NS3EDU.

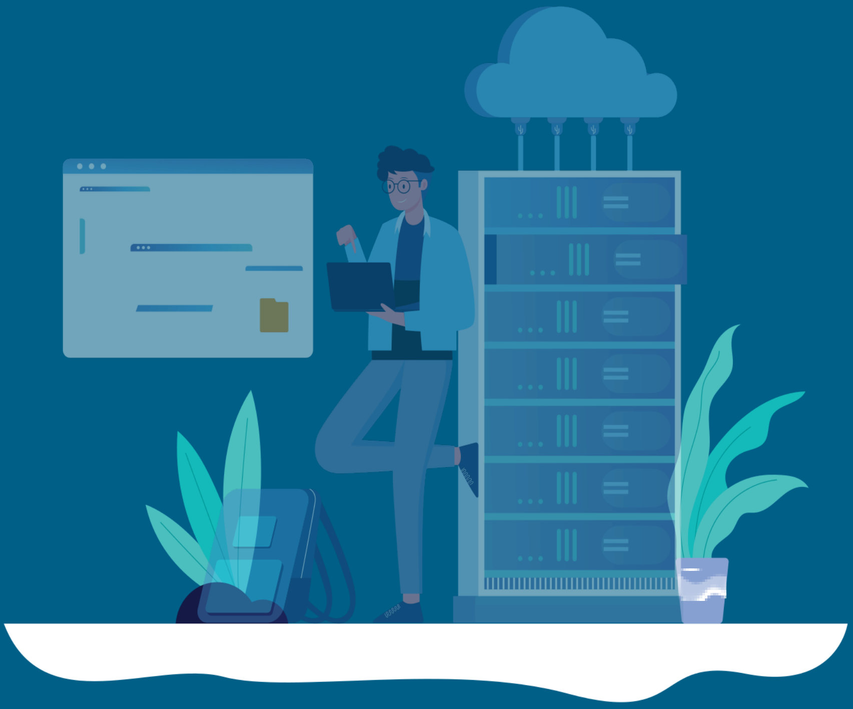
Learn Today Earn Tomorrow

CCNP Security

COURSEOUTLINE

TABLE OF CONTENT

NS3EDU: BRIDGE YOUR IT DREAMS TO REALITY



EMPOWERING CAREER THROUGH KNOWLEDGE

Looking to make it big in the world of IT networking? Look no further than NS3Edu! We help beginners learn the ropes & experienced pros master new skills. Come join us and build your dream career!

MISSION

Themissionof NS3Eduisto

empower our candidates with in-depth knowledge of IT fundamentals along with real-time industry experience and also take 100% responsibility for the placement by making them Industry fit.

VISION

In-depth knowledge + hands-on experience + analytical thinking = placement

CERTIFICATES

Cisco Certified Internetwork Expert

Cisco Certified Internetwork Expert

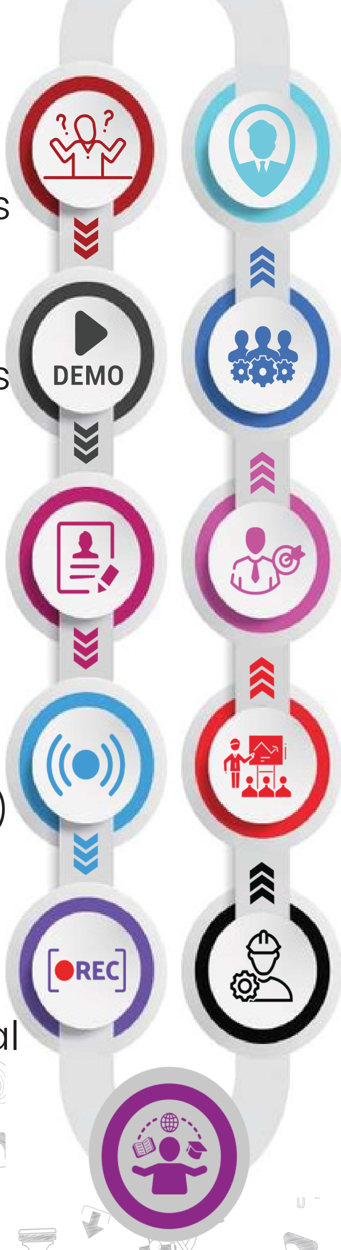
Cisco Certified Internetwork Expert

Cisco Certified Internetwork Expert

NSE Training Institute

NSE 4 Network Security Professional

ROADMAP OF JOB PLACEMENT



Confused in **Different** Career Options

Counselling & **Demo** sessions

Student Enrollment & Induction **session**

Course **Kick** off (Live Classes)

Access to Recorded Sessions, E book & Lab Manual

Course **Completion**

NS3 Tech **Industrial** Exposure

2 Week **Technical Task** Training

Screening by Corporate **HR** & **Tech** Team

Opportunities for **Job** Placement

Qualifies- Job Placement

WHAT MAKES US UNIQUE?

USP'S

Industry Demand & Customized Courses

Smart Classrooms

100% Job Placement

Offline/Online Classroom Mode

Lifetime Membership

Recorded Sessions & Mock Interviews

Employability Enhancement Program

100% Industry Fit

24*7 Lab Access & Real-time Troubleshooting

Certified Trainers & Advance Lab

COURSE OUTLINE

1. ImplementingandOperatingCisco Security Core Technologies

1. Security Concepts

- Explaincommonthreatsagainst on-premises and cloud environments
- On-premises: viruses, trojans, DoS/DDoS attacks, phishing, rootkits, man-in-the-middle attacks, SQL injection, cross-site scripting, malware
- Cloud: data breaches, insecure APIs, DoS/DDoS, compromised credentials
- Compare common security vulnerabilities such as software bugs, weak and or hardcoded passwords, SQL injection, missing encryption, buffer overflow, path traversal, cross-site scripting/forgery
- Describe functions of the cryptography components such as hashing, encryption, PKI, SSL, IPsec, NAT-T IPv4 for IPsec, pre-shared key and certificate based authorization
- Compare site-to-site VPN and remote access VPN deployment types such as sVTI, IPsec, Cryptomap, DMVPN, FLEXVPN including high availability considerations, and AnyConne
- Describe security intelligence authoring, sharing, and consumption
- Explain the role of the endpoint in protecting humans from phishing & social engineering at
- Explain North Bound and South Bound APIs in the SDN architecture
- Explain DNAC APIs for network provisioning, optimization, monitoring, and troubleshooting
- Interpret basic Python scripts used to call Cisco Security appliances APIs

2. Network Security

- Compare networksecuritysolutions that provide intrusion prevention and firewall capabilities
- Describe deployment models of network security solutions and architectures that provide intrusion prevention and firewall capabilities
- Describe the components, capabilities, and benefits of NetFlow and Flexible NetFlow records
- Configure and verify network infrastructure security methods (router, switch, wireless)
- Layer 2 methods (Network segmentation using VLANs and VRF-lite; Layer 2 and port security; DHCP snooping; Dynamic ARP inspection; storm control; PVLANs to segregate network traffic; and defenses against MAC, ARP, VLAN hopping, STP, and DHCP rogue attacks
- Device hardening of network infrastructure security devices (control plane, data plane, management plane, and routing protocol security)
- Implement segmentation, access control policies, AVC, URL filtering, and malware protection
- Implement management options for network security solutions such as intrusion prevention and perimeter security (Single vs. multidevice manager, in-band vs. out-of-band, CDP, DNS, SCP, SFTP, and DHCP security and risks)
- Configure AAA for device and network access (authentication and authorization, TACACS+, RADIUS and RADIUS flows, accounting, and dACL)
- Configure secure network management of perimeter security and infrastructure devices (secure devi management, SNMPv3, views, groups, users, authentication, and encryption, secure logging, and NTP with authentication)
- Configure and verify site-to-site VPN and remote access VPN
- Site-to-site VPN utilizing Cisco routers and IOS

3. Securing the Cloud

- Identify securitysolutions forcloud environments
- Public, private, hybrid, and community clouds
- Cloud service models: SaaS, PaaS, IaaS (NIST 800-145)
- Compare the customer vs. provider security responsibility for the different cloud service models
- Patch management in the cloud
- Security assessment in the cloud
- Cloud-delivered security solutions such as firewall, management, proxy, security intelligence, and CAS
- Describe the concept of DevSecOps (CI/CD pipeline, container orchestration, and security
- Implement application and data security in cloud environments
- Identify security capabilities, deployment models, and policy management to secure the cloud
- Configure cloud logging and monitoring methodologies
- Describe application and workload security concepts

4. Content Security

- Implement trafficredirection and capture methods
- Describe web proxy identity and authentication including transparent user identification
- Compare the components, capabilities, and benefits of local and cloud-based email and web solutio (ESA, CES, WSA)
- Configure and verify web and email security deployment methods to protect on-premises and remot users (inbound and outbound controls and policy management)
- Configure and verify email security features such as SPAM filtering, antimalware filtering, DLP, blacklisting, and email encryption
- Configure and verify secure internet gateway and web security features such as blacklisting, URL filtering, malware scanning, URL categorization, web application filtering, and TLS decryption
- Describe the components, capabilities, and benefits of Cisco Umbrella
- Configure and verify web security

5. Endpoint Protection and Detection

- CompareEndpointProtectionPlatforms(EPP)andEndpoint Detection & Response (EDR) solutions
- Explain antimalware, retrospective security, Indication of Compromise (IOC), antivirus, dynamic file analysis, and endpoint-sourced telemetry
- Configure and verify outbreak control and quarantines to limit infection
- Describe justifications for endpoint-based security
- Describe the value of endpoint device management and asset inventory such as MDM
- Describe the uses and importance of a multifactor authentication (MFA) strategy
- Describe endpoint posture assessment solutions to ensure

6. Secure Network Access, Visibility & Enforcement

- Describe identitymanagementandsecurenetworkaccessconceptssuch as guest services, profiling,
- posture assessment and BYOD
- Configure and verify network access device functionality such as 802.1X, MAB, WebAuth
  Describe network access with CoA
- Describe the benefits of device compliance and application control
- Explain exfiltration techniques (DNS tunneling, HTTPS, email, FTP/SSH/SCP/SFTP, ICMP, Messenger, IRC, NTP)
- Describe the benefits of network telemetry
- Describe the components, capabilities, and benefits of these security products and solutions
- Cisco Stealthwatch
- Cisco Stealthwatch Cloud
- Cisco pxGrid
- Cisco Umbrella Investigate
- Cisco Cognitive Threat Analytics
- Cisco Encrypted Traffic Analytics
- Cisco AnyConnect Network Visibility Module (NVM)

2) Securing Networks with Cisco Firepower

1. Deployment

- Implement NGFW modes- Routed mode and Transparent mode
- Implement NGIPS modes- Passive and Inline
- Implement high availability options- Link redundancy, Active/standby failover and Multi-instance
- Describe IRB configurations

2. Configuration

- Configure systemsettings in Cisco Firepower Management Center
- Configure these policies in Cisco Firepower Management Center- Access control, Intrusion, Malware and file, DNS, Identity, SSL and Prefilter Configure these features using Cisco Firepower
- Management Center- Network discovery, Application detectors (Open AppID), Correlation and Actions Configure objects using Firepower Management Center- Object Management,
- Intrusion Rules Configure devices using Firepower Management Center- Device Management,
- NAT, VPN, QoS, Platform Settings and Certificates

3. Management and Troubleshooting

- TroubleshootwithFMC CLI andGUI
- Configure dashboards and reporting in FMC
- Troubleshoot using packet capture procedures
- Analyze risk and standard reports

4. Integration

- Configure Cisco AMP for Networks in Firepower Management Center
- Configure Cisco AMP for Endpoints in Firepower Management Center
- Implement Threat Intelligence Director for third-party security intelligence feeds
- Describe using Cisco Threat Response for security investigations
- Describe Cisco FMC PxGrid Integration with Cisco Identify Services Engine (ISE)
- Describe Rapid Threat Containment (RTC) functionality within Firepower Management Center

3. Implementing & Configuring Cisco Identity Services Engine

1. Architecture and Deployment

- Configure personas
- Describe deployment options

2. Policy Enforcement

- Configure native ADandLDAP
- Describe identity store options- LDAP, AD, PKI, OTP, Smart Card and Local
- Configure wired/wireless 802.1X network access
- Configure 802.1X phasing deployment- Monitor mode, Low impact and Closed mode
- Configure network access devices
- Implement MAB
- Configure Cisco TrustSec
- Configure policies including authentication and authorization profiles

3. Web Auth and Guest Services

- Configure web authentication
- Configure guest access services
- Configure sponsor and guest portals

4. Profiler

- Implement profiler services
- Implement probes
- Implement CoA
- Configure endpoint identity management

5. BYOD

- Describe Cisco BYOD functionality
- Use cases and requirements
- Solution components
- BYOD flow
- Configure BYOD device on-boarding using internal CA with Cisco switches and Cisco wireless LAN controllers
- Configure certificates for BYOD
- Configure block list/allow list

6. Endpoint Compliance

- Describe endpoint compliance,posture services, and client provisioning
- Configure posture conditions and policy, and client provisioning
- Configure the compliance module
- Configure Cisco ISE posture agents and operational modes
- Describe supplicant, supplicant options, authenticator, and server

7. Network Access Device Administration

- Compare AAAprotocols
- Configure TACACS+ device administration and command authorization

4. Securing Email with Cisco Email Security Applianc

1. Cisco Email Security Appliance Administration

- Configure CiscoEmailSecurityAppliancefeatures
- Hardware performance specifications
- Initial configuration process
- Routing and delivery features
- GUI
- Describe centralized services on a Cisco Content SMA
- Configure mail policies
- Incoming and outgoing messages
- User matching
- Message splintering

2. Spam Control with Talos SenderBase and Antispam

- Control spamwith TalosSenderBaseandAntispam
- Describe graymail management solution
- Configure file reputation filtering and file analysis features
- Implement malicious or undesirable URLs protection
- Describe the bounce verification feature

3. Content and Message Filters

- Describethefunctions and capabilities ofcontent filters
- Create text resources such as content dictionaries, disclaimers, and templates 1) Dictionaries filter rules 2) Text resources management Configure message filters components, rules, processing order and attachment scanning Configure scan
- behavior Configure the Cisco ESA to scan for viruses using Sophos and McAfee
- scanning engines Configure outbreak filters Configure Data Loss Prevention (DLP)

4. LDAP and SMTP Sessions

- ConfigureandverifyLDAPserversandqueries (Queries and Directory Harvest Attack)
- Understand spam quarantine functions
- Authentication for end-users of spam quarantine
- Utilize spam quarantine alias to consolidate queries
- Understand SMTP functionality

1) Email pipeline
2) Sender and recipient domains
3) SMTP session authentication using client certificates
4) SMTP TLS authentication
5) TLS email encryption

5. Email Authentication and Encryption

- Configure DomainkeysandDKIMsigning
- Configure SPF and SIDF
- Configure DMARC verification
- Configure forged email detection
- Configure email encryption
- Describe S/MIME security services and communication encryption with other MTAs
- Manage certificate authorities

6. System Quarantines and Delivery Methods

- Configurequarantine(spam, policy,virus,and outbreak)
- Utilize safelists and blocklists to control email delivery
- Manage messages in local or external spam quarantines
- Configure virtual gateways

5. Securing the Web with Cisco Web Security Applianc

1. Cisco WSA Features

- DescribeCiscoWSAfeaturesand functionality

  1) Proxy service
  2) Cognitive Threat Analytics
  3) Data loss prevention service
  4) Integrated L4TM service
  5) Management tools
- Describe WSA solutions

  1) Cisco Advanced Web Security Reporting
  2) Cisco Content Security Management Appliance
- Integrate Cisco WSA with Splunk
- Integrate Cisco WSA with Cisco ISE
- Troubleshoot data security and external data loss using log files

2. Configuration

- Performinitial configuration tasks on Cisco WSA
- Configure an Acceptable Use Policy
- Configure and verify web proxy features

  1) Explicit proxy functionality
  2) Proxy access logs using CLI
  3) Active directory proxy authentication
- Configure a referrer header to filter web categories

3. Proxy Services

- Compare proxy terms
  1) Explicit proxy vs. transparent proxy
  2) Upstream proxy vs. downstream proxy
- Describe tune caching behavior for safety or performance
- Describe the functions of a Proxy Auto-Configuration (PAC) file
- Describe the SOCKS protocol and the SOCKS proxy services

4. Authentication

- Describe authentication features
  1) Supported authentication protocols
  2) Authentication realms
  3) Supported authentication surrogates supported
  4) Bypassing authentication of problematic agents
  5) Authentication logs for accounting records
  6) Re-authentication
- Configure traffic redirection to Cisco WSA using explicit forward proxy mode
- Describe the FTP proxy authentication
- Troubleshoot authentication issues

5. Decryption Policies to control HTTPs Traffic

- Describe SSLand TLSinspection
- Configure HTTPS capabilities
  1) HTTPS decryption policies
  2) HTTPS proxy function
  3) ACL tags for HTTPS inspection
  4) HTTPS proxy and verify TLS/SSL decryption
  5) Certificate types used for HTTPS decryption
- Configure self-signed and intermediate certificates within SSL/TLS transactions

6. Differentiated Traffic Access Policies and Identification Profiles

- Describe accesspolicies
- Describe identification profiles and authentication
- Troubleshoot using access logs

7. Acceptable Use Control

- Configure URL filtering
- Configure the dynamic content analysis engine
- Configure time-based & traffic volume acceptable use policies and end user notifications
- Configure web application visibility and control (Office 365, third-party feeds)
- Create a corporate global acceptable use policy
- Implement policy trace tool to verify corporate global acceptable use policy
- Configure WSA to inspect archive file types

8. Malware Defense

- Describe anti-malware scanning
- Configure file reputation filtering and file analysis
- Describe Advanced Malware Protection (AMP)
- Describe integration with Cognitive Threat Analytics

9. Reporting and Tracking Web Transactions

- Configure andanalyzeweb trackingreports
- Configure Cisco Advanced Web Security Reporting (AWSR)

1) Basic web usage
2) Custom filters

- Troubleshoot connectivity issues

6. Implementing Secure Solutions with Virtual Private Networks

1. Site-to-site Virtual Private Networks on Routers and Firewalls

- Describe GETVPN
- Describe uses of DMVPN
- Describe uses of FlexVPN

2. Remote Access VPNs

- Implement AnyConnect IKEv2VPNs on ASA and routers
- Implement AnyConnect SSLVPN on ASA
- Implement Clientless SSLVPN on ASA
- Implement Flex VPN on routers

3. Troubleshooting using ASDM and

- CLI
- Troubleshoot IPsec Troubleshoot DMVPN
- Troubleshoot FlexVPN Troubleshoot AnyConnect
- IKEv2 on ASA and routers Troubleshoot SSL VPN
- and Clientless SSLVPN on ASA

4. Secure Communications Architectures

- Describe functional components of GETVPN, FlexVPN,DMVPN, and IPsec for site-to-site VPN solutions
- Describe functional components of FlexVPN, IPsec, and Clientless SSL for remote access VPN solutions
- Recognize VPN technology based on configuration output for site-to-site VPN solutions
- Recognize VPN technology based on configuration output for remote access VPN solutions
- Describe split tunneling requirements for remote access VPN solutions
- Design site-to-site VPN solutions
  1) VPN technology considerations based on functional requirements
  2) High availability considerations
- Design remote access VPN solutions
  1) VPN technology considerations based on functional requirements
  2) High availability considerations
  3) Clientless SSL browser and client considerations and requirements
- Describe Elliptic Curve Cryptography (ECC) algorithms

7. Automating & Programming Cisco Security Solutior

1. Network Programmability Foundation

- Utilizecommonversioncontroloperationswithgit(add,clone, push, commit, diff, branching, and merging conflict)
- Describe characteristics of API styles (REST and RPC)
- Describe the challenges encountered and patterns used when consuming APIs synchronously and asynchronously
- Interpret Python scripts containing data types, functions, classes, conditions, and looping
- Describe the benefits of Python virtual environments
- Explain the benefits of using network configuration tools such as Ansible and Puppet for automating security platforms

2. Network Security

- Describe the eventstreaming capabilities of Firepower Management Center eStreamer API
- Describe the capabilities and components of these APIs
- Firepower (Firepower Management Center and Firepower Device Management)
- ISE
- pxGRID
- Stealthwatch Enterprise
- Implement firewall objects, rules, intrusion policies, and access policies using Firepower Managemen Center API
- Implement firewall objects, rules, intrusion policies, and access policies using Firepower Threat Defen API (also known as Firepower Device Manager API)
- Construct a Python script for pxGrid to retrieve information such as endpoint device type, network po and security telemetry
- Construct API requests using Stealthwatch API
- perform configuration modifications
- generate rich reports

3. Advanced Threat & Endpoint Security

- Describe the capabilities and components of these APIs

  1) Umbrella Investigate APIs

  2) AMP for endpoints APIs

  3) ThreatGRID API
- Construct an Umbrella Investigate API request
- Construct AMP for endpoints API requests for event, computer, and policies
- Construct ThreatGRID APIs request for search, sample feeds, IoC feeds, and threat disposition

4. Cloud, Web and Email Security

- Describethe capabilitiesandcomponentsofthese APIs

  a) Umbrella reporting and enforcement APIs

  b) Stealthwatch cloud APIs

  c) Cisco Security Management Appliance APIs
- Construct Stealthwatch cloud API request for reporting
- Construct an Umbrella Reporting and Enforcement API request
- Construct a report using Cisco Security Management Appliance API request (email and web)

OUR PLACEMENT **PARTNERS**

CISCO | HCL | Microsoft | airtel

Infosys | wipro | STL | DELL

BOSE | aws | velocis | hp | BT | Capgemini | poly | NETGEAR

intel | BOSCH | aruba a Hewlett Packard Enterprise company | IBM | FORTINET | genpact | NTT | ARICENT

SailPoint | paloalto NETWORKS | netskope | CLOUDFLARE | tcs TATA CONSULTANCY SERVICES | Tech Mahindra | CSS CORP | KONVERGE TECHNOLOGIES

YOUR FUTURE OUR RESPONSIBILITY

Free consulting

Get trained with certified trainers

24X7 Lab access

Employability enhancement program

✉ info@ns3edu.com

www.ns3edu.com

☎ +91-9821442746

3rd Floor, B9, Block B,
Old DLF Colony, Sector 14,
Gurugram, Haryana 122007

NETWORK SECURITY | CYBER SECURITY | CLOUD SERVICE | FULL STACK DEVELOPMENT | DIGITAL MARKETING | DATA SCIENCE | AI ML LEARNING