

Cisco Certified Security Professional Passport

Our CCSP passport includes the core courses and electives required for CCSP Certification.

- **£4,600 to £5,130 depending on elective for four CCSP courses**
- **Training over a 12 month period**

Cisco Certified Security Professional (CCSP®) validates advanced knowledge and skills required to secure and manage Cisco network infrastructures to protect productivity, mitigate threats, and reduce costs.

The CCSP curriculum emphasizes Cisco Router IOS (ISR) and Catalyst Switch security features, Adaptive Security Appliance (ASA), secure VPN connectivity, Intrusion Prevention Systems (IPS), Cisco Security Agent (CSA), Security Enterprise and Device Management, Network Admission Control (NAC) as well as techniques to optimize these technologies in a single, integrated network security solution.

CCSP Pre-requisites: Valid **CCNA** and **IINS** (CCNA Security)

CCSP Core Exams: 642-503 SNRS
642-524 SNAF
642-533 IPS

CCSP Electives (One required) 642-591 CANAC
642-545 MARS
642-515 SNAA

Passing the above set of exams will achieve CCSP status in addition to which delegates can achieve the following individual certifications.

Specialisation: **Cisco IOS Security Specialist**
Course (exam): Securing Networks with Cisco Routers and Switches (642--503 SNRS)

Specialisation: **Cisco ASA Specialist**
Course (exam): Securing Networks with ASA fundamentals (642-524 SNAF) *and*
Securing Networks with ASA advanced (642-515 SNAA)

Specialisation: **Cisco IPS Specialist**
Course (exam): Implementing Cisco Intrusion Prevention System (642-533 IPS)

Specialisation: **Cisco Network Admission Control Specialist**
Course (exam): Implementing NAC Appliance - Cisco Clean Access (642-591 CANAC)

Course Title: Implementing Cisco IOS Network Security (IINS)
Duration: 5 days

This course focuses on the necessity of a comprehensive security policy and how it affects the posture of the network. Delegates will be able to perform basic tasks to secure a small branch type office network using Cisco IOS security features available through web-based GUIs (Cisco Router and Security Device Manager (SDM) and the command-line interface (CLI) on Cisco routers and switches.

Certification

This course prepares delegates for the **640-553 IINS** (Implementing Cisco IOS Network Security) exam and is a pre-requisite for the Cisco Certified Security Professional.

Objectives

After completing this course the delegate will be able to:

- Develop a comprehensive network security policy to counter threats against information security.
- Configure routers on the network perimeter with Cisco IOS Software security features.
- Configure a Cisco IOS zone-based firewall to perform basic security operations on a network.
- Configure site-to-site VPNs using Cisco IOS features.
- Configure IPS on Cisco network routers.
- Configure LAN devices to control access, resist attacks, shield other network devices and systems, and protect the integrity and confidentiality of network traffic.

Pre-Requisites

- Cisco Certified Networking Associate (CCNA)
- Working knowledge of the Windows operating system

Content

- Introduction to Network Security Principles
- Perimeter Security
- Network Security Using Cisco IOS Firewalls
- Site-to-Site VPNs
- Network Security Using Cisco IOS IPS
- LAN, SAN, Voice, and Endpoint Security Overview

Course Title: **Securing Networks with Cisco Routers and Switches (SNRS)**
Duration: **5 days**

Certification

This course forms a part of the CCSP and completes course material for exam **642-503 SNRS**

Objectives

After completing this course the delegate will be able to:

- Implement Layer 2 security features
- Implement the Cisco Trust and Identity Management model to control network access
- Implement command line Network Foundation Protection to protect infrastructure devices
- Implement command line Network Foundation Protection to protect infrastructure devices
- Implement secure IPsec VPNs and GRE tunnels using Cisco routers
- Install, configure, and troubleshoot Cisco IOS Firewall features, including CBAC, Cisco IOS Firewall authentication proxy, and Cisco IOS IPS on a Cisco router
- Secure tunnels using generic routing encapsulation (GRE) and IP Security (IPsec) technology
- Basic switch access security
- The Cisco Trust and Identity Management model to control network access Command Line (CLI) Cisco Network Foundation Protection (NFP)

Pre-Requisites

- Cisco Certified Networking Associate (CCNA) and CCNA Security (IINS)
- Securing Network Devices (SND)
- Basic knowledge of Windows operating system

Content

Aimed at providing the knowledge and skills needed to secure Cisco IOS router and switch networks, the course has been updated for Cisco IOS Release 12.4(6)T.

- Module 1 Layer 2 Security
- Module 2 Trust and Identity
- Module 3 Cisco Network Foundation Protection
- Module 4 Secured Connectivity
- Module 5 Adaptive Threat Defense

Course Title: **Securing Networks with ASA Foundation (SNAF)**
Duration: **5 days**

Securing Networks with ASA Fundamentals (SNAF) v1.0 is an update to Securing Networks with PIX and ASA (SNPA) v5.0 and configurations are performed via ASDM rather than the CLI in this new course. Some of the advanced content will be in a new elective, Securing Networks with ASA Advanced (SNAA).

Certification

This course forms a part of the CCSP and completes course material for exam **642-524 SNAF**

Objectives

After completing this course the delegate will be able to:

- Installing an IPS sensor appliance in the Network and initialise it
- Use IDM to configure built-in signatures to meet the requirements of a given security policy
- Describe the functions of signature engines and their parameters and will use IDM to tune and create signatures
- IDM will be used to tune a sensor to work optimally in the network and will use the Monitoring Centre for Security and Cisco Threat Response
- Install both the NM-CIDS in a router and initialise it
- Install and recover the sensor software image and perform service pack and signature updates

Pre-Requisites

- Cisco Certified Networking Associate (CCNA) and CCNA Security (IINS)
- Familiarity with the networking and security terms and concepts
- Experience in configuring Cisco IOS software

Content

The SNAF course is a five-day, leader-led, lab-intensive course. The course takes a task-oriented approach to teaching the skills to configure, operate, and manage Cisco Adaptive Security Appliance product family.

- Module 1 Cisco Security Appliances
- Module 2 Getting Started
- Module 3 Controlling Network Access
- Module 4 Service Policy Rules
- Module 5 Virtual Private Networks

Course Title: Implementing Cisco Intrusion Prevention System (IPS)
Duration: 4 days

Certification

This course forms a part of the CCSP and completes course material for exam **642-533 IPS**

Objectives

After completing this course the delegate will be able to:

- Installing an IPS sensor appliance in the Network and initialise it
- Use IDM to configure built-in signatures to meet the requirements of a given security policy
- Describe the functions of signature engines and their parameters and will use IDM to tune and create signatures
- IDM will be used to tune a sensor to work optimally in the network and will use the Monitoring Centre for Security and Cisco Threat Response
- Install both the NM-CIDS in a router and initialise it
- Install and recover the sensor software image and perform service pack and signature updates

Pre-Requisites

- Cisco Certified Networking Associate (CCNA) and CCNA Security (IINS)
- Familiarity with the networking and security terms and concepts
- Experience in configuring Cisco IOS software

Content

- Course Introduction
- Security Fundamentals
- Intrusion Prevention Overview
- Getting Started with the IDS Command Line Interface
- Using IDM Sensor Configuration
- Cisco Intrusion Detection System Alarms and Signatures
- Signature Engines
- Signature Configuration
- Sensor Tuning
- Alarm Monitoring and Management
- Blocking Configuration
- Cisco Intrusion Detection System Network Module
- Intrusion Detection System Module Configuration
- Capturing Network Traffic for Intrusion Detection Systems
- Sensor Maintenance
- Verifying System Configuration



Course Title: Implementing NAC Appliance - Cisco Clean Access (CANAC)
Duration: 3 days

The Perfigo CleanMachines solution is a "shrink-wrapped" network admission control solution that recognizes users, their devices and roles; evaluates the security posture of the endpoint and scans for vulnerabilities; and enforces policy in the network. In particular, prior to allowing users onto the network, the Perfigo CleanMachine solution allows administrators to authenticate, authorize, interrogate and remediate users and their machines enforcing policy based access control on the network.

Certification

This course forms a part of the CCSP and completes course material for exam **642-591 CANAC**

Objectives

After completing this course the delegate will be able to:

- Given client network security requirements, explain how a NAC Appliance (Cisco Clean Access) deployment scenario will meet or exceed network security requirements
- Configure the common elements of a NAC Appliance (Cisco Clean Access) solution
- Configure the NAC Appliance (Cisco Clean Access) in-band and out-of-band implementation options
- Implement a highly available NAC Appliance (Cisco Clean Access) solution to mitigate network threats and facilitate network access for those users that meet corporate security requirements
- Maintain a highly available NAC Appliance (Cisco Clean Access) deployment in medium and enterprise network environments

Pre-Requisites

- Cisco Certified Networking Associate (CCNA) and CCNA Security (IINS)
- SNRS or working knowledge of digital certificates
- BCSI or working knowledge of HSRP.

Content

- Course Introduction
- The NAC Appliance (Cisco Clean Access) Solution
- Configuring Common NAC Appliance (Cisco Clean Access) Elements
- NAC Appliance (Cisco Clean Access) Implementation
- NAC Appliance (Cisco Clean Access) Implementation Options
- NAC Appliance (Cisco Clean Access) Monitoring and Administration

Course Title: Implementing Cisco Security, Monitoring, Analysis and Response System (MARS)
Duration: 4 days

Certification

This course is a part of the CCSP and completes course material for the exam **642-545 MARS**

Objectives

After completing this course the delegate will be able to:

- Describe the MARS solution, features and functions in context to the issues of security incidents and security information in an enterprise network.
- Cover the basic physical installation process.
- Add Cisco security and network devices into MARS appliance.
- Add Non-Cisco security and network devices into MARS appliance.
- Configure security devices to generate interesting events that constitute an attack scenario and have MARS collect the interesting events for incident investigation.
- Discuss attack mitigation and false positive confirmation in context to MARS appliance.
- Configure appliance to perform Incident Investigation and attack mitigation.
- Explain how to create, view and save a long-duration query and reports on the MARS appliance.
- Configure the MARS appliance to send an alert.
- Describe and configure rules that detect interesting patterns of network activity.
- Use management features in the MARS appliance to assign event, addressing, service, and user information.
- Configure hardware maintenance chores like viewing audit trail, data archiving, hot swapping hard drives, upgrading software on MARS appliance.
- Provide overview of MARS Global Controller.
- Provide overview of Log Parser Templates.

Pre-Requisites

- Cisco Certified Networking Associate (CCNA) and CCNA Security (IINS)
- Fundamental Knowledge of Implementing Network Security

Content

- MARS Introduction and Task Flow / Provide overview of MARS technology and STM Task Flow Overview.
- Lab 1-1 Accessing MARS 20 appliance.
- Configuring MARS, configuring administration tasks in the MARS system using User Interface.
- Lab 2-1 Adding Cisco Reporting Devices into MARS
- Lab 2-2 Adding non-Cisco Reporting Devices into MARS
- MARS Incident Investigation Configure MARS for incident investigation, create query and send alerts.
- Lab 3-1 Generating Summary Reports
- Lab 3-2 Configure appliance to perform Incident Investigation and attack mitigation.
- Lab 3-3 Creating Queries and Reports.
- MARS Rules and Management Use MARS User Interface to configure rules, management and system maintenance features.
- Lab 4-1 Distributed Threat Mitigation Lab
- Lab 4-2 Create a Custom Parser
- MARS Global Controller, Provide overview of MARS Global Controller



Course Title: Securing Networks with ASA Advanced (SNAA)
Duration: 5 days

Certification

This course forms a part of the CCSP and completes course material for exam **642-515 (SNAA)**

Pre-requisites

SNAF - Securing Networks with ASA Fundamentals

Objectives

This Cisco course develops knowledge and skills on configuring, maintaining, and operating Cisco ASA 5500 Series Adaptive Security. SNAA progress's from the SNAF covering advanced topics of Adaptive Security. We have added depth to the existing Cisco-developed hands-on labs for SNAA. Our advanced hands-on labs, delivered in an enhanced topology designed to simulate a typical production network, guide you through exercises such as managing digital certificates for IPsec and SSL VPNs, deep packet inspection, and using the 5505 in the SOHO environment.

Labs utilize ASA 5520 security appliances, though this course and lab content is applicable across the ASA and PIX families of security appliances, since the command syntax is generally the same. This course covers the features and syntax of Cisco Security Appliance Software v8.0.

Content

1. Advanced ASA NAT

- Applying NAT 0 and Policy NAT

2. Advanced Protocol Handling

- Applying the Cisco Modular Policy Framework
- Handling Advanced Protocol

3. Dynamic Routing and Switching

- Switching with VLANs
- Routing with Dynamic Protocols

4. IPsec VPNs

- Understanding IPsec and Digital Certificates
- Implementing Site-to-Site VPNs with Digital Certificates
- Configuring the Cisco VPN Client
- Implementing Remote Access VPNs with Digital Certificates
- Configuring Advanced Remote Access Features and Policy
- Configuring the ASA 5505 as an Easy VPN Hardware Client
- IPsec VPNs and QoS

5. SSL VPNs

- SSL VPN Technology Overview
- Configuring Clientless SSL VPNs
- Configuring Full Network Access SSL VPNs
- Cisco Secure Desktop
- Securing the Desktop with CSD and DAP

6. Security Services Modules

- Examining the SSMs
- CSC-SSM: Getting Started
- AIP-SSM: Getting Started