CCIE Security Syllabus

Module 1:- Firewall

□ Day 1-120 mins

- Introduction to the course
- Course Material
- Planning or CCIE
- Discuss the Table of Content

□ Day 2-120 mins

- Cisco ASA Overview
- Firewall Overview
- Firewall Technique
- Stateless Packet Filtering
- Stateful Packet Filtering
- Cisco ASA Product Family
- Introducing the Cisco ASA 5500-X Series NGFW
- Introducing the Cisco ASAV
- Different between UTM and NGFW

□ Day 3-120 mins

- Cisco ASA Features
- Using the CLI
- Using the Cisco ASDM
- Understanding Factory default configuration
- Working on the configuration les
- Cisco ASA Firewall Interfaces
- Configuring Physical interfaces
- Configuring Vlan interfaces
- Redundant Interface
- Configuring Interface Security Parameters
- Naming the interface
- Security Level
- Assigning the IP Address

□ Day 4-120 mins

- Cisco ASA IP Connectivity
- Configuring the Static Routing
- Routing with EIGRP
- Routing with OSPF
- Routing with BGP
- Verifying the routing Table
- Configuring the SSH and Telnet
- Configuring HTTP/S

□ Day 5/6-240 mins

- Cisco ASA NAT (Address Translation)
- Understanding the Nat
- Methods of NAT

- Inside NAT
- Outside NAT
- Implementation of NAT
- Auto NAT
- Manual NAT
- Types of NAT
- Static
- NAT
- PAT
- Dynamic
- NAT
- PAT
- Twice NAT
- Identity NAT

□ Day 7-120 mins

- Cisco ASA Modes
- Transparent Mode
- Routed Mode

□ Day 8/9/10-360 mins

- Cisco High Availability
- ASA Failover
- Active/Standby
- Active/Active
- Verifying failover Operations
- Clustering ASA firewall
- Wireshark Capture
- Cisco ASA ACL
- Inside/Outside ACL.
- Object ACL
- Life of a Packet on the Cisco
- Cisco ASA Context
- Admin Context
- System Context
- User Context
- Deployment Guide

Module 2:- VPN

□ Day 11-120 mins

- Cryptography Overview
- Hash Algorithm
- Encryption Overview
- Cryptanalysis
- Symmetric Encryption Algorithm
- Asymmetric Encryption Algorithm
- Digital Signatures
- PKI Overview
- PKI Operations

□ Day 12-120 mins

- What is VPN
- Introduction of Ipsec Terminology
- VPN Types
- Ipsec Features
- Confidentially, Integrity, Available and Anti-
- Replay.
- IPSec Protocols:- IKE, ESP and AH
- IKE Modes
- IKE Phases
- NAT-T
- Security Associations and Components
- How to Configure cisco IOS as CA
- Fundamentals of VPN Technologies and IPSec

□ Day 13/14-240 mins

- What is Site-toSite VPN
- Wireshark Capture
- GRE
- Gre Over IPSec
- Site-to-site VPN Labs
- Site to Site VPN

□ Day 15/16-240 mins

- DMVPN Overview
- DMVPN Terminologies
- NHRP
- MGRE
- DMVPN Working
- DMVPN Advantages and Limitations
- DMVPN Phase 1,2 and 3
- DMVPN Labs
- DMVPN Redundancy- Dual Hub DMVPN
- Deployment
- Deploying DMVPN

□ Day 15-120 mins

- Remote Access VPN Introduction
- Remote Access VPN modes
- Client Mode Software
- Client Mode Hardware
- Remote Access witrh DVTI
- Remote Access Working
- Remote Access Labs
- Remote Access VPN

□ Day 18-120 mins

- SSL VPN Overview
- SSL Handshake
- SSL VPN Modes
- Clientless and Thick Client
- SSL VPN Working
- SSL VPN Labs

- Deploying Clientless SSL VPN
- https://www.acs-networks.com

□ Day 19-120 mins

- Anyconnect Overview
- Connection Policies
- Group Policies
- Split Tunnelling
- Client Prošle
- Anyconnect Image Upload
- Deploying Anyconnect VPN

□ Day 20-120 mins

- GET VPN
- GET VPN Terminologies
- GDOI
- Key Server (KS)
- KEK (Key Encryption Key)
- TEK (Traffic Encryption Key)
- Rekey Process (Unicast and Multicasr)
- Group Member (GM)
- GET VPN Lab and Working
- GET VPN

□ Day 21/22-240 mins

- Introducing and Working IOS Flex VPN
- Flex VPN Labs
- Flex VPN

□ Day 23-120 mins

- Security Challenges
- Cisco ISE Solutions Use Cases
- Secure Access Control
- ISE function
- ISE deployment components
- Context visibility
- ISE Personas
- ISE Licensing
- Infrastructure Components
- Identity Source
- Introducing Cisco ISE Architecture and Deployment

□ Day 24-120 mins

- AAA
- Radius Overview
- Radius Messages
- AV Pair
- IEEE 802.1xPrimer
- EAP
- Types of EAP
- Tunnel EAP
- EAP-FAST
- PEAP

- EAP-TLS
- Non-Tunnel EAP
- EAP-MD5
- MSCHAP
- EAP GTC
- Host Mode
- Deployment of 802.1x
- Fundamentals of AAA

Module 3 -ISE

□ Day 25-120 mins

- Radius Commands
- AAA Commands
- Bootstrap Network Access Devices

□ Day 27/28/29-120 mins

- Dotlx Authentication and Authorization
- MAB Authentication and Authorization
- AP Authentication and Authorization
- Device Administration
- Configuring Authentication and Authorization Policy

□ Day 26-120 mins

- AD Overview and configuration
- Admin Access
- Administrative Work
- Certificate in ISE
- Personas
- Probes for ISE
- Back/Restore
- Maintenance
- Introduction to ISE GUI
- Configuring Posturing and Proling
- Posturing
- Prolling of Devices
- Cisco Trussec and its Component
- SGT/SGN Tagging
- Classification

□ Day 32/33/34/35/36-480 mins

- What is NGFW and UTM
- Components of NGFW
- Introduction of the SourceFire and Snort Rules
- Cisco Acquisitions
- FTD, NGIPS
- Off Box Management and ON Box Management
- FMC and FDM GUI
- Licensing on the FMC
- Registration of FMC with FTD and NGIPS
- Configuration of the Sensor Interface
- Configuring NAT and Routing

- Cisco NGFW

□ Day 30/31-240 mins

- Configuration the Cisci WLC and AP via GUI and CLI
- Miscellaneous Topic
- Propagation
- Inline
- SXP
- Enforcement ACL
- Cisco Anyconnect VPN authentication from ISE
- Cisco VPN Authentication
- Troubleshooting ISE
- Radius Live Log
- Diagnostic Validator
- Logs Management
- Radius Messages with Attribute Type

MODULE 4 :- NGFW

□ Day 37/38/39-360 mins

- Describe the Cisco WSA
- Install and verify the WSA
- Deploy proxy Services for the WSA
- WCCP Services and Transport Proxy
- Utilize authentication with the WSA
- Configure various policies for the WSA
- Enforce acceptable use using the WSA
- Defend against malware
- Configure data security
- Permorm Administration and Troubleshooting of WSA's
- WSA/ESA
- Configuring the Policies
- Access Control Policy
- SSL Policy
- Pre-Filter Policy
- Security Intelligence
- DNS Policy
- HTTP Response
- Blocking Gambling and Social Networking Sites
- Intrusion Policy
- Life of a Packet the Cisco Next Generation Firewall

MODULE 5 :- NGFW

□ Day 37/38/39-360 mins

- Describe the Cisco WSA
- Install and verify the WSA
- Deploy proxy Services for the WSA
- WCCP Services and Transport Proxy
- Utilize authentication with the WSA

- Configure various policies for the WSA
- Enforce acceptable use using the WSA
- Defend against malware
- Configure data security
- Permorm Administration and Troubleshooting of WSA's
- WSA/ESA
- Configuring the Policies
- Access Control Policy
- SSL Policy
- Pre-Filter Policy
- Security Intelligence
- DNS Policy
- HTTP Response
- Blocking Gambling and Social Networking Sites
- Intrusion Policy
- Life of a Packet the Cisco Next Generation Firewall

MODULE 6:- Cisco Stealth Watch And Cisco Umbrella

□ Day 40/41/42/43-480 mins

- Stealth Watch
- Introduction to Netflow
- Why we need Cisco StealthWatch
- Components of StealthWatch
- Advance Feature of StealthWatch
- Configuring the StealthWatch Management
- Using the Appliances Setup Tool with the SMC
- Configuring the StealthWatch Flow Collector

□ Day 14/45/46-360 mins

- Umbrella
- Cisco Umbrella- Security Solution
- Implementing Cisco Umbrella
- Roaming Client
- Umbrella Roaming Security
- Reporting
- Active Directory User Sync
- Finalising the Flow Collector Con@guration
- Adding a Flow Collector to the SMC
- Exploring Where to Enable Network on a Network
- Configuring NetFlow on Cisco IOS Routers/ASA/Switches
- An Example of a NetFlow Cong Generator Tool
- Introduction to the Stealthwatch GUIs
- Organizing Hosts with Host Groups
- Analyzing Flows
- Enabling Cognitive Analytics
- Configuring Encrypted Traffic Analytics
- Creating Custom Policies
- Acknowledge Alarms
- Installing Stealthwatch Apps

- Capturing Packets for Diagnostics
- Logs, Stats, and Diagnostic Packs

MODULE 7:- CCIE LAB

□ Day 40/41/42/43-480 mins

- CCIE LAB Preparation
- 20x8hr Session =120 Hrs
- Multiple Mock Labs
- 80 Hrs Technology Labs
- Preparation for the Design/Tshoot/Configuration
- Self-Analysis Sheet