CCNP Security

Implementing Cisco Secure Access Solutions (SISAS) 1.0

Course Objectives

Upon completing this course, the learner will be able to meet these overall objectives:

- Understand Cisco Identity Services Engine architecture and access control capabilities.
- Understand 802.1X architecture, implementation and operation.
- Understand commonly implemented Extensible Authentication Protocols (EAP).
- Implement Public-Key Infrastructure with ISE.
- Understand the implement Internal and External authentication databases.
- Implement MAC Authentication Bypass.
- Implement identity based authorization policies.
- Understand Cisco TrustSec features.
- Implement Web Authentication and Guest Access.
- Implement ISE Posture service.
- Implement ISE Profiling.
- Understand Bring Your Own Device (BYOD) with ISE.
- Troubleshoot ISE .

Course Outline

- Course Introduction
- Lab Guide
- Threat Mitigation through Identity Services
- Cisco ISE Fundamentals
- Advance Access Control
- Web Authentication and Guest Access
- Endpoint Access Control
- Troubleshooting Network Access Control

Implementing Cisco Edge Network Security Solutions (SENSS) 1.0

Course Objectives

- Understanding and implementing Cisco modular Network Security Architectures such as SecureX and TrustSec.
- Deploy Cisco Infrastructure management and control plane security controls.
- Configuring Cisco layer 2 and layer 3 data plane security controls.
- Implement and maintain Cisco ASA Network Address Translations (NAT).
- Implement and maintain Cisco IOS Software Network Address Translations (NAT).
- Designing and deploying Cisco Threat Defense solutions on a Cisco ASA utilizing access policy and application and identity based inspection.
- Implementing Botnet Traffic Filters.
- Deploying Cisco IOS Zone-Based Policy Firewalls (ZBFW).
- Configure and verify Cisco IOS ZBFW Application Inspection Policy.

Course Outline

- Course Introduction
- Cisco Secure Design Principles
- Deploying Cisco Network Infrastructure Protection Solutions
- Deploying NAT on Cisco IOS and Cisco Adaptive Security Appliance (ASA) Firewalls
- Deploying Threat Controls on Cisco ASA Firewalls
- Deploying Threat Controls on Cisco IOS Software
- Lab Guide

Implementing Cisco Secure Mobility Solutions (SIMOS) 1.0

Course Objectives

Upon completing this course, the learner will be able to meet these overall objectives:

- Describe the various VPN technologies and deployments as well as the cryptographic algorithms and protocols that provide VPN security.
- Implement and maintain Cisco site-to-site VPN solutions.
- Implement and maintain Cisco FlexVPN in point-to-point, hub-and-spoke, and spoke-to-spoke IPsec VPNs.
- Implement and maintain Cisco clientless SSL VPNs.
- Implement and maintain Cisco AnyConnect SSL and IPsec VPNs.
- Implement and maintain endpoint security and dynamic access policies (DAP).

Course Outline

- Course Introduction
- Fundamentals of VPN Technologies and Cryptography
- Deploying Secure Site-to-Site Connectivity Solutions
- Deploying Cisco IOS Site-to-Site FlexVPN Solutions
- Deploying Clientless SSL VPN -Deploying AnyConnect VPN for Remote Access
- Deploying Endpoint Security and Dynamic Access Policies & #61550; Lab Guide

Implementing Cisco Threat Control Solutions (SITCS) 1.5

Course Content

This course provides network professional with the knowledge to implement Cisco FirePOWER NGIPS (Next-Generation Intrusion Prevention System) and Cisco AMP (Advanced Malware Protection), as well as Web Security, Email Security and Cloud Web Security. You will gain hands-on experience configuring various advance Cisco security solutions for mitigating outside threats and securing traffic traversing the firewall.

Course Outline

- Module 1: Network Security
- Module 2: Network Threat Defense
- Module 3: Cisco FirePOWER Next-Generation IPS (NGIPS)
- Module 4: Security Architectures
- Module 5: Troubleshooting, Monitoring and Reporting Tools