



Dear Candidate,

We would like to take this opportunity to thank you for inquiring about our training services here at Brand College. This package has been compiled to provide the information you will need to choose the training program that will be most beneficial for you.

In this package, you will find information on:

- Our organization and its philosophy
- Training programs we offer
- Details on the training program of your inquiry

Every journey begins with a first step. You have already taken this first step by expressing interest in pursuing an educational program. We would welcome the opportunity to be your partner on this journey and help you complete your journey successfully.

Brand College was founded in direct response to the overwhelming demand for qualified computer professionals in today's information age. Armed with extensive background in information technology consulting and training, we are committed to providing students with high quality education that is relevant for today's rapidly changing IT environment. Our team is comprised of certified engineers and trainers who, as a group, have accumulated more than fifty years of practical experience in the field of information technology. Our goal is to maximize each student's educational experience by ensuring that entry-level students are not overwhelmed while more experienced students remain challenged.

Brand College currently offers several certification programs including:

- **CompTIA A+** PC Hardware Technician
- **CompTIA Linux+** Linux Certified Professional
- **MCITP** Microsoft Certified IT Professional
- **CCNA** Cisco Certified Network Associate
- **CCNA Voice** Cisco Certified Network Associate Voice
- **CCNP** Cisco Certified Network Professional
- **CCSP** Cisco Certified Security Professional
- **CCVP** Cisco Certified Voice Professional
- **CNTE** Certified Network Technologies Expert
- **CDNS** Certified Desktop and Network Specialist
- **CLWS** Certified LAN and WAN Specialist
- **CMNS** Certified Multi-Platform Network Specialist
- **CCNE** Cisco Certified Network Expert

Once again, thank you for your inquiry and we look forward to hearing from you in the very near future. Should you have any questions, please do not hesitate to contact our Admissions department by e-mail at [info@brandcollege.us](mailto:info@brandcollege.us) or by phone at (818) 550-0770.

Sincerely,

Brand College

### Cisco Certified Security Professional (CCSP)

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 (five exams) necessary to become a Cisco Certified Security Professional (CCSP).

- 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
<b>Total</b>		<b>6</b>	<b>96</b>

#### TERM 2

Course No.	Course Name	Quarter Credit Hours	Clock Hours
CSP120	Security III	3	48
CSP130	Security IV	3	48
<b>Total</b>		<b>6</b>	<b>96</b>

#### TERM 3

Course No.	Course Name	Quarter Credit Hours	Clock Hours
CSP140	Security V	6	96
<b>Total</b>		<b>6</b>	<b>96</b>

### 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.

### 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: 640-553

- Describe and list mitigation methods for common network attacks
- Describe and list mitigation methods for Worm, Virus, and Trojan Horse attacks
- Describe the Cisco Self Defending Network architecture
- Secure Cisco routers using the SDM Security Audit feature
- Use the One-Step Lockdown feature in SDM to secure a Cisco router
- Secure administrative access to Cisco routers by setting strong encrypted passwords, exec timeout, login failure rate and using IOS login enhancements
- Secure administrative access to Cisco routers by configuring multiple privilege levels
- Secure administrative access to Cisco routers by configuring role based CLI
- Secure the Cisco IOS image and configuration file
- Explain the functions and importance of AAA
- Describe the features of TACACS+ and RADIUS AAA protocols
- Configure AAA authentication
- Configure AAA authorization
- Configure AAA accounting
- Explain the functionality of standard, extended, and named IP ACLs used by routers to filter packets
- Configure and verify IP ACLs to mitigate given threats (filter IP traffic destined for Telnet, SNMP, and DDoS attacks) in a network using CLI
- Configure IP ACLs to prevent IP address spoofing using CLI
- Discuss the caveats to be considered when building ACLs
- Use CLI and SDM to configure SSH on Cisco routers to enable secured management access
- Use CLI and SDM to configure Cisco routers to send Syslog messages to a Syslog server
- Describe how to prevent layer 2 attacks by configuring basic Catalyst switch security features
- Describe the operational strengths and weaknesses of the different firewall technologies
- Explain stateful firewall operations and the function of the state table
- Implement Zone Based Firewall using SDM
- Define network based vs. host based intrusion detection and prevention
- Explain IPS technologies, attack responses, and monitoring options
- Enable and verify Cisco IOS IPS operations using SDM
- Explain the different methods used in cryptography
- Explain IKE protocol functionality and phases
- Describe the building blocks of IPSec and the security functions it provides
- Configure and verify an IPSec site-to-site VPN with pre-shared key authentication using SDM

### COURSE CSP110

Title: Securing Networks with Cisco Routers & Switches (SNRS)

Exam: 642-503

- Utilize Cisco IOS commands to mitigate Layer 2 attacks
- Implement Cisco Identity-Based Networking Services on Cisco Catalyst Switches
- Implement Identity Management using ACS as the Authentication Server
- Identify and describe the advanced capabilities of the IOS firewall feature set
- Configure IOS Firewall to dynamically mitigate identified threats to the network
- Verify and troubleshoot IOS Firewall configuration and operation.
- Configure authentication proxy to apply security policies on a per-user basis

- Verify and troubleshoot authentication proxy configuration and operation
- Configure IOS zone-based Firewalls
- Troubleshoot Zone-based Firewalls
- Configure APPFW application Firewalls
- Configure Granular Protocol Inspection
- Identify and describe the advanced capabilities of the IOS-IPS feature
- Configure the IPS features to identify threats and dynamically block them from entering the network
- Verify and troubleshoot IPS operation
- Describe IPSec features and functionality
- Configure secure connectivity for site-to-site IPSec VPN using pre-shared keys
- Describe GRE features and functionality
- Configure secure connectivity for site-to-site VPN using certificate authorities
- Describe DMVPN features and functionality
- Configure secure connectivity for site-to-site VPN using DMVPN
- Verify and troubleshoot secure site-to-site connectivity operations
- Implement Clientless IOS SSL VPN
- Verify Clientless IOS SSL VPNs
- Configure Easy VPN server with pre-shared keys
- Configure administrative access to the CSACS server
- Configure CSACS system settings
- Configure AAA clients on the CSACS
- Configure users, groups and access rights
- Configure shared profile components in CSACS
- Configure network access profiles in CSACS
- Configure NADS to enable AAA to use a Radius Server
- Verify and troubleshoot AAA operation
- Describe NFP features and functionality
- Secure the management plane using Cisco IOS security features
- Secure the data plane using Cisco IOS security features
- Secure the control plane using Cisco IOS security features

## COURSE CSP120

Title: Securing Networks with ASA Foundation

Exam: 642-524

- Explain the functions of the three types of firewalls used to secure today's computer networks.
- Describe the technology and features of Cisco security appliances.
- Given diagrams of networks protected by Cisco Adaptive Security Appliances (ASAs) and Cisco PIX Security Appliances, explain how each appliance protects network devices from attacks and why each is an appropriate choice for the example network.
- Prepare the security appliance for configuration via the Cisco Adaptive Security Device Manager (ASDM), and launch and navigate ASDM.
- Use ASDM and the CLI to perform essential security appliance configuration.
- Use ASDM to configure dynamic and static address translations in the security appliance.
- Use ASDM to configure switching and routing on the security appliance.
- Use ASDM to configure access control lists, filter malicious active codes, and filter URLs to meet the requirements of the security policy.
- Use the packet tracer for troubleshooting.
- Use ASDM to configure object groups that meet the requirements of the security policy.
- Use ASDM to configure AAA as needed to meet the requirements of the security policy.
- Use ASDM to configure a modular policy that supports the security policy.

- Use ASDM to configure protocol inspection to meet the requirements of the security policy.
- Use ASDM and the CLI to configure threat detection to meet the requirements of the security policy.
- Use ASDM to configure the security appliance to support a site-to-site VPN that meets the requirements of the security policy.
- Use ASDM to configure the security appliance to provide secure connectivity using remote access VPNs.
- Configure the security appliance to run in transparent firewall mode as needed to meet the requirements of the security policy.
- Enable, configure, and manage multiple contexts as needed to meet the requirements of the security policy.
- Select and configure the type of failover that best suits the network topology.
- Monitor and manage an installed security appliance.

## COURSE CSP130

Title: Implementing Cisco Intrusion Prevention System

Exam: 642-533

- List sensor requirements for inline operations
- Explain the difference between inline and promiscuous mode sensor operations
- Explain how Cisco IPS protects network devices from attacks (Describe signatures, alerts, and actions)
- Explain the evasive techniques used by hackers and how Cisco IPS defeats those techniques
- Describe the considerations necessary for selection, placement, and deployment of a network intrusion prevention system
- Explain the Cisco IPS signature features
- Explain AIP-SSM functionalities
- Use the CLI to initialize the sensor
- Configure user accounts and explain the different user roles
- Configure management access to the sensor appliance
- Explain how allowed hosts are used and how they are configured
- Describe sensor interfaces, interface pairs, VLAN-pairs, and VLAN-groups
- Use the Cisco IDM to configure sensor interfaces (enable, create pairs, assign to virtual sensors)
- Describe and configure software bypass
- Describe sensor communications with external management and monitoring systems
- Launch, navigate, and use the Cisco IDM to manage and monitor the sensor
- Describe the various CLI configuration modes and sub modes and navigate between them
- List the tasks for installing and configuring the IDSM-2 and AIP-SSM
- Plan the mitigation of specific network vulnerabilities and exploits
- Describe sensor tuning
- Explain IP fragment and TCP stream reassembly options
- Explain how IP logging should be used and how it is configured
- Explain the use of Event Variables
- Describe signature engines and their functionality
- Determine which response actions need to be configured for a given scenario
- Describe the purpose of the Meta Event Generator
- Explain Target Value Ratings and how they are used
- Determine the need for Event Action Rules in a given scenario
- Explain event Risk Ratings and how they are used
- Use the IDM to tune the sensor to work optimally in the network
- Use the IDM to tune signatures to provide maximum protection for a network
- Given a scenario, use the IDM to create custom signature to meet the requirements
- Configure response actions for a signature
- Configure the sensor to take response actions based on a risk rating

- Use the Cisco IDM to create a Meta signature and disable alert production for the component signatures
- Configure Event Action Filters
- Configure Target Value Ratings
- Configure general settings for Event Action Rules
- Configure Event Variables
- Use the sensor application policy enforcement feature
- Configure passive OS fingerprinting (POSFP)
- Explain the External Product Interface, its benefits, and specifications
- Configure a virtual sensor
- Configure anomaly detection
- Use IDM/CLI to monitor advanced features such as POSFP and AD
- Move software images/upgrades and configuration files via HTTP, HTTPS, SCP, and FTP
- Apply the appropriate system image to the sensor
- Perform sensor password recovery
- Explain sensor licensing and how to install a license
- Describe service pack and signature update file names and how to install them

## COURSE CSP140

Title: Implementing Cisco security Monitoring, Analysis, and Respond System

Exam: 642-544

- Identify the components, features and functions of the Cisco Security MARS product
- Describe the process of installing the Cisco Security MARS appliance
- Add Cisco reporting devices into the Cisco Security MARS appliance
- Add non-Cisco reporting devices into the Cisco Security MARS appliance
- Investigate events that the Cisco Security MARS appliance collects from configured security devices
- Configure the Cisco Security MARS appliance to send alerts
- Create and view a long-duration query on the Cisco Security MARS appliance
- Configure rules to detect interesting patterns of network activity and other anomalous network behavior
- Use the management features in the Cisco Security MARS appliance to assign event, addressing, service, and user information
- Configure the Cisco Security MARS appliance hardware maintenance activities
- Utilize the Global Controller to manage multiple Cisco Security MARS appliances