REQUEST FOR PROPOSAL

RFP No. SERC\NB\DOT\1 (Training Program)

As part of the project from Dept. Telecommunication, Govt. of Indi, SERC, IISc is planning to conduct training on Networking and Security for Officials of DoT.

The courses are

1. CCNP_Enterprises
2. CCNP_Security

Interested Vendors (Domestic) with proven experience in conducting Training on Networking & Security are requested to submit proposal. Detailed Syllabus to be covered is given as Annexure with this RFP.

General Information & conditions:

1. The training should be conducted at the premises of
   National Centre for Communication Security
   BSNL Building
   Sampangiram Nagar
   Bangalore
2. No. of participant will be around 15 persons.
3. Quote should be made for Lump sum amount.
4. No advance will be paid.
5. Quotation should be valid for 30 days
6. Any query regarding this can be addressed by email to the undersigned.
7. Two cover systems will be followed. Technical evaluation will identify technically competent vendor followed by opening of the commercial to identify L1.
8. The vendor should have conducted minimum of 3 similar courses for large organizations. Proof should be provided.
9. Turnover of Vendor for the last 3 years should be minimum of Rs 25 lacs per year. Audited statement of account should be submitted.
10. There will be a video conference 12/04/2021 at 3 pm for query and clarification. Link will be shared on that day.
11. The Quotations should be addressed to
    The Chairman
    Supercomputer Education and Research Centre
    Indian Institute of Science
    Bangalore
    Attention : M.R. Muralidharan

12. A hard copy of the quote should be submitted to the following address on or before 5 pm 10th, March 2021 at

Room No. 406, Supercomputer Education and Research Centre
Indian Institute of Science
Bangalore -950012

Proposal should contain the following,

1. Vendors should submit separate technical and commercial quote.
2. Separate Technical and Commercial bid in sealed cover for each program and should put in another larger cover.
3. Technical proposal should contain,

   a) Details of no. of hours allocated for each theory topic and practical.
   b) Purchase order copies of courses conducted should be provided.
   c) Audited statement of account for the last 3 years.
   d) Details of the Faculty, qualification and experience
   e) Copy of the commercial proposal with cost part blanked out.

4. Commercial Quote should indicate Tax component separately.
5. Bidders should be willing to register as suppliers at IISc portal, details will be communicated later.

Important Dates

1. Clarification meeting over VC 12/04/2021 at 3 pm.
2. Last date for submission of Quotation 19/04/2021 at 5pm at SERC

Brief details of the Courses and requirement:

Sl No	Name of the Course	Duration	Trainer Profile	Syllabus
1	CCNP_Enterprise (Consisting of following Four Modules) Mod 1: Core Mod 2: Adv Routing and services Mod 3: SD-WAN Mod 4: Automation	Theory: Not less than 70 hours Hands on Lab Practice: Not less than 70 hours	Trainer shall have relevant CCNP certification and shall have minimum 3 years of teaching experience (OR) Trainer shall have atleast 10 years of experience in teaching Cisco Certification courses.	Refer Annexure
2	CCNP_Security (Consisting of following Four Modules) Mod 1: Core Mod 2: FW and IPS	Theory: Not less than 80 hours Hands on Lab Practice: Not less than 80 hours	Trainer shall have CCNP Security Certification and minimum 3 years of teaching	Refer Annexure

	Mod 3: Web Security Mod 4: VPN		experience. (OR) Trainer shall have atleast 10 years of experience in teaching Cisco Certification courses.	

Other conditions:

1) Face to Face (In person) training at the premises of NCCS, DoT.
2) Lab set up for practical has to be made at NCCS, DoT premises.
3) Hard copies of study materials and lab session have to be issued to participants before the commencement of course.
4) Hands-on lab practice shall include case studies covering the topics taught.
5) Successful bidder shall finalise the training/session plan in consultation with NCCS, DoT.

Name of the course	**Module**	**Objective**	**Outline**	**Lab Outline**
1. CCNP_Enterprise	**Module 1: Core**	Illustrate the hierarchical network design model and architecture using the access, distribution, and core layers Compare and contrast the various hardware and software switching mechanisms and operation, while defining the Ternary Content Addressable Memory (TCAM) and Content Addressable Memory (CAM), along with process switching, fast switching, and Cisco Express Forwarding concepts Troubleshoot Layer 2 connectivity using VLANs and trunking Implementation of redundant switched networks using Spanning Tree Protocol Troubleshooting link aggregation using Etherchannel Describe the features, metrics, and path selection concepts of Enhanced Interior Gateway Routing Protocol (EIGRP) Implementation and optimization of Open Shortest Path First (OSPF)v2 and OSPFv3, including adjacencies, packet types, and areas, summarization, and route filtering for IPv4 and IPv6 Implementing External Border Gateway	Examining Cisco Enterprise Network Architecture Understanding Cisco Switching Paths Implementing Campus LAN Connectivity Building Redundant Switched Topology Implementing Layer 2 Port Aggregation Understanding EIGRP Implementing OSPF Optimizing OSPF Exploring EBGP Implementing Network Redundancy Implementing NAT Introducing Virtualization Protocols and Techniques Understanding Virtual	Investigate the CAM Analyze Cisco Express Forwarding Troubleshoot VLAN and Trunk Issues Tuning Spanning Tree Protocol (STP) and Configuring Rapid Spanning Tree Protocol (RSTP) Configure Multiple Spanning Tree Protocol Troubleshoot EtherChannel Implement Multi-area OSPF Implement OSPF Tuning Apply OSPF Optimization Implement OSPFv3 Configure and Verify Single-Homed EBGP

		Protocol (EBGP) interdomain routing, path selection, and single and dual-homed networking Implementing network redundancy using protocols including Hot Standby Routing Protocol (HSRP) and Virtual Router Redundancy Protocol (VRRP) Implementing internet connectivity within Enterprise using static and dynamic Network Address Translation (NAT) Describe the virtualization technology of servers, switches, and the various network devices and components Implementing overlay technologies such as Virtual Routing and Forwarding (VRF), Generic Routing Encapsulation (GRE), VPN, and Location Identifier Separation Protocol (LISP) Describe the components and concepts of wireless networking including Radio Frequency (RF) and antenna characteristics, and define the specific wireless standards Describe the various wireless deployment models available, include autonomous Access Point (AP) deployments and cloud-based designs within the centralized Cisco Wireless LAN Controller (WLC) architecture Describe wireless roaming and location services Describe how APs communicate with WLCs to obtain software, configurations, and	Private Networks and Interfaces Understanding Wireless Principles Examining Wireless Deployment Options Understanding Wireless Roaming and Location Services Examining Wireless AP Operation Understanding Wireless Client Authentication Troubleshooting Wireless Client Connectivity Introducing Multicast Protocols Introducing QoS Implementing Network Services Using Network Analysis Tools Implementing Infrastructure Security Implementing Secure Access Control	Implementing Hot Standby Routing Protocol (HSRP) Configure Virtual Router Redundancy Protocol (VRRP) Implement NAT Configure and Verify Virtual Routing and Forwarding (VRF) Configure and Verify a Generic Routing Encapsulation (GRE) Tunnel Configure Static Virtual Tunnel Interface (VTI) Point-to-Point Tunnels Configure Wireless Client Authentication in a Centralized Deployment Troubleshoot Wireless Client Connectivity Issues Configure Syslog Configure and Verify Flexible NetFlow Configuring Cisco IOS Embedded Event Manager (EEM)

		centralized management Configure and verify Extensible Authentication Protocol (EAP), WebAuth, and Pre-shared Key (PSK) wireless client authentication on a WLC Troubleshoot wireless client connectivity issues using various available tools Troubleshooting Enterprise networks using services such as Network Time Protocol (NTP), Simple Network Management Protocol (SNMP), Cisco Internetwork Operating System (Cisco IOS®) IP Service Level Agreements (SLAs), NetFlow, and Cisco IOS Embedded Event Manager Explain the use of available network analysis and troubleshooting tools, which include show and debug commands, as well as best practices in troubleshooting Configure secure administrative access for Cisco IOS devices using the Command-Line Interface (CLI) access, Role-Based Access Control (RBAC), Access Control List (ACL), and Secure Shell (SSH), and explore device hardening concepts to secure devices from less secure applications, such as Telnet and HTTP Implement scalable administration using Authentication, Authorization, and Accounting (AAA) and the local database, while exploring the features and benefits Describe the enterprise network security architecture, including the purpose and function of VPNs, content security, logging, endpoint security, personal firewalls, and other	Understanding Enterprise Network Security Architecture Exploring Automation and Assurance Using Cisco DNA Center Examining the Cisco SD-Access Solution Understanding the Working Principles of the Cisco SD-WAN Solution Understanding the Basics of Python Programming Introducing Network Programmability Protocols Introducing APIs in Cisco DNA Center and vManage	Troubleshoot Connectivity and Analyze Traffic with Ping, Traceroute, and Debug Configure and Verify Cisco IP SLAs Configure Standard and Extended ACLs Configure Control Plane Policing Implement Local and Server-Based AAA Writing and Troubleshooting Python Scripts Explore JavaScript Object Notation (JSON) Objects and Scripts in Python Use NETCONF Via SSH Use RESTCONF with Cisco IOS XE Software

		security features Explain the purpose, function, features, and workflow of Cisco DNA Center™ Assurance for Intent-Based Networking, for network visibility, proactive monitoring, and application experience Describe the components and features of the Cisco SD-Access solution, including the nodes, fabric control plane, and data plane, while illustrating the purpose and function of the Virtual Extensible LAN (VXLAN) gateways Define the components and features of Cisco SD-WAN solutions, including the orchestration plane, management plane, control plane, and data plane Describe the concepts, purpose, and features of multicast protocols, including Internet Group Management Protocol (IGMP) v2/v3, Protocol-Independent Multicast (PIM) dense mode/sparse mode, and rendezvous points Describe the concepts and features of Quality of Service (QoS), and describe the need within the enterprise network Explain basic Python components and conditionals with script writing and analysis Describe network programmability protocols such as Network Configuration Protocol (NETCONF) and RESTCONF Describe APIs in Cisco DNA Center and vManage		

	Module 2 Adv Routing and Services	Configure classic Enhanced Interior Gateway Routing Protocol (EIGRP) and named EIGRP for IPv4 and IPv6 Optimize classic EIGRP and named EIGRP for IPv4 and IPv6 Troubleshoot classic EIGRP and named EIGRP for IPv4 and IPv6 Configure Open Shortest Path First (OSPF)v2 and OSPFv3 in IPv4 and IPv6 environments Optimize OSPFv2 and OSPFv3 behavior Troubleshoot OSPFv2 for IPv4 and OSPFv3 for IPv4 and IPv6 Implement route redistribution using filtering mechanisms Troubleshoot redistribution Implement path control using Policy-Based Routing (PBR) and IP Service Level Agreement (SLA) Configure Multiprotocol-Border Gateway Protocol (MP-BGP) in IPv4 and IPv6 environments Optimize MP-BGP in IPv4 and IPv6 environments Troubleshoot MP-BGP for IPv4 and IPv6 Describe the features of Multiprotocol Label Switching (MPLS)	Implementing EIGRP Optimizing EIGRP Troubleshooting EIGRP Implementing OSPF Optimizing OSPF Troubleshooting OSPF Configuring Redistribution Troubleshooting Redistribution Implementing Path Control Implementing Internal Border Gateway Protocol (IBGP) Optimizing BGP Implementing MP-BGP Troubleshooting BGP Exploring MPLS Introducing MPLS L3 VPN Architecture Introducing MPLS L3 VPN Routing	•Configure EIGRP Using Classic Mode and Named Mode for IPv4 and IPv6 •Verify the EIGRP Topology Table •Configure EIGRP Stub Routing, Summarization, and Default Routing •Configure EIGRP Load Balancing and Authentication •Troubleshoot EIGRP Issues •Configure OSPFv3 for IPv4 and IPv6 •Verify the Link-State Database •Configure OSPF Stub Areas and Summarization •Configure OSPF Authentication •Troubleshoot OSPF Issues •Implement Routing Protocol Redistribution •Manipulate Redistribution •Manipulate Redistribution

		Describe the major architectural components of an MPLS VPN Identify the routing and packet forwarding functionalities for MPLS VPNs Explain how packets are forwarded in an MPLS VPN environment Implement Cisco Internetwork Operating System (IOS®) Dynamic Multipoint VPNs (DMVPNs) Implement Dynamic Host Configuration Protocol (DHCP) Describe the tools available to secure the IPV6 first hop Troubleshoot Cisco router security features Troubleshoot infrastructure security and services	Configuring Virtual Routing and Forwarding (VRF)-Lite Implementing DMVPN Implementing DHCP Introducing IPv6 First Hop Security Securing Cisco Routers Troubleshooting Infrastructure Security and Services Troubleshooting with DNA Center Assurance	Using Route Maps •Troubleshoot Redistribution Issues •Implement PBR •Configure IBGP and External Border Gateway Protocol (EBGP) •Implement BGP Path Selection •Configure BGP Advanced Features •Configure BGP Route Reflectors •Configure MP-BGP for IPv4 and IPv6 •Troubleshoot BGP Issues •Configure Routing with VRF-Lite •Implement Cisco IOS DMVPN •Obtain IPv6 Addresses Dynamically •Troubleshoot DHCPv4 and DHCPv6 Issues •Troubleshoot IPv4 and IPv6 Access Control List

				(ACL) Issues •Configure and Verify Unicast Reverse Path Forwarding (uRPF) •Troubleshoot Network Management Protocol Issues: Lab 1 •Troubleshoot Network Management Protocol Issues: Lab 2
	Module 3: SD-WAN	Describe the Cisco SD-WAN overlay network and how modes of operation differ in legacy WAN versus SD-WAN Describe options for SD-WAN cloud and on-premises deployments, as well as how to deploy virtual vEdge and physical cEdge devices with Zero Touch Provisioning (ZTP) and device templates Describe best practices in WAN routing protocols, as well as how to configure and implement transport-side connectivity, service-side routing, interoperability, and redundancy and high availability Describe dynamic routing protocols and best practices in an SD-WAN environment, transport-side connectivity, service-side connectivity, and how redundancy and high availability are achieved in SD-WAN environments Explain how to migrate from legacy WAN to	Cisco SD-WAN Overlay Network Examining Cisco SD-WAN Architecture Cisco SD-WAN Deployment Examining Cisco SD-WAN Deployment Options Deploying Edge Devices Deploying Edge Devices with Zero-Touch Provisioning Using Device Configuration Templates Redundancy, High Availability, and Scalability Cisco SD-WAN Routing	Deploying Cisco SD-WAN Controllers Adding a Branch Using Zero Touch Provisioning (ZTP) Deploying Devices Using Configuration Templates Configuring Controller Affinity Implementing Dynamic Routing Protocols on Service Side Implementing Transport Location (TLOC) Extensions Implementing Control Policies

		Cisco SD-WAN, including typical scenarios for data center and branch Explain how to perform SD-WAN Day 2 operations, such as monitoring, reporting, logging, and upgrading	Options Using Dynamic Routing Providing Site Redundancy and High Availability Configuring Transport-Side Connectivity Cisco SD-WAN Policy Configuration Reviewing Cisco SD-WAN Policy Defining Advanced Control Policies Defining Advanced Data Policies Implementing Application-Aware Routing Implementing Internet Breakouts and Network Address Translation (NAT) Cisco SD-WAN Migration and Interoperability Examining Cisco SD-WAN Hybrid Scenarios Performing a Migration Cisco SD-WAN Management and Operations Performing Day-2	Implementing Data Policies Implementing Application-Aware Routing Implementing Internet Breakouts Migrating Branch Sites Performing an Upgrade

			Operations Performing Upgrades	
	Module 4: Automation	• Describe the various models and APIs of the Cisco IOS-XE platform to perform Day 0 operations, improve troubleshooting methodologies with custom tools, augment the Command-Line Interface (CLI) using scripts, and integrate various workflows using Ansible and Python • Explain the paradigm shift of model-driven telemetry and the building blocks of a working solution • Learn how to use the tools and APIs to automate Cisco DNA infrastructure managed by Cisco DNA Center™ • Demonstrate workflows (configuration, verification, health checking, and monitoring) using Python, Ansible, and Postman • Learn how to automate repetitive tasks using Ansible automation engine. • Understand Cisco SD-WAN solution components, implement a Python library that works with the Cisco SD-WAN APIs to perform configuration, inventory management, and monitoring tasks, and implement reusable Ansible roles to automate provisioning new branch sites on an existing Cisco SD-WAN infrastructure	Introducing Cisco SD-WAN Programmability Building Cisco SD-WAN Automation with Python Building Cisco SD-WAN Automation with Ansible Managing Configuration with Python and Ansible Implementing On-Box Programmability and Automation with Cisco IOS XE Software Implementing Model-Driven Telemetry Day 0 Provisioning with Cisco IOS-XE Automating Cisco Meraki Implementing Meraki Integration APIs Implementing Automation in Enterprise Networks Building Cisco DNA Center Automation with	Automate Networks with Netmiko Postman for REST API Consumption Use Ansible to Configure and Verify Device Configuration Perform Administrative Tasks Using the Cisco SD-WAN API Build, Manage, and Operate Cisco SD-WAN Programmatically Consume SD-WAN APIs Using the Uniform Resource Identifier (URI) Module Build Reports Using Ansible-Viptela Roles Manage Policies with Ansible Use NAPALM to Configure and Verify Device Configuration

		• Manage the tools and APIs to automate Cisco Meraki managed infrastructure and demonstrate workflows (configuration, verification, health checking, monitoring) using Python, Ansible, and Postman • Explore a Python programming language, Python libraries and Python virtual environments and learn how can they be used for automation of network configuration tasks. • Learn about the GIT version control system and its common operations.	Python Automating Operations using Cisco DNA Center Automating APIs and Protocols Network Programmability Foundation	Implement On-Box Programmability and Automation with Cisco IOS XE Software Use Python on Cisco IOS XE Software Implement Streaming Telemetry with Cisco IOS XE Implement Cisco Meraki API Automation Explore Cisco Meraki Integration APIs Explore Cisco Meraki Webhook Alerts Implement ZTP on Cisco IOS-XE with a Custom Python Script Explore Intent APIs for Cisco DNA center (Postman) Build Python Scripts with Cisco DNA Center Intent APIs (Python based) Build Python Scripts with Cisco DNA Center Assurance APIs (Python)

Name of the course	**Module**	**Objective**	**Outline**	**Lab Outline**
2. CCNP_Security(Four Modules)	Module 1: Core	Describe information security concepts and strategies within the network Describe common TCP/IP, network application, and endpoint attacks Describe how various network security technologies work together to guard against attacks Implement access control on Cisco ASA appliance and Cisco Firepower Next-Generation Firewall Describe and implement basic email content security features and	Describing Information Security Concepts Information Security Overview Assets, Vulnerabilities, and Countermeasures Managing Risk Describing Common TCP/IP Attacks* Legacy TCP/IP Vulnerabilities IP Vulnerabilities Internet Control Message Protocol (ICMP) Vulnerabilities Describing Common Network Application Attacks*	Configure Network Settings and NAT on Cisco ASA Configure Cisco ASA Access Control Policies Configure Cisco Firepower NGFW NAT Configure Cisco Firepower NGFW Access Control Policy Configure Cisco Firepower NGFW Discovery and IPS Policy Configure Cisco NGFW Malware and File Policy Configure Listener, Host Access Table (HAT), and Recipient Access Table (RAT) on Cisco Email

		functions provided by Cisco Email Security Appliance Describe and implement web content security features and functions provided by Cisco Web Security Appliance Describe Cisco Umbrella® security capabilities, deployment models, policy management, and Investigate console Introduce VPNs and describe cryptography solutions and algorithms Describe Cisco secure site-to-site connectivity solutions and explain how to deploy Cisco Internetwork Operating System (Cisco IOS®) Virtual Tunnel Interface (VTI)-based point-to-point IPsec VPNs, and point-to-point IPsec VPN on the Cisco ASA and Cisco Firepower Next-Generation Firewall (NGFW) Describe and deploy	Password Attacks Domain Name System (DNS)-Based Attacks DNS Tunneling Describing Common Endpoint Attacks* Buffer Overflow Malware Reconnaissance Attack Describing Network Security Technologies Defense-in-Depth Strategy Defending Across the Attack Continuum Network Segmentation and Virtualization Overview Deploying Cisco ASA Firewall Cisco ASA Deployment Types Cisco ASA Interface Security Levels Cisco ASA Objects and Object Groups Deploying Cisco Firepower Next-	Security Appliance (ESA) Configure Mail Policies Configure 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

		Cisco secure remote access connectivity solutions and describe how to configure 802.1X and Extensible Authentication Protocol (EAP) authentication Provide basic understanding of endpoint security and describe Advanced Malware Protection (AMP) for Endpoints architecture and basic features Examine various defenses on Cisco devices that protect the control and management plane Configure and verify Cisco IOS software Layer 2 and Layer 3 data plane controls Describe Cisco Stealthwatch Enterprise and Stealthwatch Cloud solutions Describe basics of cloud computing and common cloud attacks and how to secure cloud environment	Generation Firewall Cisco Firepower NGFW Deployments Cisco Firepower NGFW Packet Processing and Policies Cisco Firepower NGFW Objects Deploying Email Content Security Cisco Email Content Security Overview Simple Mail Transfer Protocol (SMTP) Overview Email Pipeline Overview Deploying Web Content Security Cisco Web Security Appliance (WSA) Overview Deployment Options Network Users Authentication Deploying Cisco Umbrella* Cisco Umbrella Architecture	Endpoints Perform Endpoint Analysis Using AMP for Endpoints Console Explore File Ransomware Protection by Cisco AMP for Endpoints Console Explore Cisco Stealthwatch Enterprise v6.9.3 Explore Cognitive Threat Analytics (CTA) in Stealthwatch Enterprise v7.0 Explore the Cisco Cloudlock Dashboard and User Security Explore Cisco Cloudlock Application and Data Security Explore Cisco Stealthwatch Cloud Explore Stealthwatch Cloud Alert Settings, Watchlists, and Sensors

			Deploying Cisco Umbrella Cisco Umbrella Roaming Client Explaining VPN Technologies and Cryptography VPN Definition VPN Types Secure Communication and Cryptographic Services Introducing Cisco Secure Site-to-Site VPN Solutions Site-to-Site VPN Topologies IPsec VPN Overview IPsec Static Crypto Maps Deploying 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 Deploying 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 Introducing Cisco Secure Remote Access VPN Solutions Remote Access VPN Components Remote Access VPN Technologies Secure Sockets Layer (SSL) Overview Deploying Remote Access SSL VPNs on the Cisco ASA and Cisco Firepower NGFW Remote Access Configuration Concepts Connection Profiles Group Policies Explaining Cisco Secure Network Access	

			Solutions Cisco Secure Network Access Cisco Secure Network Access Components AAA Role in Cisco Secure Network Access Solution 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 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 Describing Endpoint	

			Security Technologies* Host-Based Personal Firewall Host-Based Anti-Virus Host-Based Intrusion Prevention System Deploying Cisco Advanced Malware Protection (AMP) for Endpoints* Cisco AMP for Endpoints Architecture Cisco AMP for Endpoints Engines Retrospective Security with Cisco AMP Introducing Network Infrastructure Protection* Identifying Network Device Planes Control Plane Security Controls Management Plane Security Controls Deploying Control Plane Security Controls* Infrastructure ACLs	

			Control Plane Policing Control Plane Protection Deploying 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 Deploying Layer 3 Data Plane Security Controls* Infrastructure Antispoofing ACLs Unicast Reverse Path Forwarding IP Source Guard Deploying Management Plane Security Controls* Cisco Secure Management Access Simple Network Management Protocol Version 3 Secure Access to Cisco Devices Deploying Traffic	

			Telemetry Methods* Network Time Protocol Device and Network Events Logging and Export Network Traffic Monitoring Using NetFlow Deploying Cisco Stealthwatch Enterprise* Cisco Stealthwatch Offerings Overview Cisco Stealthwatch Enterprise Required Components Flow Stitching and Deduplication Describing Cloud and Common Cloud Attacks* Evolution of Cloud Computing Cloud Service Models Security Responsibilities in Cloud Securing the Cloud* Cisco Threat-Centric Approach to Network	

			Security Cloud Physical Environment Security Application and Workload Security Deploying Cisco Stealthwatch Cloud* Cisco Stealthwatch Cloud for Public Cloud Monitoring Cisco Stealthwatch Cloud for Private Network Monitoring Cisco Stealthwatch Cloud Operations Describing Software-Defined Networking (SDN*) Software-Defined Networking Concepts Network Programmability and Automation Cisco Platforms and APIs	
	Module 2: FW_IPS	FW: Describe key concepts of NGIPS and NGFW technology and the Cisco Firepower Threat Defense system,	• FW: Cisco Firepower Threat Defense Overview • Examining Firewall and	FW:Initial Device Setup Device Management Configuring High

		and identify deployment scenarios Perform initial Cisco Firepower Threat Defense device configuration and setup tasks Describe how to manage traffic and implement Quality of Service (QoS) using Cisco Firepower Threat Defense Describe how to implement NAT by using Cisco Firepower Threat Defense Perform an initial network discovery, using Cisco Firepower to identify hosts, applications, and services Describe the behavior, usage, and implementation procedure for access control policies Describe the concepts and procedures for implementing security intelligence features Describe Cisco Advanced	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	Availability Migrating from Cisco ASA to Cisco Firepower Threat Defense 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 IPS: Perform Initial Device Setup Perform Device

		Malware Protection (AMP) for Networks and the procedures for implementing file control and advanced malware protection Implement and manage intrusion policies Describe the components and configuration of site-to-site VPN Describe and configure a remote-access SSL VPN that uses Cisco AnyConnect® Describe SSL decryption capabilities and usage IPS: Describe the components of Cisco Firepower Threat Defense and the managed device registration process Detail Next-Generation Firewalls (NGFW) traffic control and configure the Cisco Firepower system for network discovery	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	Management Configure Network Discovery Implement an Access Control Policy Implement Security Intelligence Implement Control and Advanced Malware Protection Implement NGIPS Customize a Network Analysis Policy Perform Analysis Configure Firepower Platform Integration with Splunk Configure Alerting and Event Correlation Perform System Administration Troubleshoot Firepower

		Implement access control policies and describe access control policy advanced features Configure security intelligences features and the Advanced Malware Protection (AMP) for Networks implementation procedure for file control and advanced malware protection Implement and manage intrusion and network analysis policies for NGIPS inspection Describe and demonstrate the detailed analysis techniques and reporting features provided by the Cisco Firepower Management Center Integrate the Cisco Firepower Management Center with an external logging destination Describe and demonstrate the external alerting options available to Cisco Firepower Management	• 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	

		Center and configure a correlation policy Describe key Cisco Firepower Management Center software update and user account management features Identify commonly misconfigured settings within the Cisco Firepower Management Center and use basic commands to troubleshoot a Cisco Firepower Threat Defense device	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 • IPS: • Cisco Firepower Threat Defense Overview • Cisco Firepower NGFW Device Configuration • Cisco Firepower NGFW Traffic Control • Cisco Firepower	

			Discovery • Implementing Access Control Policies • Security Intelligence • File Control and Advanced Malware Protection • Next-Generation Intrusion Prevention Systems • Network Analysis Policies • Detailed Analysis Techniques • Cisco Firepower Platform Integration • Alerting and Correlation Policies • Performing System Administration • Firepower Troubleshooting	
	Module 3: Web Security	• Describe Cisco WSA • Deploy proxy services	• Describing Cisco WSA • Technology Use Case	Configure the Cisco Web Security Appliance

		• Utilize authentication • Describe decryption policies to control HTTPS traffic • Understand differentiated traffic access policies and identification profiles • Enforce acceptable use control settings • Defend against malware • Describe data security and data loss prevention • Perform administration and troubleshooting •	• 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	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 •

			(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	
	Module 4: VPN	Introduce site-to-site VPN options available on Cisco router and firewalls Introduce remote access VPN options available on Cisco router and firewalls Review site-to-site and remote access VPN design options Review troubleshooting processes for various VPN options available on Cisco router and firewalls	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	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