



# CISCO CCNP 350-701

## Training and Certification

Cyber Security Educational Courses Professional Sessions

### ABOUT US

We offer Cyber Security and Information Security training and Certification in Delhi for Cyber Security and Information Technology aspirants. Since Decade, we have been in the Information Technology and Cybersecurity industry. You can learn more about cybersecurity, Techniques, and Tools to choose a better career path.

### DESCRIPTION

Cisco CCNP Training in Delhi Engineer responsible for Security in Routers, Switches, Firewall, and Ips, as well as choosing, deploying, supporting, and troubleshooting Firewalls, with the substantial increase in cybercrime attacks. To earn CCNP Training in Delhi, you pass two exams: a core exam and a security concentration exam of your choice. And now every exam in the CCNP Security program earns an individual Specialist certification, so you get recognized for your accomplishments along the way.



Duration -  
40Hrs



Language -  
Hindi & English



Mode -  
Online & Offline

### BENEFITS

1. Basic to Advanced Courses
2. Interview Cracking and Proposal-Making Sessions
3. Transparent Syllabus
4. Career-Oriented Courses and Certifications
5. International Accreditation

## CRAW ACADEMY

#### SAKET ADDRESS

1st Floor, Plot no. 4, Lane no. 2,  
Kehar Singh Estate, Westend Marg,  
Behind Saket Metro Station,  
Saidulajab New Delhi - 110030

#### LAXMI NAGAR ADDRESS

R31/ 32, 2nd floor Jandu Tower,  
Vikas marg, Shakarpur,  
New Delhi -110092

www.craw.in

+91 951 380 5401



SAMPLE CERTIFICATE





# CISCO CCNP 350-701

Training and Certification

Cyber Security Educational Courses Professional Sessions

## CISCO CCNP 350-701 MODULE



### Module 1: Cisco ASA Overview

- 1.1 Firewall Overview
- 1.2 Firewall Techniques
- 1.3 Stateless Packet Filtering
- 1.4 Stateful Packet Filtering
- 1.5 Cisco ASA Product Family
- 1.6 Introducing the Cisco ASA 5500-X Series NGFW
- 1.7 Introducing the Cisco ASAv
- 1.8 Difference between UTM and NGFW
- 1.9 Cisco ASA Features
- 1.10 Using the CLI
- 1.11 Using the Cisco ASDM
- 1.12 Understanding Factory default configuration
- 1.13 Working on the configuration files
- 1.14 Cisco ASA Firewall Interfaces
- 1.15 Configuring Physical interfaces
- 1.16 Configuring Vlan interfaces
- 1.17 Redundant Interface
- 1.18 Configuring Interface Security Parameters
- 1.19 Naming the interface
- 1.20 Security Level
- 1.21 Assigning the IP Address
- 1.22 Cisco ASA IP Connectivity
- 1.23 Configuring the Static Routing
- 1.24 Routing with EIGRP
- 1.25 Routing with OSPF
- 1.26 Routing with BGP
- 1.27 Verifying the Routing Table
- 1.28 Configuring the SSH and Telnet
- 1.29 Configuring HTTP/S
- 1.30 Cisco ASA NAT (Network Address Translation)
- 1.31 Understanding the NAT
- 1.32 Methods of NAT
- 1.33 Inside NAT
- 1.34 Outside NAT
- 1.35 Implementation of NAT
- 1.36 Auto NAT
- 1.37 Manual NAT
- 1.38 Types of NAT
- 1.39 Static
- 1.40 NAT
- 1.41 PAT
- 1.42 Dynamic
- 1.43 NAT
- 1.44 PAT
- 1.45 Twice NAT
- 1.46 Identity NAT
- 1.47 Cisco ASA ACL
- 1.48 Inside/ Outside ACL.
- 1.49 Object GROUP ACL.
- 1.50 Life of a Packet on the Cisco
- 1.51 Cisco ASA Modes
- 1.52 Transparent Mode
- 1.53 Routed Mode
- 1.54 Cisco ASA Context
- 1.55 Admin Context
- 1.56 System Context
- 1.57 User Context
- 1.58 Deployment Guide
- 1.59 Cisco High Availability
- 1.60 ASA Failover
- 1.61 Active/Standby
- 1.62 Active/Active
- 1.63 Verifying failover Operations
- 1.64 Clustering ASA firewallWireshark Capture



# CISCO CCNP 350-701

Training and Certification

Cyber Security Educational Courses Professional Sessions

## CISCO CCNP 350-701 MODULE

---

### Module 2: Cryptography Overview

- 2.1 Hash Algorithm
- 2.2 Encryption Overview
- 2.3 Cryptanalysis
- 2.4 Symmetric Encryption Algorithm
- 2.5 Asymmetric Encryption Algorithm
- 2.6 Digital Signatures
- 2.7 PKI Overview
- 2.8 PKI Operations
- 2.9 Fundamentals of VPN Technologies and IPsec
- 2.10 What is VPN
- 2.11 Introduction of Ipvsec Terminology
- 2.12 VPN Types
- 2.13 Ipvsec Features
- 2.14 Confidentiality, Integrity, Availability and Anti-Replay.
- 2.15 IPsec Protocols: – IKE, ESP and AH
- 2.16 IKE Modes
- 2.17 IKE Phases
- 2.18 NAT-T
- 2.19 Security Associations and Components
- 2.20 How to configure cisco IOS as CA
- 2.21 Site to Site VPN ROUTER AND ALSO ON CISCO ASA
- 2.22 What is Site-to Site VPN
- 2.23 Wireshark Capture
- 2.24 GRE
- 2.25 Gre over IPsec
- 2.26 Site-to-Site VPN Labs
- 2.27 Deploying DMVPN
- 2.28 DMVPN Overview
- 2.29 DMVPN Terminologies
- 2.30 NHRP
- 2.31 MGRE
- 2.32 DMVPN Working
- 2.33 DMVPN Advantages and Limitations
- 2.34 DMVPN Phase 1, 2 and 3
- 2.35 DMVPN Labs
- 2.36 DMVPN Redundancy – Dual Hub DMVPN Deployment
- 2.37 Remote Access VPN
- 2.38 Remote Access VPN Introduction
- 2.39 Remote Access VPN modes
- 2.40 Client Mode Software
- 2.41 Client Mode Hardware
- 2.42 Remote Access with DVTI
- 2.43 Remote Access Working
- 2.44 Remote Access Labs
- 2.45 Deploying Clientless SSL VPN
- 2.46 SSL VPN Overview
- 2.47 SSL Handshake
- 2.48 SSL VPN Modes
- 2.49 Clientless and Thick Client
- 2.50 SSL VPN Working
- 2.51 SSL VPN Labs
- 2.52 Deploying Anyconnect VPN
- 2.53 Anyconnect Overview
- 2.54 Connection Policies
- 2.55 Group Policies
- 2.56 Split Tunnelling
- 2.57 Client Profile
- 2.58 Anyconnect Image Upload
- 2.59 GET VPN
- 2.60 GET VPN
- 2.61 GET VPN Terminologies
- 2.62 GDOI
- 2.63 Key Server (KS)
- 2.64 KEK (Key Encryption Key)
- 2.65 TEK (Traffic Encryption Key)
- 2.66 Rekey Process (Unicast and Multicast)
- 2.67 Group Member (GM)
- 2.68 GET VPN Lab and Working
- 2.69 Flex VPN
- 2.70 Introduction and Working IOS Flex VPN
- 2.71 Flex VPN Labs





# CISCO CCNP 350-701

Training and Certification

Cyber Security Educational Courses Professional Sessions

## CISCO CCNP 350-701 MODULE



### Module 3: Introducing Cisco ISE Architecture and Deployment

- 3.1 Security challenges
- 3.2 Cisco ISE solutions Use Cases
- 3.3 Secure Access Control
- 3.4 ISE function
- 3.5 ISE deployment components
- 3.6 Context visibility
- 3.7 ISE Personas
- 3.8 ISE Licensing
- 3.9 Infrastructure Components
- 3.10 Identity Source
- 3.11 Fundamentals of AAA
- 3.12 AAA
- 3.13 Radius Overview
- 3.14 Radius Messages
- 3.15 AV Pair
- 3.16 IEEE 802.1x Primer
- 3.17 EAP
- 3.18 Types of EAP
- 3.19 Tunnel EAP
- 3.20 EAP-FAST
- 3.21 PEAP
- 3.22 EAP-TLS
- 3.23 Non-Tunnel EAP
- 3.24 EAP-MD5
- 3.25 MSCHAP
- 3.26 EAP GTC
- 3.27 Host Mode
- 3.28 Deployment of 802.1x
- 3.29 Bootstrap Network Access Devices
- 3.30 Radius Commands
- 3.31 AAA Commands
- 3.32 Introduction to ISE GUI
- 3.33 AD overview and configuration
- 3.34 Admin Access
- 3.35 Administrative Work
- 3.36 Certificate in ISE
- 3.37 Personas
- 3.38 Probes for ISE
- 3.39 Backup/Restore
- 3.40 Maintenance
- 3.41 Configuring Authentication and Authorization Policy
- 3.42 Dot1x Authentication and Authorization
- 3.43 MAB Authentication and Authorization
- 3.44 AP Authentication and Authorization
- 3.45 Device Administration
- 3.46 Configuring Posturing and Profiling
- 3.47 Posturing
- 3.48 Profiling of Devices
- 3.49 Cisco TrustSec and Its Component
- 3.50 SGT/SGN Tagging
- 3.51 Classification
- 3.52 Propagation
- 3.53 Inline
- 3.54 SXP
- 3.55 Enforcement ACL
- 3.56 Miscellaneous Topics
- 3.57 Configuring the Cisco WLC and AP via GUI and CLI
- 3.58 Cisco VPN Authentication
- 3.59 Cisco Anyconnect VPN authentication from ISE
- 3.60 Troubleshooting ISE
- 3.61 Radius Live Log
- 3.62 Diagnostic Validator
- 3.63 Logs Management
- 3.64 Radius Messages with Attribute Type



# CISCO CCNP 350-701

Training and Certification

Cyber Security Educational Courses Professional Sessions

## CISCO CCNP 350-701 MODULE



### Module 4: Cisco NGFW

- 4.1 What are NGFW and UTM
- 4.2 Components of NGFW
- 4.3 Introduction of the SourceFire and Snort Rules
- 4.4 Cisco Acquisitions
- 4.5 FTD, NGIPS
- 4.6 Off-Box Management and On-Box Management
- 4.7 FMC and FDM GUI
- 4.8 Licensing on the FMC
- 4.9 Registration of FMC with FTD and NGIPS
- 4.10 Configuration of the Sensor Interface
- 4.11 Configuring NAT and Routing

### Module 5: WSA/ESA

- 5.1 Describe the Cisco WSA
- 5.2 Install and verify the WSA
- 5.3 Deploy proxy services for the WSA
- 5.4 WCCP Services and Transparent Proxy
- 5.5 Utilize authentication with the WSA
- 5.6 Configure various policies for the WSA
- 5.7 Enforce acceptable use using the WSA
- 5.8 Defend against malware
- 5.9 Configure data security
- 5.10 Perform Administration and Troubleshooting of WSA's

### Module 6: Introduction to Netflow

- 6.1 Why we need Cisco StealthWatch
- 6.2 Components of StealthWatch
- 6.3 Advance Features of StealthWatch
- 6.4 Configuring the Stealthwatch Management Console
- 6.5 Using the Appliance Setup Tool with the SMC
- 6.6 Configuring the Stealthwatch Flow Collector

## CRAW SECURITY

LEARN | RESEARCH | INNOVATE

### SAKET ADDRESS

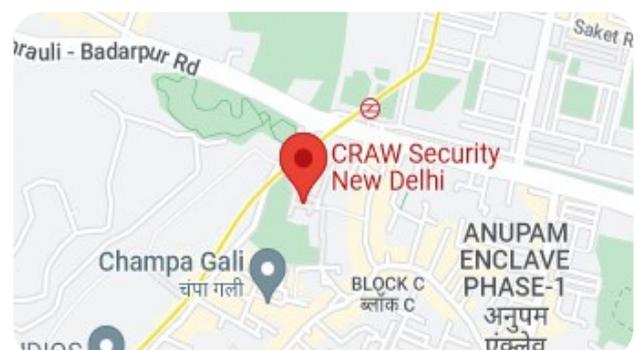
- 1st Floor, Plot no. 4, Lane no. 2, Kehar Singh Estate, Westend Marg, Behind Saket Metro Station, Saidulajab New Delhi - 110030

### LAXMI NAGAR ADDRESS

- R31/ 32, 2nd floor Jandu Tower, Vikas marg, Shakarpur, New Delhi -110092

[www.craw.in](http://www.craw.in)

+91 951 380 5401



@crawsec

