow from the ISPs through the Core to the workgroups and data center. Red boxes labeled 'ACL Port Block' are placed on the Layer 3 switches to indicate where access control lists are applied to block traffic on specific ports.

1 2 3 4 5

All contents copyright © 2007-2009 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Course Description

CCNA Security aims to develop an in-depth understanding of network security principles as well as the tools and configurations available. The course covers the following concepts:

- Protocol sniffers/analyzers
- TCP/IP and common desktop utilities
- Cisco IOS® Software
- Cisco VPN client
- Packet Tracer
- Web-based resources

Various types of hands-on labs provide practical experience, including procedural and troubleshooting labs, skills integration challenges, and model building. The curriculum also includes Packet Tracer-based skills integration challenges that build throughout the course and lead to an “exam-like” culminating activity in the last chapter.

21st Century Skills

CCNA Security integrates practical skills into the technical curriculum to create a learning experience for success in future educational, entrepreneurial, and occupational endeavors.

In addition to learning the fundamentals of designing, building, and operating secure networks, students also develop problem solving, critical thinking, collaboration, teamwork, negotiation, and entrepreneurship skills which can help them succeed in the 21st century global workplace.

Assessments

Innovative formative and summative assessments are integrated into the CCNA Security curriculum and supported by an advanced online delivery system. Immediate, rich feedback supports instructor and student evaluation of acquired knowledge and skills. Assessments can be as simple as a multiple choice question or as complex as troubleshooting a simulated network.

Packet Tracer

Packet Tracer is a powerful network simulation program developed by Networking Academy that allows students to experiment with network behavior and ask “what if” questions. As an integral part of the CCNA Security curriculum, Packet Tracer provides simulation, visualization, authoring, assessment, and collaboration capabilities and makes teaching and learning complex security technology concepts easier.

Packet Tracer supplements physical equipment by allowing students to create a network with an almost unlimited number of devices; encouraging open practice, discovery, and troubleshooting. The simulation-based learning environment helps students develop 21st century skills such as decision making, creative and critical thinking, and problem solving.

Course Outline	
Chapter	Goals
1. Modern Network Security Threats	Explain network threats, mitigation techniques, and the basics of securing a network
2. Securing Network Devices	Secure administrative access on Cisco routers
3. Authentication, Authorization and Accounting	Secure administrative access with AAA
4. Implementing Firewall Technologies	Implement firewall technologies to secure the network perimeter
5. Implementing Intrusion Prevention	Configure IPS to mitigate attacks on the network
6. Securing the Local Area Network	Describe LAN security considerations and implement endpoint and Layer 2 security features
7. Cryptography	Describe methods for implementing data confidentiality and integrity
8. Implementing Virtual Private Networks	Implement secure virtual private networks
9. Putting It All Together	Given the security needs of an enterprise, create and implement a comprehensive security policy

Upon completion of the CCNA Security course, students will be able to perform the following tasks:

- Describe the security threats facing modern network infrastructures
- Secure network device access
- Implement AAA on network devices
- Mitigate threats to networks using ACLs
- Implement secure network management and reporting
- Mitigate common Layer 2 attacks
- Implement the Cisco IOS firewall feature set
- Implement the Cisco IOS IPS feature set
- Implement site-to-site IPSec VPNs
- Administer effective security policies

Learning Environment

CCNA Security can be delivered as an independent curriculum or integrated into a broader course of study, such as technology or continuing education programs. The curriculum can be offered in an in-person or a blended distance learning (BDL) environment.

All hands-on labs in the course can be completed on actual physical equipment or in conjunction with the NDG NETLAB solution, which provides remote access to equipment over the Internet.

CCNA Security Certification

CCNA Security helps prepare students for the Implementing Cisco IOS® Network Security (IINS) certification exam (640-553) leading to the Cisco CCNA Security certification. With a CCNA Security certification, an individual demonstrates the skills required to develop a security infrastructure, recognize network threats and vulnerabilities, and mitigate security threats.

Careers

CCNA Security supports students who plan to start a career, build a career, or switch focus in an IT networking career to security technologies. The curriculum emphasizes practical experience to help students develop the skills needed for job roles such as network security specialists, security administrators, and network security support engineers. The CCNA Security curriculum is designed to meet the needs of today's IT professionals.

Cisco Networking Academy

In partnership with schools and organizations around the world, the Cisco Networking Academy program delivers a comprehensive learning experience to help students develop information and communication technology (ICT) skills for entry-level career opportunities, continuing education, and globally recognized career certifications. The curricula also help students build 21st

CCNA Security encourages students to explore networking concepts using tools such as Packet Tracer. Packet Tracer is a powerful network simulation tool developed by Cisco that allows students to experiment with network behavior and develop critical thinking, collaboration, and problem solving skills, while gaining practical knowledge.

century skills such as collaboration and problem solving by encouraging practical application of knowledge through hands-on activities and network simulations.

Networking Academy teaches ICT skills to students from virtually every socioeconomic background and region of the world. Students gain the skills needed to pursue networking careers in a variety of industries such as technology, healthcare, financial services, fashion, entertainment, and more. Students also gain access to a global support group, career developments tools, and social networking resources to help them become architects of the human network.

For More Information

Cisco Networking Academy
www.cisco.com/go/netacad

Course Catalog
www.cisco.com/go/netacadcourses

Locate an academy
www.cisco.com/go/academylocator

Certifications
www.cisco.com/go/certifications



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

©2011 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

C78-546106-00 04/11