529 Hahn Ave. Suite 101 ♦ Glendale CA 91203-1052 ♦ Tel 818.550.0770 ♦ Fax 818.550.8293 ♦ www.brandcollege.edu

Cisco Certified Security Professional (CCNP Security)

Program Summary

This instructor-led program with a combination of lecture and hands-on laboratory exercises covers advanced topics and concepts related to securing Cisco networks. This course covers a wide array of security topics including: Cisco IOS firewall implementation; PIX firewall technology and features; VPN concepts and implementation; IPSec; implementation and design of intrusion detection systems; Cisco's SAFE implementation; AAA; protocol monitoring and management and much more. The goal of this course is to give the student the tools and knowledge necessary to secure and manage complex network infrastructures – protecting data and productivity, as well as, reducing costs. These are advanced courses providing the skills and knowledge necessary to pass the Cisco certification exams necessary to become a Cisco Certified Network Professional (CCNP) Security.

- Certification program
- 288 Contact Hours, 18 Credit Hours, 36 Weeks

TERM 1

Course No.	Course Name	Quarter Credit Hours	Clock Hours
CCS100	Security I	3	48
CCS110	Security II	3	48
	Total	**6**	**96**

TERM 2

Course No.	Course Name	Quarter Credit Hours	Clock Hours
CCS120	Security III	3	48
CCS130	Security IV	3	48
	Total	**6**	**96**

TERM 3

Course No.	Course Name	Quarter Credit Hours	Clock Hours
CCS140	Security V	6	96
	Total	**6**	**96**

Prerequisites

Candidates wishing to enter this course should have completed the Cisco Certified Network Professional program, the Cisco Certified Network Associate program or have commensurate experience in with Cisco routers and network infrastructure implementation.

Type of Document Received Upon Graduation

Upon successful completion of all program requirements, each student will be awarded a Certificate of Completion.

Certification Tests
All certification exams are scored on a pass/fail basis. Depending on the specific exam, a correct response to 75% - 80% of the questions will be required to achieve a passing score. Students are encouraged to take exams immediately following completion of the corresponding course.

Career Development
Students who successfully complete this program will be prepared for midlevel to advanced level professional opportunities in the IT field with emphasis on network security including installation, configuration and maintenance security components supported in a Local Area Network (LAN) and Wide Area Network (WAN) infrastructure. Although titles may vary by hiring organizations, students with these credentials are qualified to meet the requirements of positions such as Network Security Engineer, Network Security Support Specialist, Network Security Administrator, Sr. Network Security Engineer or similar designations.

This program also aligns with the following career opportunities classified by US Department of Labor under the Standard Occupational Classification (SOC) system.

- 15-1122 Information Security Analysts
- 25-1021 Computer Science Teacher, Postsecondary

Recommended Next Course
Candidates wishing to further their education are recommended to consider the CCIE program as the next logical step towards becoming an expert IT professional.

CCSP Program Details

COURSE CCS100

Title: Implementing Cisco Network Security (IINS)
Exam: 210-260

Course Description

This instructor-led program with a combination of lecture and hands-on laboratory exercises is associated with the CCNA Security certification. This exam tests a candidate's knowledge of securing Cisco routers and switches and their associated networks. It leads to validated skills for installation, troubleshooting and monitoring of network devices to maintain integrity, confidentiality and availability of data and devices and develops competency in the technologies that Cisco uses in its security infrastructure.

Course Objectives

This course will cover the following subjects:

- Common Security Principals
- Common Security Treats
- Cryptography Concepts
- Describe Network Topologies
- Secure Management
- AAA Concepts
- 802.1X Authentication
- BYOD
- VPN Concepts
- Remote Access VPN
- Site to Site VPN
- Security on Cisco Routers
- Securing Routing Protocols
- Securing the Control Plane
- Common Layer to Attacks
- Mitigation Procedures
- VLAN security
- Describe Operational Strengths and weaknesses of the Different Firewall Technologies
- Compare Stateful vs. Stateless Firewalls
- Implement NAT on Cisco ASA 9.x
- Implement Zone-Based Firewall
- Firewall Features on the Cisco Adaptive Security Appliance 9.x
- Describe IPS Deployment Considerations
- Describe IPS Technologies
- Describe Mitigation Technology for Email-Based Treats
- Describe Mitigation Technology for Web-Based Treats
- Describe Mitigation Technology for Endpoint Treats

COURSE CCS110

Title: Implementing Cisco Secure Access Solutions (SISAS)
Exam: 300-208

Course Description

This instructor-led program with a combination of lecture and hands-on laboratory exercises is one of the exams associated with the CCNP Security certification. This course will cover the components and architecture of secure access, by utilizing 802.1X and Cisco TrustSec. It includes knowledge of Cisco Identity Services Engine (ISE) architecture, solution, and components as an overall network threat mitigation and endpoint control solutions. It also includes the fundamental concepts of bring your own device (BYOD) using posture and profiling services of ISE. Candidates can prepare for this exam by taking the Implementing Cisco Secure Access Solutions (SISAS) course.

Course Objectives

This course will cover the following subjects:

- Implement Device Administration
- Describe Identity Management
- Implement Wired/Wireless 802.1X
- Implement MAB
- Implement network authorization enforcement
- Implement Central Web Authentication
- Implement Profiling
- Implement Guest Services
- Implement Posture Services
- Implement BYOD Access
- Describe TrustSec Architecture
- Troubleshoot Identity Management Solutions
- Design Highly Secure Wireless Solution with ISE
- Device Administration
- Identity Management
- Profiling
- Guest Services
- Posturing Services
- BYOD Access

COURSE CCS120

Title: Implementing Cisco Edge Network Security Solutions (SENSS)
Exam: 300-206

Course Description

This instructor-led program with a combination of lecture and hands-on laboratory exercises is one of the exams associated with the CCNP Security. The Implementing Cisco Edge Network Security Course includes the knowledge of a network security engineer to configure and implement security on Cisco network perimeter edge devices such as a Cisco switch, Cisco router, and Cisco ASA firewall. This course focuses on the technologies used to strengthen security of a network perimeter such as Network Address Translation (NAT), ASA policy and application inspect, and a zone-based firewall on Cisco routers.

Course Objectives

This course will cover the following subjects:

- Implement Firewall
- Implement Layer 2 Security
- Configure Device Hardening Per Best Practices
- Implement SSHv2, HTTPS, and SNMPv3 Access on the Network Devices
- Implement RBAC on the ASA/IOS using CLI and ASDM
- Describe Cisco Prime Infrastructure
- Describe Cisco Security Manager
- Implement Device Mangers
- Configure NetFlow Exporter on Cisco Routers, Switches, and ASA
- Implement SNMPv3
- Implement Logging on Cisco Routers, Swtiches, and ASA Using Cisco Best Practices
- Implement NTP with Authentication on Cisco Routers, Switches, and ASA
- Describe CDP, DNS, SCP, SFTP, and DHCP
- Analyze Packet Tracer on the Fire Using CLI/ASDM
- Configure and Analyze Packet Capture Using CLI/ASDM
- Analyze Syslog Events Generated From ASA
- Design a Firewall Solution
- Layer 2 Security Solutions
- Describe Security Operations Management Architectures
- Describe Data Center Security Components and Considerations
- Describe Common IPv6 Security Considerations

COURSE CCS130

Title: Implementing Cisco Secure Mobility Solutions (SIMOS)
Exam: 300-209

Course Description

This instructor-led program with a combination of lecture and hands-on laboratory exercises is associated with the Implementing Cisco Secure Mobility Solutions (SIMOS) tests a network security engineer on the variety of Virtual Private Network (VPN) solutions that Cisco has available on the Cisco ASA firewall and Cisco IOS software platforms. This course provides the knowledge necessary to properly implement highly secure remote communications through VPN technology, such as remote access SSL VPN and site-to-site VPN (DMVPN, FlexVPN). Candidates can prepare for this exam by taking the Implementing Cisco Secure Mobility Solutions (SIMOS) course.

Course Objectives

This course will cover the following subjects:

- Site-to-Site VPNs on Routers and Firewalls
- Describe GETVPN
- Implement IPsec
- Implement DMVPN
- Implement FlexVPN
- Implement Remote Access VPNs
- Implement AnyConnect IKEv2 VPNs on ASA and Routers
- Implement AnyConnect SSLVPN on ASA and Routers
- Implement Clientless SSLVPN on ASA and Routers
- Implement FLEX VPN on Routers
- Troubleshoot VPN Using ASDM & CLI
- Troubleshoot IPsec
- Troubleshoot DMVPN
- Troubleshoot FlexVPN
- Troubleshoot AnyConnect IKEv2 and SSL VPNs on ASA and Routers
- Troubleshoot Clientless SSLVPN on ASA and Routers
- Design Site-to-Site VPN Solutions
- Identify Functional Components of GETVPN, FlexVPN, DMVPN, and IPsec
- VPN Technology Consideration Based on Functional Requirements
- High Availability Consideration
- Identify VPN Technology Based on Configuration Output
- Design Remote Access VPN Solution
- Clientless SSL Browser and Client Considerations / Requirements
- Identify Split Tunneling Requirements
- Describe Encryption, Hashing, and Next generation Encryption (NGE)
- Describe PKI Components Protection Methods
- Compare and Contrast SSL, DTLS, and TLS

COURSE CCS140

Title: Implementing Cisco Threat Control Solutions (SITCS)
Exam: 300-207

Course Description

This instructor-led program with a combination of lecture and hands-on laboratory exercises is associated with the Cisco Certified Network Professional Security certification. The Implementing Cisco Threat Control Solutions (SITCS) provides a network security engineer on advanced firewall architecture and configuration with the Cisco next-generation firewall, utilizing access and identity policies. This Course covers integration of Intrusion Prevention System (IPS) and context-aware firewall components, as well as Web (Cloud) and Email Security solutions. Candidates can prepare for this exam by taking the Implementing Cisco Threat Control Solutions (SITCS) course.

Course Objectives

This course will cover the following subjects:

- Cisco ASA 5500-X NGFW Security Services
- Describe Features and Functionality
- Implement Web Usage Control
- Implement AVS
- Cisco Cloud Web Security
- Implement IOS and ASA Connectors
- Implement AnyConnect Web Security Module
- Implement Anti-Malware
- Cisco WSA
- Implement Data Security
- Describe Decryption Policies
- Describe Traffic Redirection and Capture Methods
- Cisco ESA
- Implement email Encryption
- Implement Anti-Spam Policies
- Implement Virus Outbreak Filter
- Network IPS
- Implement Traffic Redirection and Capture Methods
- Implement Network IPS Deployment Modes
- Describe Signatures Enginees
- Configure Device Hardening Per Best practices
- Content Security
- Configure IME and IP Logging for IPS
- Content Security
- Monitor Cisco Security IntelliShield
- Design IPS Solution
- Design Web Security Solution
- Design Email Security Solution
- Design Application Security Solution