School of Networking
A Unit of Lan n Wan Technology

CCIE HUB

CCIE Security SYLLABUS

EXAM TOPICS – LAB EXAM

TALK TO US :

- +919217518688
- info@cciehub.in

www.cciehub.in

ASA FIREWALL

1. BASICS OF ASA
   - Fundamentals of Firewall
   - Modes of Firewall (L3 Router Mode,
   - & L2 Transparent Mode)
   - Modes of security context
   - Configure Interfaces of ASA
   - Security Level & Range
   - Implicit Rules TCP/UDP & explicit Rules (ACL)
   - Same Security Levels (Inter-zone & intra-zone)
   - ICMP inspection
   - Backup
   - Remote access telnet & SSH
   - (Remote CLI Access)
   - ASDM & https Access (GUI ACCESS)
   - Connection Table
   - Packet Flow Till 8.2 & above 8.3 till now

2. TRANSLATION

- Source / Destination Translation
- Inbound / Outbound Translation
- Pre-nat / Post-nat
- Auto NAT / Manual NAT (only in cisco Firewall ASA & FTD)
- Dynamic NAT
- Xlate table
- Dynamic PAT
- (using extra single Public IP)
- Interface Level Command
- (Outside int ip)
- Static NAT
- Static PAT
- Identity NAT
- Policy NAT/manual nat/dual nat

3. MULTI-CONTEXT

- MULTI-CONTEXT ON ASA

4. HA ON ASA FIREWALL

- Interface Level Redundancy
- ISP Level Redundancy
- Hardware/software Level Active/Standby with DUAL Failover Link
- Hardware Active Active with DUAL Failover Link

5. TRANSPARENT FIREWALL

- CONFIGURING MANAGEMENT ON A TRANSPARENT FW
- CONFIGURE INSIDE & OUTSIDE INTERFACE
- ALLOW DYNAMIC PROTOCOLS EIGRP, RIP, OSPF

6. MODULAR POLICY FRAMEWORK (MPF)

- L3, L4, L7
- Class-map > define protocols
- policy-map > to define action
- service-policy > Applying Policy

7. CLUSTERING

- Port Channels
- Clustering – Interface sapnned Mode

8. IOS ZONE BASED FW

- IOS Zone Based Firewall configuration on Cisco Routers

Firepower Threat Defence FTD

Theory

- Introduction to NGFW Cisco
- Software Overview
- Deliver Options FTD Configuration options
- FirePOWER Management Center
- FirePOWER Defense Manager FTD Initial Setup
- Management-interface Considerations on ASA5500-X
- Reimage from ASA to Firepower Threat Defense
- Firewall Deployment Modes
- Routed Mode
- Transparent Mode
- FTD Security Zones
- Working With FTD Interfaces
- NAT on FTD

- Routing on FTD FTD NGFW Policies
- Malware & File Policy
- Intrusion Policy
- Access Control Policy
- Access Control Policy Rules
- URL Filtering
- Network Discovery
- Custom Application Detector
- SSL Policy
- Rate Limiting/QoS
- Safe Search Management And Events
- Connection Events
- User Identification
- User-based Indications of Compromise
- Packet Tracer and Capture
- URL Lookups
- ISE and SGT tags without Identity
- REST API Reports and Dashboards
- Dashboards
- Reporting Setup FirePOWER Device Manager

Lab

- LAB 1: Firepower Threat Defence Mgmt. IP Configuration
- LAB 2: Firepower Management Centre Configuration for GUI access
- LAB 3: Time Synchronization on FMC
- LAB 4: User & Role configuration ON FMC
- LAB 5: Add FTD on Firepower Management Center
- LAB 6: Configure FTD INSIDE,OUTSIDE & DMZ interfaces
- LAB 7: Migrate devices from one Base policy to another Base Policy
- LAB 8: Configuring Access Control Rule Between INSIDE & DMZ
- LAB 9: Dynamic Routing Protocol RIPv2 configuration
- LAB 10: Dynamic Routing Protocol OSPF configuration

- LAB 11: Redistribution between RIPv2 & OSPF on FTD
- LAB 12: Configure Default Route on FTD at OUTSIDE Interface
- LAB 13: Dynamic NAT on FTD
- LAB 14: Dynamic PAT on FTD
- LAB 15: Geolocation
- LAB 16: Configuring Access Control Rule Between inside & outside
- LAB 17: Application Visibility & Control / AVC / Deep Packet Inspection
- LAB 19: Configuring Static NAT on FTD
- LAB 20: Configuring Static PAT on FTD
- LAB 21: Configuring Site to Site VPN
- LAB 22: HA on FTD Active Standby
- LAB 23: AD integration With Firepower
- LAB 24: ISE integration With Firepower
- LAB 25: Transparent Firewall
- LAB 26: URL Filtering
- LAB 27: Licensing

FirePower NGIPS

- NGIPS Deployment & Modes
- Passive mode
- Inline mode
- NGIPS Policies & Inspection
- Default policy
- Balanced policy
- Connectivity over security
- Security over connectivity
- Rule tuning & rule states (enable/disable, drop, alert)
- Preprocessor tuning
- Network Analysis Policies
- Access control policies with IPS inspection
- File & malware inspection (AMP integration)
- SSL/TLS decryption for IPS inspection
- NGIPS Monitoring & Reporting
- Reconnaissance Attacks

- Denial of Service (DoS/DDoS)
- Application & Web Attacks
- Malware & Exploits
- Evasion Techniques
- Network/Protocol Exploits
- Authentication & Identity Attacks
- Insider Threats & Data Exfiltration
- Cloud-Specific Threats

Security Over Routing & Switching

- Spoofing Attacks L2
- MAC Layer Attacks
- VLAN Attacks & Switch Spoofing attack, CDP Attack
- PVLAN
- NTP Authentication
- DHCP spoofing attack & Snooping
- NetFlow 5,9, Ipfix v10
- Overview of Routing Protocol with Authentication
- Infrastructure ACLs & uRPF L3 Security
- DAI (Dynamic ARP Inspection)

VPN TOPICS

- VPN Theory
- Types of VPN
- Cryptographic Method
- Key types
- IPsec Protocol Deep Dive
- IKEv1 Site to Site Policy Based VPN (Between routers)
- IKEv1 Site-to Site between ASA & Router
- GRE Routing Based VPN without IPsec, with IPsec IKEv1 & SVTI (Site to Site)
- MGRE with NHRP Protocol
- DMVPN PHASE-1, PAHES-2 & PHASE-3, IPsec over DMVPN , Dual HUB
- Overlapping (VPN)
- NAT-T
- GET VPN Using GDOI Protocol

- VRF lite Aware VPN using ikev1
- IKEv2 Theory & Message Exchange
- IKEv2 between Firewalls Policy Base
- IKEv2 Routing Based VPN
- FLEX VPN with DVTI, VTI & SVTI
- SSL Clientless Remote Access VPN
- SSL Fullclient Remote Access VPN (Anyconnect/ Thick Client)
- L2TP (Layer 2 VPN)
- Certificate Authority Based Site to Site VPN

WSA TOPICS

- Intro of WSA
- Explicit forwarding
- Web-proxy configuration (on browser)
- Packet Flow of Web-proxy configuration (Explicit forwarding mode)
- PAC file creation, PAC file hosting
- Transparent redirection (WCCP V2) & Packet Flow
- Service Group ID Details & Uses
- Transparent redirection with exemption
- URL filtering/Custom URL
- Bandwidth usage control (AVC)
- Anti-Malware and Reputation
- HTTPS proxy
- Active Directory Integration
- External User Based Authentication
- Reporting

Designing and Implementing Secure Cloud Access for Users and Endpoints

Theory

- Cisco Security Reference Architecture & SAFE framework
- SASE (Secure Access Service Edge) & Zero Trust Network Access use cases
- Industry security frameworks (NIST, CISA, DISA)
- Identity & device authentication with certificates
- Multi-Factor Authentication (MFA) and Single Sign-On (SAML/OIDC)
- Endpoint posture assessment & security policies

- URL filtering, DNS security, and application control policies
- SaaS application access controls (O365, Salesforce, Workday, etc.
- Remote user access (VPN / application-based secure access)
- Cisco Secure Firewall (ASA/FTD) & Security Edge enforcement
- Cloud attacks & MITRE ATT&CK framework countermeasures
- Microsegmentation & workload protection with Cisco Secure Workload
- Hybrid & multi-cloud (AWS, Azure, GCP) security policies
- Visibility & assurance with Cisco XDR, SIEM, Telemetry, Secure Analytics
- Threat response automation (contain, report, remediate, reinstate)

Lab

- Describe the components of the Cisco Security Reference Architecture
- Threat intelligence
- Security operations toolset
- User/device security
- Network security: cloud edge and on-premises
- Workload, application, and data security
- open-dns cloud infrastructure
- Cisco Umbrella cloud infrastructure
- DNS-layer security
- Cloud Web Security Packet Flow
- URL Filtering
- Custom URL Filtering
- Web-proxy configuration (on browser)
- Bandwidth usage control
- application visibility and control
- Anti-Malware and Reputation
- Report & Event management

IDENTITY SERVICE ENGINE OVERVIEW

Theory

- Understand the business objectives
- Where can ISE help
- ISE deployment models
- ISE deployment options PAN, PSN, MnT, pxGrid
- ISE Personas & Services
- Standalone Deployment
- Cisco Secure Access Control System SNS-36xx appliances
- ISE deployment Models Standalone, Hybrid, Distributed
- Scaling ISE services Agenda & general Considerations
- Standalone redundant
- ISE platform Properties

- Bandwidth and Latency
- Understanding the ISE License Types Evaluation, Base, Plus APEX
- Visibility Data Sources
- Radius Probes
- Types of Dot1x Deployment
- Trust SEC
- Micro Segmentation
- Security Group Tag (SGT)
- Security Group ACL (SGACL)
- IP to SGT Ma*ping (IP-SGT MAP)
- Security Group Tag Exchange
- Protocol (SXP)
- MAC Sec (802.1ae)

Lab

- LAB Setup & ISE installation
- ISE password management policy/ ISE access password policy & Radius Packet
- User Identity Management configuration on ISE for Dot1x authentication
- Network Resources configuration such as Device grouping, Locations & Protocols
- Wired Dot1x Authentication with default Policies
- Dot1x Authentication with Custom Policies & Protocols
- VLAN Assignment with custom authorization policy
- Downloadable ACL (dACL) Post AUTH ACL
- Troubleshooting Feature Of ISE Configuration Validator
- PC Wired MAB Authentication & Profiling, VLAN Assignment, DACL
- Active Directory Integration with ISE 3.1 & sequencing

- Validating Authentication Sever with certificate as a part of authentication Process
- Device Authentication using TACACS+ protocol
- Device EXEC level Authorization using TACACS+ protocol
- Device command level Authorization using ACACS+ protocol
- SSL Full Client Remote Access VPN on ASA &
- Integration with ISE
- Self-signed Certificate Registration & High Availability on ISE

Trust Sec

- SXP Scalable group tag exchange Protocol
- SGACL configuration
- Environment Data Download
- Micro segmentation

WLC & AP

- Wireless AP configuration
- Wireless User management
- Wireless Controller configuration

Email Security Appliance

Theort & Lab

- Cisco Email Security Appliance (ESA) Administration
- Mail Policies (incoming/outgoing message policies, user matching, message splintering)
- Spam Control & Anti-Spam (Talos SenderBase, graymail, reputation filtering, malicious URLs, bounce verification)
- Content & Message Filters (content filters, text resources, message filtering, attachment scanning, virus scanning, outbreak filters, Data Loss Prevention – DLP)
- LDAP & SMTP Sessions (LDAP queries, directory harvest attack prevention, spam quarantine, SMTP pipeline, TLS)
- Email Protocols (SMTP, POP3, IMAP)

- Email Authentication & Encryption (SPF, DKIM, DMARC, S/MIME, forged email detection, certificate authorities)
- System Quarantines & Delivery Methods (spam/policy/virus/outbreak quarantines, safelists/blocklists, virtual gateways)
- Centralized Management & Clustering (cluster configuration, best practices, content security manager)
- Testing & Troubleshooting (mail flow tracing, listener troubleshooting, message tracking, performance, GUI/CLI logging, alerts, hardware/software issues)

DNAC

Theort & Lab

- Introduction of SD-Access Key features & Use Cases
- Introduction to the concept of Software Defined Access
- Control Plane & Data Plane within the SDA Fabric
- Communicating to Shared Services & External Networks
- Overview of Virtual Networks - Macro-Segmentation & Inter-VN Communications
- SDA Components & Roles
- DNAC & ISE Integrations Overview
- Configuring DNAC & ISE Integration
- Configuring Border Switch Initial Configuration
- Configuring Fusion Router Initial Configuration

- DNAC Design - Network Hierarchy – Site & Building
- DNAC Design – Server Configuration – AAA, NTP
- DNAC Design - Device Credentials
- DNAC Design - IP Address Pools
- DNAC Discovery – Discover the Seed Device (Border)
- DNAC Provisioning - Assign Seed Device to HQ
- Configuring the Underlay for Manual Fabric Discovery
- Discovering the Fabric Edge Nodes
- Assigning the Fabric Edge Nodes to HQ Building
- Cleanig up the Fabric Edge and Border Node in preparation for LAN Automation
- DNAC Provisioning – Enable LAN Automation to Discover the Fabric
- Provision the devices to HQ Site
- Reserve the IP Pools for HQ Site for Overlay & Underlay

- Create VNs for the Fabric
- Create the Transit Network (L3HANDOFF)
- Configure Host Onboarding
- Provision the Control-Border Device
- Provision the Edge Device
- Configure the Fusion Router to match the border configuration
- Configure User & Groups on ISE
- Configure Authorization Profiles for the DNAC VNs
- Configure Authorization Policies for the DNAC VNs
- Configure the DHCP Server to provide IP Configuration to Clients
- Verifying Macro Segmentation
- Dot1x Auth
- Create the SGT
- Re-configure ISE Authorization Policies to use SGTs
- Using a default contract to block all communications between SGTs
- Creating a SG ACL – Contract
- Applying and verifying a Custom SG ACL- Contract

- Create VNs for the Fabric
- Create the Transit Network (L3HANDOFF)
- Configure Host Onboarding
- Provision the Control-Border Device
- Provision the Edge Device
- Configure the Fusion Router to match the border configuration
- Configure User & Groups on ISE
- Configure Authorization Profiles for the DNAC VNs
- Configure Authorization Policies for the DNAC VNs
- Configure the DHCP Server to provide IP Configuration to Clients
- Verifying Macro Segmentation
- Dot1x Auth
- Create the SGT
- Re-configure ISE Authorization Policies to use SGTs
- Using a default contract to block all communications between SGTs
- Creating a SG ACL – Contract
- Applying and verifying a Custom SG ACL- Contract

- Create VNs for the Fabric
- Create the Transit Network (L3HANDOFF)
- Configure Host Onboarding
- Provision the Control-Border Device
- Provision the Edge Device
- Configure the Fusion Router to match the border configuration
- Configure User & Groups on ISE
- Configure Authorization Profiles for the DNAC VNs
- Configure Authorization Policies for the DNAC VNs
- Configure the DHCP Server to provide IP Configuration to Clients
- Verifying Macro Segmentation
- Dot1x Auth
- Create the SGT
- Re-configure ISE Authorization Policies to use SGTs
- Using a default contract to block all communications between SGTs
- Creating a SG ACL – Contract
- Applying and verifying a Custom SG ACL- Contract

Designing Cisco Security Infrastructure v1.0 (300-745)

1.0 Secure Infrastructure

- 1.1 Select the security approaches to protect against threats
- 1.1.a Endpoint and client devices (on-network, off-network, and remote)
- 1.1.b Identity such as MFA, passwordless, continuous trust, and identity intelligence
- 1.1.c Email (phishing, ransomware, business email compromise, malware, and spoofing)
- 1.2 Modify the security architecture to address technical requirements
- 1.2.a Hybrid workers
- 1.2.b IoT
- 1.2.c SaaS
- 1.2.d Applications across data center and multi-cloud

- 1.3 Select a VPN and tunneling solution such as SD-WAN, IPsec, MPLS, GRE, DMVPN, and public cloud tunnel options based on business and technical requirements
- 1.4 Select the approach to secure the infrastructure management and control planes
- 1.5 Select the firewall feature or architecture such as traditional firewall, Nextgen firewall,Web Application Firewall, IPS/IDS, distributed firewall, eBPF, and host-based firewallgiven business and technical requirements

2.0 Applications

- 2.1 Select the security solution such as firewalls, SSL offloading, SSL decryption, DLP, and
- endpoint based on application and flow data, to protect an application
- 2.2 Select the design for cloud-native applications, microservices, containers, and serverless architectures to ensure segmentation/microsegmentation

- 2.3 Describe the design policies to address the impacts of emerging technologies such as generative AI, machine learning, and quantum computing

3.0 Risk, Events, and Requirements

- 3.1 Describe how the SOC leverages incident handling and incident response tools
- 3.2 Modify a design to mitigate risk
- 3.3 Modify a security design following an incident
- 3.4 Describe the use of frameworks such as MITRE CAPEC, NIST SP 800-37, and SAFE in the lifecycle of a security design
- 3.5 Match the regulatory and industry compliance document to a given business or technical scenario

4.0 Artificial Intelligence, Automation, and DevSecOps

4.1 Describe the functions, uses, and role of AI in securing network infrastructure

4.2 Select the feature or element required to support automated security architecture/infrastructure such as API tooling, Infrastructure as Code, monitoring, container scanning, security telemetry, alerting, and SOAR

4.3 Select the next step in workflows and pipelines to be implemented by DevSecOps engineers to minimize risk from automated deployments

CCIEHUB

CONTACT US

+91-9217518688 +91-8700479492

info@cciehub.in

www.cciehub.in

33, & 34, C Block, Sector 2,
Noida, Uttar Pradesh 201301