CCNA Security

http://cisco.novsu.ru/courses/ccna-security/

CCNA Security helps students develop the skills needed to succeed in IT-related degree programs and prepare for the CCNA Security certification. It provides a theoretically rich, hands-on introduction to network security, in a logical sequence driven by technologies.

The goals of CCNA Security are as follows:

- Provide an in-depth, theoretical understanding of network security
- Provide students with the knowledge and skills necessary to design and support network security
- Provide an experience-oriented course that employs industry-relevant instructional approaches to prepare students for associate-level jobs in the industry
- Enable students to have significant hands-on interaction with IT equipment to prepare them for certification exams and career opportunities

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

Chapter Outline

Chapter/Section	Goals/Objectives
Chapter 1. Modern Network Security Threats	**Explain network threats, mitigation techniques, and the basics of securing a network**
1.1 Fundamental Principles of a Secure Network	Describe the fundamental principles of securing a network
1.2 Worms, Viruses and Trojan Horses	Describe the characteristics of worms, viruses, and Trojan horses and mitigation methods
1.3 Attack Methodologies	Describe common network attack methodologies and mitigation techniques such as Reconnaissance, Access, Denial of Service,

	and DDoS
Chapter 2. Securing Network Devices	**Secure administrative access on Cisco routers**
2.1 Securing Device Access and Files	Configure secure administrative access and router resiliency
2.2 Privilege Levels and Role-Based CLI	Configure command authorization using privilege levels and role-based CLI
2.3 Monitoring Devices	Configure network devices for monitoring
2.4 Using Automated Features	Secure IOS-based routers using automated features
Chapter 3. Authentication, Authorization and Accounting	**Secure administrative access with AAA**
3.1 Purpose of AAA	Describe the purpose of AAA and the various implementation techniques
3.2 Configuring Local AAA	Implementing AAA using the local database
3.3 Configure Server-Based AAA	Implementing AAA using TACACS+ and RADIUS protocols
Chapter 4. Implementing Firewall Technologies	**Implement firewall technologies to secure the network perimeter**
4.1 Access Control Lists	Implement ACLs
4.2 Firewall Technologies	Describe the purpose and operation of firewall technologies
4.3 Context-Based Access Control	Implement CBAC
4.4 Zone-Based Policy Firewall	Implement Zone-based policy Firewall using SDM and CLI
Chapter 5. Implementing Intrusion Prevention	**Configure IPS to mitigate attacks on the network**
5.1 IPS Technologies	Describe the purpose and operation of network-based and host-based Intrusion Prevention Systems
5.2 Implementing IPS	Implement Cisco IOS IPS operations using SDM and CLI
Chapter 6. Securing the Local Area Network	Describe LAN security considerations and implement endpoint and Layer 2 security features
6.1 Endpoint Security Considerations	Describe endpoint vulnerabilities and protection methods
6.2 Layer 2 Security Considerations	Describe basic Catalyst switch vulnerabilities such as VLAN attacks, STP manipulation, CAM table overflow attacks, and MAC address spoofing attacks
6.3 Wireless, VoIP and SAN Security Considerations	Describe the fundamentals of Wireless, VoIP and SANs, and the associated security considerations
6.4 Configuring Switch Security	Configure and verify switch security features, including port security and storm control

6.5 SPAN and RSPAN	Describe Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN)
Chapter 7. Cryptography	**Describe methods for implementing data confidentiality and integrity**
7.1 Cryptographic Services	Describe how different types of encryption, hashes, and digital signatures work together to provide confidentiality, integrity, and non-repudiation
7.2 Hashes and Digital Signatures and authentication	Describe the mechanisms to ensure data integrity
7.3 Symmetric and Asymmetric Encryption	Describe the mechanisms used to ensure data confidentiality
Chapter 8. Implementing Virtual Private Networks	**Implement secure virtual private networks**
8.1 VPNs	Describe the purpose and operation of VPN types
8.2 IPSec VPN Components and Operation	Describe the components and operations of IPSec VPNs
8.3 Implementing Site-to-Site IPSec VPNs	Configure and verify a site-to-site IPSec VPN with pre-shared key authentication using SDM and CLI
8.4 Implementing a Remote Access VPN	Configure and verify a remote access VPN
8.5 Implementing SSL VPNs	Configure and verify SSL VPNs
Chapter 9. Managing a Secure Network	**Given the security needs of an enterprise, create and implement a comprehensive security policy**
9.1 Secure Network Lifecycle	Describe the secure network lifecycle
9.2 Self-Defending Network	Describe the components of a self-defending network and business continuity plans
9.3 Building a Comprehensive Security Policy	Establish a comprehensive security policy to meet the security needs of a given enterprise
Chapter 10. Implementing the Cisco Adaptive Security Appliance (ASA)	**Implement firewall technologies using the ASA to secure the network perimeter**
10.1 Introduction to the ASA	Describe the ASA as an advanced stateful firewall
10.2 ASA Firewall Configuration	Implement an ASA firewall configuration
10.3 ASA VPN Configuration	Implement remote-access VPNs on an ASA