CCNP Security Overview

Cisco Certified Network Professional Security (CCNP Security) certification course is aligned for job role of the Cisco Network Security Engineer responsible for Security in Networking devices, Routers, appliances, and Switches, along with supporting, deploying, choosing, and troubleshooting Firewalls, VPNS, and IDS/IPS solutions for their networking environments. This CCNP Security certification acknowledges your skills and knowledge with security solutions.

About the training

- **Study Material:-** Live lectures Videos, Online Instructor-led Training, Online Lab Workbook, and Remote Virtual Lab access.
- **Duration:-** 3 Months

Requirements

Aspirants are recommended to have atleast one certification of CCNA Security or CCSP or CCNA plus Securing Cisco Network Devices (SND) exam pass (retired in November 2008) or 2 to 4 years of experience.

What you will learn

- Secure access and identity management
- Identity management architectures
- Threat Defense Architectures
- Threat defense
- Reporting, troubleshooting, and monitoring tools
- Cisco secured CLI management and security devices GUIs
- Management services on Cisco devices
- Reporting, troubleshooting, and monitoring tools
- Security components and considerations
- Secure communications
- Content security
- Network threat defense
- Cisco FirePOWER Next-Generation IPS (NGIPS)
- Security architectures

About Instructor

The trainer of this course has 6+ years of industrial experience and is expert in technology. The trainer is also verified by UniNets itself. He has delivered vast and complex project on the same around the globe.

Course content

Required Exam (SCOR 350 – 701)

- Describing Information Security Concepts*
  - Information Security Overview
  - Assets, Vulnerabilities, and Countermeasures
  - Managing Risk
  - Vulnerability Assessment
  - Exploring Common Vulnerability Scoring System (CVSS)
- Describing Common TCP/IP Attacks*
  - Legacy TCP/IP Vulnerabilities
  - IP Vulnerabilities
  - Internet Control Message Protocol (ICMP) Vulnerabilities
  - TCP Vulnerabilities
  - User Datagram Protocol (UDP) Vulnerabilities
  - Attack Surface and Attack Vectors
  - Reconnaissance Attacks
  - Access Attacks
  - Man-in-the-Middle Attacks
  - Denial of Service and Distributed Denial of Service Attacks
  - Reflection and Amplification Attacks
  - Spoofing Attacks
  - Dynamic Host Configuration Protocol (DHCP) Attacks
- Describing Common Network Application Attacks*
  - Password Attacks
  - Domain Name System (DNS)-Based Attacks
  - DNS Tunneling
  - Web-Based Attacks
  - HTTP 302 Cushioning
  - Command Injections
  - SQL Injections
  - Cross-Site Scripting and Request Forgery
  - Email-Based Attacks
- Describing Common Endpoint Attacks*
  - Buffer Overflow
  - Malware
  - Reconnaissance Attack
  - Gaining Access and Control
  - Gaining Access via Social Engineering

- Gaining Access via Web-Based Attacks
- Exploit Kits and Rootkits
- Privilege Escalation
- Post-Exploitation Phase
- Angler Exploit Kit

- Describing Network Security Technologies
  - Defense-in-Depth Strategy
  - Defending Across the Attack Continuum
  - Network Segmentation and Virtualization Overview
  - Stateful Firewall Overview
  - Security Intelligence Overview
  - Threat Information Standardization
  - Network-Based Malware Protection Overview
  - Intrusion Prevention System (IPS) Overview
  - Next Generation Firewall Overview
  - Email Content Security Overview
  - Web Content Security Overview
  - Threat Analytic Systems Overview
  - DNS Security Overview
  - Authentication, Authorization, and Accounting Overview
  - Identity and Access Management Overview
  - Virtual Private Network Technology Overview
  - Network Security Device Form Factors Overview
- Deploying Cisco ASA Firewall
  - Cisco ASA Deployment Types
  - Cisco ASA Interface Security Levels
  - Cisco ASA Objects and Object Groups
  - Network Address Translation
  - Cisco ASA Interface Access Control Lists (ACLs)
  - Cisco ASA Global ACLs
  - Cisco ASA Advanced Access Policies
  - Cisco ASA High Availability Overview
- Deploying Cisco Firepower Next-Generation Firewall
  - Cisco Firepower NGFW Deployments
  - Cisco Firepower NGFW Packet Processing and Policies
  - Cisco Firepower NGFW Objects
  - Cisco Firepower NGFW Network Address Translation (NAT)
  - Cisco Firepower NGFW Prefilter Policies
  - Cisco Firepower NGFW Access Control Policies
  - Cisco Firepower NGFW Security Intelligence

- Cisco Firepower NGFW Discovery Policies
- Cisco Firepower NGFW IPS Policies
- Cisco Firepower NGFW Malware and File Policies

- Deploying Email Content Security
  - Cisco Email Content Security Overview
  - Simple Mail Transfer Protocol (SMTP) Overview
  - Email Pipeline Overview
  - Public and Private Listeners
  - Host Access Table Overview
  - Recipient Access Table Overview
  - Mail Policies Overview
  - Protection Against Spam and Graymail
  - Anti-virus and Anti-malware Protection
  - Outbreak Filters
  - Content Filters
  - Data Loss Prevention
  - Email Encryption
- Deploying Web Content Security
  - Cisco Web Security Appliance (WSA) Overview
  - Deployment Options
  - Network Users Authentication
  - Secure HTTP (HTTPS) Traffic Decryption
  - Access Policies and Identification Profiles
  - Acceptable Use Controls Settings
  - Anti-Malware Protection
- Deploying Cisco Umbrella*
  - Cisco Umbrella Architecture
  - Deploying Cisco Umbrella
  - Cisco Umbrella Roaming Client
  - Managing Cisco Umbrella
  - Cisco Umbrella Investigate Overview and Concepts
- Introducing VPN Technologies and Cryptography
  - VPN Definition
  - VPN Types
  - Secure Communication and Cryptographic Services
  - Keys in Cryptography
  - Public Key Infrastructure
- Explaining Cisco Secure Site-to-Site VPN Solutions
  - Site-to-Site VPN Topologies
  - IPsec VPN Overview

- IPsec Static Crypto Maps
- IPsec Static Virtual Tunnel Interface
- Dynamic Multipoint VPN
- Cisco IOS FlexVPN

- Implementing Cisco IOS VTI-Based Point-to-Point IPsec VPNs
  - Cisco IOS VTIs
  - Static VTI Point-to-Point IPsec Internet Key Exchange (IKE) v2 VPN Configuration
- Implementing Point-to-Point IPsec VPNs on the Cisco ASA and Cisco Firepower NGFW
  - Point-to-Point VPNs on the Cisco ASA and Cisco Firepower NGFW
  - Cisco ASA Point-to-Point VPN Configuration
  - Cisco Firepower NGFW Point-to-Point VPN Configuration
- Explaining Cisco Secure Remote Access VPN Solutions
  - Remote Access VPN Components
  - Remote Access VPN Technologies
  - Secure Sockets Layer (SSL) Overview
- Implementing Remote Access SSL VPNs on the Cisco ASA and Cisco Firepower NGFW
  - Remote Access Configuration Concepts
  - Connection Profiles
  - Group Policies
  - Cisco ASA Remote Access VPN Configuration
  - Cisco Firepower NGFW Remote Access VPN Configuration
- Implementing Cisco Secure Network Access Solutions
  - Cisco Secure Network Access
  - Cisco Secure Network Access Components
  - AAA Role in Cisco Secure Network Access Solution
  - Cisco Identity Services Engine
  - Cisco TrustSec
- Describing 802.1X Authentication
  - 802.1X and Extensible Authentication Protocol (EAP)
  - EAP Methods
  - Role of Remote Authentication Dial-in User Service (RADIUS) in 802.1X Communications
  - RADIUS Change of Authorization
- Configuring 802.1X Authentication
  - Cisco Catalyst® Switch 802.1X Configuration
  - Cisco Wireless LAN Controller (WLC) 802.1X Configuration
  - Cisco Identity Services Engine (ISE) 802.1X Configuration
  - Supplicant 802.1x Configuration

- Cisco Central Web Authentication

- Explaining Endpoint Security Technologies*
  - Host-Based Personal Firewall
  - Host-Based Anti-Virus
  - Host-Based Intrusion Prevention System
  - Application Whitelists and Blacklists
  - Host-Based Malware Protection
  - Sandboxing Overview
  - File Integrity Checking
- Implementing Cisco Advanced Malware Protection (AMP) for Endpoints*
  - Cisco AMP for Endpoints Architecture
  - Cisco AMP for Endpoints Engines
  - Retrospective Security with Cisco AMP
  - Cisco AMP Device and File Trajectory
  - Managing Cisco AMP for Endpoints
- Explaining Network Infrastructure Protection*
  - Identifying Network Device Planes
  - Control Plane Security Controls
  - Management Plane Security Controls
  - Network Telemetry
  - Layer 2 Data Plane Security Controls
  - Layer 3 Data Plane Security Controls
- Deploying Control Plane Security Controls*
  - Infrastructure ACLs
  - Control Plane Policing
  - Control Plane Protection
  - Routing Protocol Security
- Implementing Layer 2 Data Plane Security Controls*
  - Overview of Layer 2 Data Plane Security Controls
  - Virtual LAN (VLAN)-Based Attacks Mitigation
  - Spanning Tree Protocol (STP) Attacks Mitigation
  - Port Security
  - Private VLANs
  - Dynamic Host Configuration Protocol (DHCP) Snooping
  - Address Resolution Protocol (ARP) Inspection
  - Storm Control
  - MACsec Encryption
- Implementing Layer 3 Data Plane Security Controls*
  - Infrastructure Antispoofing ACLs
  - Unicast Reverse Path Forwarding

- IP Source Guard

- Implementing Management Plane Security Controls*
  - Cisco Secure Management Access
  - Simple Network Management Protocol Version 3
  - Secure Access to Cisco Devices
  - AAA for Management Access
- Deploying Traffic Telemetry Methods*
  - Network Time Protocol
  - Device and Network Events Logging and Export
  - Network Traffic Monitoring Using NetFlow
- Implementing Cisco Stealthwatch Enterprise*
  - Cisco Stealthwatch Offerings Overview
  - Cisco Stealthwatch Enterprise Required Components
  - Flow Stitching and Deduplication
  - Stealthwatch Enterprise Optional Components
  - Stealthwatch Enterprise and ISE Integration
  - Cisco Stealthwatch with Cognitive Analytics
  - Cisco Encrypted Traffic Analytics
  - Host Groups
  - Security Events and Alarms
  - Host, Role, and Default Policies
- Compare Cloud and Common Cloud Attacks*
  - Evolution of Cloud Computing
  - Cloud Service Models
  - Security Responsibilities in Cloud
  - Cloud Deployment Models
  - Common Security Threats in Cloud
  - Patch Management in the Cloud
  - Security Assessment in the Cloud
- Securing the Cloud*
  - Cisco Threat-Centric Approach to Network Security
  - Cloud Physical Environment Security
  - Application and Workload Security
  - Cloud Management and API Security
  - Network Function Virtualization (NFV) and Virtual Network Functions (VNF)
  - Cisco NFV Examples
  - Reporting and Threat Visibility in Cloud
  - Cloud Access Security Broker
  - Cisco CloudLock®
  - OAuth and OAuth Attacks

- Implementing Cisco Stealthwatch Cloud*
  - Cisco Stealthwatch Cloud for Public Cloud Monitoring
  - Cisco Stealthwatch Cloud for Private Network Monitoring
  - Cisco Stealthwatch Cloud Operations
- Comparing Software-Defined Networking (SDN*)
  - Software-Defined Networking Concepts
  - Network Programmability and Automation
  - Cisco Platforms and APIs
  - Basic Python Scripts for Automation

Lab outline

- Configure and Implement Network Settings and NAT on Cisco ASA
- Configure and Implement Cisco ASA Access Control Policies
- Configure and Implement Cisco Firepower NGFW NAT
- Configure and Implement Cisco Firepower NGFW Access Control Policy
- Configure and Implement Cisco Firepower NGFW Discovery and IPS Policy
- Configure and Implement Cisco NGFW Malware and File Policy
- Implement Listener, Host Access Table (HAT), and Recipient Access Table (RAT) on Cisco Email Security Appliance (ESA)
- Configure Mail Policies
- Implement Proxy Services, Authentication, and HTTPS Decryption
- Enforce Acceptable Use Control and Malware Protection
- Examine the Umbrella Dashboard
- Examine Cisco Umbrella Investigate
- Explore DNS Ransomware Protection by Cisco Umbrella
- Configure Static VTI Point-to-Point IPsec IKEv2 Tunnel
- Configure Point-to-Point VPN between the Cisco ASA and Cisco Firepower NGFW
- Configure Remote Access VPN on the Cisco Firepower NGFW
- Explore Cisco AMP for Endpoints
- Do Endpoint Analysis Using AMP for Endpoints Console
- Do File Ransomware Protection by Cisco AMP for Endpoints Console
- Do Cisco Stealthwatch Enterprise v6.9.3
- Do Cognitive Threat Analytics (CTA) in Stealthwatch Enterprise v7.0
- Do the Cisco Cloudlock Dashboard and User Security
- Do Cisco Cloudlock Application and Data Security
- Do Cisco Stealthwatch Cloud
- Do Stealthwatch Cloud Alert Settings, Watchlists, and Sensors

Concentration Exam (choose any one)

Concentration Exam Option 1: Securing Networks with Cisco Firepower Next Generation Firewall (300-710 SNCF)

Theory Outline

- Cisco Firepower Threat Defense Overview
  - Examining Firewall and IPS Technology
  - Firepower Threat Defense Features and Components
  - Examining Firepower Platforms
  - Examining Firepower Threat Defense Licensing
  - Cisco Firepower Implementation Use Cases
- Cisco Firepower NGFW Device Configuration
  - Firepower Threat Defense Device Registration
  - FXOS and Firepower Device Manager
  - Initial Device Setup
  - Managing NGFW Devices
  - Examining Firepower Management Center Policies
  - Examining Objects
  - Examining System Configuration and Health Monitoring
  - Device Management
  - Examining Firepower High Availability
  - Configuring High Availability
  - Cisco ASA to Firepower Migration
  - Migrating from Cisco ASA to Firepower Threat Defense
- Cisco Firepower NGFW Traffic Control
  - Firepower Threat Defense Packet Processing
  - Implementing QoS
  - Bypassing Traffic
- Cisco Firepower NGFW Address Translation
  - NAT Basics
  - Implementing NAT
  - NAT Rule Examples
  - Implementing NAT
- Cisco Firepower Discovery
  - Examining Network Discovery
  - Configuring Network Discovery
- Implementing Access Control Policies
  - Examining Access Control Policies
  - Examining Access Control Policy Rules and Default Action
  - Implementing Further Inspection
  - Examining Connection Events

    - Access Control Policy Advanced Settings
    - Access Control Policy Considerations
    - Implementing an Access Control Policy
- Security Intelligence
    - Examining Security Intelligence
    - Examining Security Intelligence Objects
    - Security Intelligence Deployment and Logging
    - Implementing Security Intelligence
- File Control and Advanced Malware Protection
    - Examining Malware and File Policy
    - Examining Advanced Malware Protection
- Next-Generation Intrusion Prevention Systems
    - Examining Intrusion Prevention and Snort Rules
    - Examining Variables and Variable Sets
    - Examining Intrusion Policies
- Site-to-Site VPN
    - Examining IPsec
    - Site-to-Site VPN Configuration
    - Site-to-Site VPN Troubleshooting
    - Implementing Site-to-Site VPN
- Remote-Access VPN
    - Examining Remote-Access VPN
    - Examining Public-Key Cryptography and Certificates
    - Examining Certificate Enrollment
    - Remote-Access VPN Configuration
    - Implementing Remote-Access VPN
- SSL Decryption
    - Examining SSL Decryption
    - Configuring SSL Policies
    - SSL Decryption Best Practices and Monitoring
- Detailed Analysis Techniques
    - Examining Event Analysis
    - Examining Event Types
    - Examining Contextual Data
    - Examining Analysis Tools
    - Threat Analysis
- System Administration
    - Managing Updates
    - Examining User Account Management Features
    - Configuring User Accounts
    - System Administration
- Cisco Firepower Troubleshooting
    - Examining Common Misconfigurations
    - Examining Troubleshooting Commands

    - Firepower Troubleshooting

Lab Outline

- Initial Device Setup
- Device Management
- Configuring High Availability
- Cisco ASA to Cisco Firepower Threat Defense migration
- Implementing QoS
- Implementing NAT
- Configuring Network Discovery
- Implementing an Access Control Policy
- Implementing Security Intelligence
- Implementing Site-to-Site VPN
- Implementing Remote Access VPN
- Threat Analysis
- System Administration
- Firepower Troubleshooting

Concentration Exam Option 2: Implementing and Configuring Cisco Identity Services Engine (300-715 SISE)

Theory Outline

- Introducing Cisco ISE Architecture and Deployment
    - Using Cisco ISE as a Network Access Policy Engine
    - Cisco ISE Use Cases
    - Describing Cisco ISE Functions
    - Cisco ISE Deployment Models
    - Context Visibility
- Cisco ISE Policy Enforcement
    - Using 802.1X for Wired and Wireless Access
    - Use MAC Authentication Bypass for Wired and Wireless Access
    - Introducing Identity Management
    - Configuring Certificate Services
    - Introducing Cisco ISE Policy
    - Executing Third-Party Network Access Device Support
    - Introducing Cisco TrustSec
    - Cisco TrustSec Configuration
    - Easy Connect
- Web Authentication and Guest Services
    - Introducing Web Access with Cisco ISE

    - Introducing Guest Access Components
    - Configuring Guest Access Settings
    - Configuring Sponsor and Guest Portals
- Cisco ISE Profiler
    - Introducing Cisco ISE Profiler
    - Profiling Deployment and Best Practices
- Cisco ISE BYOD
    - Introducing the Cisco ISE BYOD Process
    - Describing BYOD Flow
    - Configuring the My Devices Portal
    - Configuring Certificates in BYOD Scenarios
- Cisco ISE Endpoint Compliance Services
    - Introducing Endpoint Compliance Services
    - Designing Client Posture Services and Provisioning in Cisco ISE
- Working with Network Access Devices
    - Review TACACS+
    - Cisco ISE TACACS+ Device Administration
    - Configure TACACS+ Device Administration
    - TACACS+ Device Administration Guidelines and Best Practices
    - Migrating from Cisco ACS to Cisco ISE

Lab Outline

- Access the SISE Lab and Install ISE 2.4
- Design Initial Cisco ISE Setup, GUI Familiarization, and System Certificate Usage
- Integrate Cisco ISE with Active Directory
- Configure Basic Policy on Cisco ISE
- Configure Policy Sets
- Configure Access Policy for Easy Connect
- Configure Guest Access
- Configure Guest Access Operations
- Create Guest Reports
- Configure Profiling
- Customize the Cisco ISE Profiling Configuration
- Create Cisco ISE Profiling Reports
- Configure BYOD
- Blacklisting a Device
- Configure Cisco ISE Compliance Services
- Configure Client Provisioning
- Configure Posture Policies
- Test and Monitor Compliance-Based Access
- Test Compliance Policy
- Configure Cisco ISE for Basic Device Administration
- Configure TACACS+ Command Authorization

Concentration Exam Option 3: Securing Email with Cisco Email Security Appliance (300-720 SESA)

Theory Outline

- Describing the Cisco Email Security Appliance
  - Cisco Email Security Appliance Overview
  - Technology Use Case
  - Cisco Email Security Appliance Data Sheet
  - SMTP Overview
  - Email Pipeline Overview
  - Installation Scenarios
  - Initial Cisco Email Security Appliance Configuration
  - Centralizing Services on a Cisco Content SMA
  - Release Notes for AsyncOS 11.x
- Administering the Cisco Email Security Appliance
  - Distributing Administrative Tasks
  - System Administration
  - Managing and Monitoring Using the CLI
  - Other Tasks in the GUI
  - Advanced Network Configuration
  - Using Email Security Monitor
  - Tracking Messages
  - Logging
- Controlling Sender and Recipient Domains
  - Public and Private Listeners
  - Configuring the Gateway to Receive Email
  - Host Access Table Overview
  - Recipient Access Table Overview
  - Configuring Routing and Delivery Features
- Controlling Spam with Talos SenderBase and Anti-Spam
  - SenderBase Overview
  - Anti-Spam
  - Managing Graymail
  - Protecting Against Malicious or Undesirable URLs
  - File Reputation Filtering and File Analysis
  - Bounce Verification
- Using Anti-Virus and Outbreak Filters
  - Anti-Virus Scanning Overview
  - Sophos Anti-Virus Filtering
  - McAfee Anti-Virus Filtering
  - Configuring the Appliance to Scan for Viruses
  - Outbreak Filters
  - How the Outbreak Filters Feature Works
  - Managing Outbreak Filters
- Using Mail Policies
  - Email Security Manager Overview
  - Mail Policies Overview
  - Handling Incoming and Outgoing Messages Differently
  - Matching Users to a Mail Policy
  - Message Splintering

    - Configuring Mail Policies
- Using Content Filters
    - Content Filters Overview
    - Content Filter Conditions
    - Content Filter Actions
    - Filter Messages Based on Content
    - Text Resources Overview
    - Using and Testing the Content Dictionaries Filter Rules
    - Understanding Text Resources
    - Text Resource Management
    - Using Text Resources
- Using Message Filters to Enforce Email Policies
    - Message Filters Overview
    - Components of a Message Filter
    - Message Filter Processing
    - Message Filter Rules
    - Message Filter Actions
    - Attachment Scanning
    - Examples of Attachment Scanning Message Filters
    - Using the CLI to Manage Message Filters
    - Message Filter Examples
    - Configuring Scan Behavior
- Preventing Data Loss
    - Overview of the Data Loss Prevention (DLP) Scanning Process
    - Setting Up Data Loss Prevention
    - Policies for Data Loss Prevention
    - Message Actions
    - Updating the DLP Engine and Content Matching Classifiers
- Using LDAP
    - Overview of LDAP
    - Working with LDAP
    - Using LDAP Queries
    - Authenticating End-Users of the Spam Quarantine
    - Configuring External LDAP Authentication for Users
    - Testing Servers and Queries
    - Using LDAP for Directory Harvest Attack Prevention
    - Spam Quarantine Alias Consolidation Queries
    - Validating Recipients Using an SMTP Server
- SMTP Session Authentication
    - Configuring AsyncOS for SMTP Authentication
    - Authenticating SMTP Sessions Using Client Certificates
    - Checking the Validity of a Client Certificate
    - Authenticating User Using LDAP Directory
    - Authenticating SMTP Connection Over Transport Layer Security (TLS) Using a Client Certificate
    - Establishing a TLS Connection from the Appliance
    - Updating a List of Revoked Certificates
- Email Authentication
    - Email Authentication Overview
    - Configuring DomainKeys and DomainKeys Identified Mail (DKIM) Signing
    - Verifying Incoming Messages Using DKIM

    - Overview of Sender Policy Framework (SPF) and SIDF Verification
    - Domain-based Message Authentication Reporting and Conformance (DMARC) Verification
    - Forged Email Detection
- Email Encryption
    - Overview of Cisco Email Encryption
    - Encrypting Messages
    - Determining Which Messages to Encrypt
    - Inserting Encryption Headers into Messages
    - Encrypting Communication with Other Message Transfer Agents (MTAs)
    - Working with Certificates
    - Managing Lists of Certificate Authorities
    - Enabling TLS on a Listener's Host Access Table (HAT)
    - Enabling TLS and Certificate Verification on Delivery
    - Secure/Multipurpose Internet Mail Extensions (S/MIME) Security Services
- Using System Quarantines and Delivery Methods
    - Describing Quarantines
    - Spam Quarantine
    - Setting Up the Centralized Spam Quarantine
    - Using Safelists and Blocklists to Control Email Delivery Based on Sender
    - Configuring Spam Management Features for End Users
    - Managing Messages in the Spam Quarantine
    - Policy, Virus, and Outbreak Quarantines
    - Managing Policy, Virus, and Outbreak Quarantines
    - Working with Messages in Policy, Virus, or Outbreak Quarantines
    - Delivery Methods
- Centralized Management Using Clusters
    - Overview of Centralized Management Using Clusters
    - Cluster Organization
    - Creating and Joining a Cluster
    - Managing Clusters
    - Cluster Communication
    - Loading a Configuration in Clustered Appliances
    - Best Practices
- Testing and Troubleshooting
    - Debugging Mail Flow Using Test Messages: Trace
    - Using the Listener to Test the Appliance
    - Troubleshooting the Network
    - Troubleshooting the Listener
    - Troubleshooting Email Delivery
    - Troubleshooting Performance
    - Web Interface Appearance and Rendering Issues
    - Responding to Alerts
    - Troubleshooting Hardware Issues
    - Working with Technical Support
- References
    - Model Specifications for Large Enterprises
    - Model Specifications for Midsize Enterprises and Small-to-Midsize Enterprises or Branch Offices
    - Cisco Email Security Appliance Model Specifications for Virtual Appliances
    - Packages and Licenses

Lab Outline

- Verify and Test Cisco ESA Configuration
- Perform Basic Administration
- Advanced Malware in Attachments (Macro Detection)
- Protect Against Malicious or Undesirable URLs Beneath Shortened URLs
- Protect Against Malicious or Undesirable URLs Inside Attachments
- Intelligently Handle Unscannable Messages
- Leverage AMP Cloud Intelligence Via Pre-Classification Enhancement
- Integrate Cisco ESA with AMP Console
- Prevent Threats with Anti-Virus Protection
- Applying Content and Outbreak Filters
- Configure Attachment Scanning
- Configure Outbound Data Loss Prevention
- Integrate Cisco ESA with LDAP and Enable the LDAP Accept Query
- Domain Keys Identified Mail (DKIM)
- Sender Policy Framework (SPF)
- Forged Email Detection
- Configure the Cisco SMA for Tracking and Reporting

Concentration Exam Option 4: Securing the Web with Cisco Web Security Appliance (300-725 SWSA)

Theory Outline

- Describing Cisco WSA
    - Technology Use Case
    - Cisco WSA Solution
    - Cisco WSA Features
    - Cisco WSA Architecture
    - Proxy Service
    - Integrated Layer 4 Traffic Monitor
    - Data Loss Prevention
    - Cisco Cognitive Intelligence
    - Management Tools
    - Cisco Advanced Web Security Reporting (AWSR) and Third-Party Integration
    - Cisco Content Security Management Appliance (SMA)
- Deploying Proxy Services
    - Explicit Forward Mode vs. Transparent Mode
    - Transparent Mode Traffic Redirection
    - Web Cache Control Protocol
    - Web Cache Communication Protocol (WCCP) Upstream and Downstream Flow
    - Proxy Bypass
    - Proxy Caching

    - Proxy Auto-Config (PAC) Files
    - FTP Proxy
    - Socket Secure (SOCKS) Proxy
    - Proxy Access Log and HTTP Headers
    - Customizing Error Notifications with End User Notification (EUN) Pages
- Utilizing Authentication
    - Authentication Protocols
    - Authentication Realms
    - Tracking User Credentials
    - Explicit (Forward) and Transparent Proxy Mode
    - Bypassing Authentication with Problematic Agents
    - Reporting and Authentication
    - Re-Authentication
    - FTP Proxy Authentication
    - Troubleshooting Joining Domains and Test Authentication
    - Integration with Cisco Identity Services Engine (ISE)
- Creating Decryption Policies to Control HTTPS Traffic
    - Transport Layer Security (TLS)/Secure Sockets Layer (SSL) Inspection Overview
    - Certificate Overview
    - Overview of HTTPS Decryption Policies
    - Activating HTTPS Proxy Function
    - Access Control List (ACL) Tags for HTTPS Inspection
    - Access Log Examples
- Understanding Differentiated Traffic Access Policies and Identification Profiles
    - Overview of Access Policies
    - Access Policy Groups
    - Overview of Identification Profiles
    - Identification Profiles and Authentication
    - Access Policy and Identification Profiles Processing Order
    - Other Policy Types
    - Access Log Examples
    - ACL Decision Tags and Policy Groups
    - Enforcing Time-Based and Traffic Volume Acceptable Use Policies, and End User Notifications
- Defending Against Malware
    - Web Reputation Filters
    - Anti-Malware Scanning
    - Scanning Outbound Traffic
    - Anti-Malware and Reputation in Policies
    - File Reputation Filtering and File Analysis
    - Cisco Advanced Malware Protection
    - File Reputation and Analysis Features
    - Integration with Cisco Cognitive Intelligence
- Enforcing Acceptable Use Control Settings
    - Controlling Web Usage

    - URL Filtering
    - URL Category Solutions
    - Dynamic Content Analysis Engine
    - Web Application Visibility and Control
    - Enforcing Media Bandwidth Limits
    - Software as a Service (SaaS) Access Control
    - Filtering Adult Content
- Data Security and Data Loss Prevention
    - Data Security
    - Cisco Data Security Solution
    - Data Security Policy Definitions
    - Data Security Logs
- Performing Administration and Troubleshooting
    - Monitor the Cisco Web Security Appliance
    - Cisco WSA Reports
    - Monitoring System Activity Through Logs
    - System Administration Tasks
    - Troubleshooting
    - Command Line Interface
- References
    - Comparing Cisco WSA Models
    - Comparing Cisco SMA Models
    - Overview of Connect, Install, and Configure
    - Deploying the Cisco Web Security Appliance Open Virtualization Format (OVF) Template
    - Mapping Cisco Web Security Appliance Virtual Machine (VM) Ports to Correct Networks
    - Connecting to the Cisco Web Security Virtual Appliance
    - Enabling Layer 4 Traffic Monitor (L4TM)
    - Accessing and Running the System Setup Wizard
    - Reconnecting to the Cisco Web Security Appliance
    - High Availability Overview
    - Hardware Redundancy
    - Introducing Common Address Redundancy Protocol (CARP)
    - Configuring Failover Groups for High Availability
    - Feature Comparison Across Traffic Redirection Options
    - Architecture Scenarios When Deploying Cisco AnyConnect® Secure Mobility

Lab Outline

- Configure the Cisco Web Security Appliance
- Deploy Proxy Services
- Configure Proxy Authentication

- Configure HTTPS Inspection
- Create and Enforce a Time/Date-Based Acceptable Use Policy
- Configure Advanced Malware Protection
- Configure Referrer Header Exceptions
- Utilize Third-Party Security Feeds and MS Office 365 External Feed
- Validate an Intermediate Certificate
- View Reporting Services and Web Tracking
- Perform Centralized Cisco AsyncOS Software Upgrade Using Cisco SMA

Concentration Exam Option 5: Implementing Secure Solutions with Virtual Private Networks (300-730 SVPN)

Theory Outline

- Introducing VPN Technology Fundamentals
- Implementing Site-to-Site VPN Solutions
- Implementing Cisco Internetwork Operating System (Cisco IOS®) Site-to-Site FlexVPN Solutions
- Implement Cisco IOS Group Encrypted Transport (GET) VPN Solutions
- Implementing Cisco AnyConnect VPNs
- Implementing Clientless VPNs

Lab Outline

- Explore IPsec Technologies
- Implement and Verify Cisco IOS Point-to-Point VPN
- Implement and Verify Cisco Adaptive Security Appliance (ASA) Point-to-Point VPN
- Implement and Verify Cisco IOS Virtual Tunnel Interface (VTI) VPN
- Implement and Verify Dynamic Multipoint VPN (DMVPN)
- Troubleshoot DMVPN
- Implement and Verify FlexVPN with Smart Defaults
- Implement and Verify Point-to-Point FlexVPN
- Implement and Verify Hub and Spoke FlexVPN
- Implement and Verify Spoke-to-Spoke FlexVPN
- Troubleshoot Cisco IOS FlexVPN
- Implement and Verify AnyConnect Transport Layer Security (TLS) VPN on ASA
- Implement and Verify Advanced Authentication, Authorization, and Accounting (AAA) on Cisco AnyConnect VPN
- Implement and Verify Clientless VPN on ASA

Concentration Exam Option 6: Implementing Automation for Cisco Security Solutions (300-735 SAUTO)

Theory Outline

- Introducing Cisco Security APIs
- Consuming Cisco Advanced Malware Protection APIs
- Using Cisco ISE
- Using Cisco pxGrid APIs
- Using Cisco Threat Grid APIs
- Investigating Cisco Umbrella Security Data Programmatically
- Exploring Cisco Umbrella Reporting and Enforcement APIs
- Automating Security with Cisco Firepower APIs
- Operationalizing Cisco Stealthwatch and the API Capabilities
- Using Cisco Stealthwatch Cloud APIs
- Describing Cisco Security Management Appliance APIs

Lab Outline

- Query Cisco AMP Endpoint APIs for Verifying Compliance
- Use the REST API and Cisco pxGrid with Cisco Identity Services Engine
- Construct a Python Script Using the Cisco Threat Grid API
- Generate Reports Using the Cisco Umbrella Reporting API
- Explore the Cisco Firepower Management Center API
- Use Ansible to Automate Cisco Firepower Threat Defense Configuration
- Automate Firewall Policies Using the Cisco Firepower Device Manager API
- Automate Alarm Policies and Create Reports Using the Cisco Stealthwatch APIs
- Construct a Report Using Cisco Stealthwatch Cloud APIs

Note: ***Most of the course topics are covered with hands-on lab exercises and others are theoretical

Thank You

Visit us

https://www.uninets.com/