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

Cisco Certified Security Professional (CCSP)

Program Summary

This program 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
CSP100	Security I	3	48
CSP110	Security II	3	48
	Total	**6**	**96**

TERM 2

Course No.	Course Name	Quarter Credit Hours	Clock Hours
CSP120	Security III	3	48
CSP130	Security IV	3	48
	Total	**6**	**96**

TERM 3

Course No.	Course Name	Quarter Credit Hours	Clock Hours
CSP140	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 CSP100

Title: Implementing Cisco IOS Network Security
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:

Security Concepts

- Common security principles
- Describe confidentiality, integrity, availability (CIA)
- Describe SIEM technology
- Identify common security terms
- Identify common network security zones
- Common security threats
- Identify common network attacks
- Describe social engineering
- Identify malware
- Classify the vectors of data loss/exfiltration
- Cryptography concepts
- Describe key exchange
- Describe hash algorithm
- Compare and contrast symmetric and asymmetric encryption
- Describe digital signatures, certificates, and PKI
- Describe network topologies
- Campus area network (CAN)
- Cloud, wide area network (WAN)
- Data center
- Small office/home office (SOHO)
- Network security for a virtual environment

Secure Access

- Secure management
- Compare in-band and out-of band
- Configure secure network management
- Configure and verify secure access through SNMP v3 using an ACL
- Configure and verify security for NTP
- Use SCP for file transfer
- AAA concepts
- Describe RADIUS and TACACS+ technologies
- Configure administrative access on a Cisco router using TACACS+
- Verify connectivity on a Cisco router to a TACACS+ server
- Explain the integration of Active Directory with AAA

- Describe authentication and authorization using ACS and ISE
- 802.1X authentication
- Identify the functions 802.1X components
- BYOD
- Describe the BYOD architecture framework
- Describe the function of mobile device management (MDM)

VPN
- VPN concepts
- Describe IPsec protocols and delivery modes (IKE, ESP, AH, tunnel mode, transport mode)
- Describe hairpinning, split tunneling, always-on, NAT traversal
- Remote access VPN
- Implement basic clientless SSL VPN using ASDM
- Verify clientless connection
- Implement basic AnyConnect SSL VPN using ASDM
- Verify AnyConnect connection
- Identify endpoint posture assessment
- Site-to-site VPN
- Implement an IPsec site-to-site VPN with pre-shared key authentication on Cisco routers and ASA firewalls
- Verify an IPsec site-to-site VPN

Secure Routing and Switching
- Security on Cisco routers
- Configure multiple privilege levels
- Configure Cisco IOS role-based CLI access
- Implement Cisco IOS resilient configuration
- Securing routing protocols
- Implement routing update authentication on OSPF
- Securing the control plane
- Explain the function of control plane policing
- Common Layer 2 attacks
- Describe STP attacks
- Describe ARP spoofing
- Describe MAC spoofing
- Describe CAM table (MAC address table) overflows
- Describe CDP/LLDP reconnaissance
- Describe VLAN hopping
- Describe DHCP spoofing
- Mitigation procedures
- Implement DHCP snooping
- Implement Dynamic ARP Inspection
- Implement port security
- Describe BPDU guard, root guard, loop guard
- Verify mitigation procedures
- VLAN security
- Describe the security implications of a PVLAN
- Describe the security implications of a native VLAN

Cisco Firewall Technologies
- Describe operational strengths and weaknesses of the different firewall technologies
- a Proxy firewalls
- Application firewall
- Personal firewall

- Compare stateful vs. stateless firewalls
- Operations
- Function of the state table
- Implement NAT on Cisco ASA 9.x
- Static
- Dynamic
- PAT
- Policy NAT
- Verify NAT operations
- Implement zone-based firewall
- Zone to zone
- Self Zone
- Firewall features on the Cisco Adaptive Security Appliance (ASA) 9.x
- Configure ASA access management
- Configure security access policies
- Configure Cisco ASA interface security levels
- Configure default Cisco Modular Policy Framework (MPF)
- Describe modes of deployment (routed firewall, transparent firewall)
- Describe methods of implementing high availability
- Describe security contexts
- Describe firewall services

IPS

- Describe IPS deployment considerations
- Network-based IPS vs. host-based IPS
- Modes of deployment (inline, promiscuous - SPAN, tap)
- Placement (positioning of the IPS within the network)
- False positives, false negatives, true positives, true negatives
- Describe IPS technologies
- Rules/signatures
- Detection/signature engines
- Trigger actions/responses (drop, reset, block, alert, monitor/log, shun)
- Blacklist (static and dynamic)

Content and Endpoint Security

- Describe mitigation technology for email-based threats
- SPAM filtering, anti-malware filtering, DLP, blacklisting, email encryption
- Describe mitigation technology for web-based threats
- Local and cloud-based web proxies
- Blacklisting, URL filtering, malware scanning, URL categorization, web application filtering, TLS/SSL decryption
- Describe mitigation technology for endpoint threats
- Anti-virus/anti-malware
- Personal firewall/HIPS
- Hardware/software encryption of local data

COURSE CSP110

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:

- Threat Mitigation through Identity Services
- Identity Services
- 802.1X and EAP
- Configure 802.1X Components
- ISE Fundamentals
- Describe Cisco ISE Features and configure the fundamentals
- Cisco ISE with PKI
- Cisco ISE Authentication
- Cisco ISE with External Authentication
- Advance Access Control
- Certificate Based User Authentication
- Authorization
- Cisco TrustSec
- Web Authentication and Guest Access
- Web Authentication
- Guest Access Services
- Endpoint
- Posture
- Profiler
- BYOD
- Troubleshooting Network Access Control
- Troubleshooting ISE
- View More

COURSE CSP120

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:

- Secure Design Principles
- Course Overview
- Network Security Zoning
- Cisco Module Network Security Architecture
- Cisco SecureX Architecture
- Cisco TrustSec Solution
- Deploying Network Infrastructure Protection
- Introducing Cisco Network Infrastructure Protection
- Deploying Cisco IOS Control Plane Security Controls
- Deploying Cisco IOS Management Plane Security Controls
- Deploying Cisco ASA Management Plane Security Controls
- Deploying Cisco Traffic Telemetry Methods
- Deploying Cisco IOS Layer 2 and Layer 3 Data Plane Security Controls
- Deploying NAT on Cisco IOS and Cisco ASA
- Introducing Network Address Translation
- Deploying Cisco ASA Network Address Translation
- Deploying Cisco IOS Software Network Address Translation
- Deploying Threat Controls on Cisco ASA
- Introducing Cisco Firewall Threat Controls
- Deploying Basic Cisco ASA Access Policies
- Deploying Advanced Cisco ASA Application Inspection Policies
- Deploying Cisco ASA Botnet Traffic Filtering
- Deploying Cisco ASA Identity Based Firewall
- Deploying Threat Controls on Cisco IOS Software
- Deploying Basic Cisco IOS Software with Basic Zone-Based Firewall Access Policies
- Deploying Advanced Cisco IOS Software ZBFW with Application Inspection Policies

COURSE CSP130

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:

- Fundamentals of VPN Technologies and Cryptography
- The Role of VPNs in Network Security
- VPNs and Cryptography
- Deploying Secure Site-to-Site Connectivity Solutions
- Introducing Cisco Secure Site-to-Site Connectivity Solutions
- Deploying Point-to-Point IPsec VPNs on the Cisco ASA
- Deploying Cisco IOS VTI-Based Point-to-Point IPsec VPNs
- Deploying Cisco IOS DMVPNs
- Deploying Cisco IOS Site-to-Site FlexVPN Solutions
- Introducing Cisco IOS Site-to-Site FlexVPN Solutions
- Deploying Point-to-Point IPsec VPNs Using Cisco IOS FlexVPN
- Deploying Hub-and-Spoke IPsec VPNs Using Cisco IOS FlexVPN
- Deploying Spoke-to-Spoke IPsec VPNs Using Cisco IOS FlexVPN
- Deploying Basic Cisco Clientless SSL VPN
- Clientless SSL VPN Overview
- Deploying Basic Cisco Clientless SSL VPN on Cisco ASA
- Deploying Application Access in Cisco ASA Clientless SSL VPN
- Deploying Advanced Authentication and Authorization in Clientless SSL VPN
- Deploying Cisco AnyConnect VPNs
- Deploying Basic Cisco AnyConnect SSL VPN on Cisco ASA
- Deploying Advanced Cisco AnyConnect SSL VPN on Cisco ASA
- Deploying Advanced Authentication and Authorization in Cisco AnyConnect VPNs
- Deploying Cisco AnyConnect IPsec/IKEv2 VPNs
- Deploying Endpoint Security and Dynamic Access Policies
- Implementing Host Scan
- Implementing DAP for SSL VPNs

COURSE CSP140

Title: Implementing Cisco Threat Control Solutions (SITCS)
Exam: 300-210

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 Web Security Appliance
- Cisco Web Security Appliance (WSA) Solutions
- Integrating the Cisco Web Security Appliance
- Configuring Cisco Web Security Appliance Identities and User Authentication Controls
- Configuring Cisco Web Security Appliance Acceptable Use Control
- Configuring Cisco Web Security Appliance Anti-Malware Controls
- Configuring Cisco Web Security Appliance Decryption
- Configuring Cisco Web Security Appliance Data Security Controls
- Cisco Cloud Web Security
- Cisco Cloud Web Security Solutions
- Configuring Cisco Cloud Web Security Connectors
- Web Filtering Policy in Cisco ScanCenter
- Cisco Email Security Appliance
- Cisco Email Security Solutions
- Cisco Email Security Appliance Basic Setup Components
- Configuring Cisco Email Security Appliance Basic Incoming and Outgoing Mail Policies
- Advanced Malware Protection for Endpoints
- AMP for Endpoints Overview and Architecture
- Customizing Detection and AMP Policy
- IOCs and IOC Scanning
- Deploying AMP Connectors
- AMP Analysis Tools
- Cisco FirePOWER Next-Generation IPS
- Cisco FireSIGHT System
- Configuring and Managing Cisco FirePOWER Devices
- Implementing an Access Control Policy
- Discovery Technology
- Configuring File-Type and Network Malware Detection
- Managing SSL Traffic with Cisco FireSIGHT
- IPS Policy and Configuration Concepts
- Network Analysis Policy
- Creating Reports
- Correlation Rules and Policies
- Basic Rule Syntax and Usage
- Cisco ASA FirePOWER Services
- Installing Cisco ASA 5500-X Series FirePOWER Services (SFR)