# Lab – CCIE Security

Zetlan Technologies

# Online Course

ZETLAN TECHNOLOGIES
www.zetlantech.com

# Course Modules

## 1. Perimeter Security and Intrusion Prevention

- Deployment modes on Cisco ASA and Cisco FTD
  - Routed
  - Transparent
  - Single
  - Multi-context
  - Multi-instance
- Firewall features on Cisco ASA and FTD
  - NAT
  - Application inspection
  - Traffic zones
  - Policy-based routing
  - Traffic redirection to service modules
  - Identity firewall
- Security features on Cisco IOS/IOS XE
  - Application awareness
  - Zone-based firewall
  - NAT
- Cisco FMC features
  - Alerting
  - Logging
  - Reporting
  - Dynamic objects

# Lab – CCIE Security

## Course Modules

- Cisco NGIPS deployment modes
  - o In-line
  - o Passive
  - o TAP
- Cisco NGFW features
  - o SSL inspection
  - o User identity
  - o Geolocation
  - o AVC
- Detect and mitigate common types of attacks
  - o DoS/DDoS
  - o Evasion techniques
  - o Spoofing
  - o Man-in-the-middle
  - o Botnet
- Clustering & high avlablty features on Cisco ASA & Cisco FTD
- Policies and rules for traffic control on Cisco ASA & Cisco FTD
- Routg protocols securty on Cisco IOS, Cisco ASA,& Cisco FTD
- Network connectivity through Cisco ASA and Cisco FTD
- Correlation and remediation rules on Cisco FMC

# Lab – CCIE Security

## 2. Secure Connectivity and Segmentation

- Cisco AnyConnect client-based, remote-access VPN tchnlgs
- Cisco IOS CA for VPN authentication
- FlexVPN, DMVPN, and IPsec L2L tunnels
- VPN high availability methods
  - Cisco ASA VPN clustering
  - Dual-hub DMVPN deployments
- Infrastructure segmentation methods
  - VLAN
  - PVLAN
  - GRE
  - VRF-Lite
- Micro segmentation with Cisco Trust Sec using SFT and SXP

## 3. Security Infrastructure

- Device hardening techniques & cntrl plane protection methods
  - CoPP
  - IP source routing
  - iACLs
- Management plane protection techniques
  - CPU
  - Memory thresholding
  - Securing device access

# Lab – CCIE Security

- Data plane protection techniques
  - o uRPF
  - o QoS
  - o RTBH
- Layer 2 security techniques
  - o DAI
  - o IPDT
  - o STP security
  - o Port security
  - o DHCP snooping
  - o RA Guard
  - o VACL
- Wireless security technologies
  - o WPA
  - o WPA2
  - o WPA3

o TKIP

o AES

- Monitoring protocols
  - o NetFlow/IPFIX/NSEL
  - o SNMP
  - o SYSLOG
  - o RMON
  - o eStreamer

# Lab – CCIE Security

- Security features to comply with organizational security policies
  - o ISO 27001
  - o RFC 2827
  - o PCI-DSS
- Cisco SAFE model to validate network security design
- Interaction with network devices through APIs usg basc Python
  - o REST API requests and responses
    - ☒ HTTP action verbs, error codes, cookies, headers
    - ☒ JSON or XML payload
    - ☒ Authentication
  - o Data encoding formats
    - ☒ JSON
    - ☒ XML
    - ☒ YAML
- Cisco DNAC Northbound APIs use cases
  - o Authentication and authorization
  - o Network discovery
  - o Network device
  - o Network host

# Lab – CCIE Security

## 4. Identity Management, Infrmtn Exchange, & Access Control

- Cisco ISE scalability using multiple nodes and personas
- Cisco switches and Cisco Wireless LAN Controllers
- Cisco devices for administrative access with Cisco ISE
- AAA for network access with 802.1X and MAB using Cisco ISE
- Guest lifecycle management using Cisco ISE and Cisco WLC
- BYOD on-boarding and network access flows
- Cisco ISE integration with external identity sources
  - o LDAP
  - o AD
  - o External RADIUS
- Provisioning Cisco AnyConnect with Cisco ISE and Cisco ASA
- Posture assessment with Cisco ISE
- Endpoint profiling using Cisco ISE & Cisco network infrastrctr
- Integration of MDM with Cisco ISE
- Certification-based authentication using Cisco ISE
- Authentication methods
  - o EAP Chaining and TEAP
  - o MAR
- Identity mapping on Cisco ASA, Cisco ISE, Cisco WSA, & FTD
- PxGrid integration between security devices Cisco WSA,etc
- Integration of Cisco ISE with multifactor authentication
- Access ctrl & single sign-on using Cisco DUO secrty tchnology
- Cisco IBNS 2.0 (C3PL) for authentication, access control, etc

## 5. Advanced Threat Protection and Content Security

- Cisco AMP for networks, Cisco AMP for endpoints, & AMP
- Detect, analyze, and mitigate malware incidents
- Perform packet capture and analysis using Wireshark, etc
- Cloud security
  - o DNS proxy through Cisco Umbrella virtual appliance
  - o DNS security policies in Cisco Umbrella
  - o RBI policies in Cisco Umbrella
  - o CASB policies in Cisco Umbrella
  - o DLP policies in Cisco Umbrella
- Web filtering, user identification, and Application Visibility etc
- WCCP redirection on Cisco devices
- Email security features
  - o Mail policies
  - o DLP
  - o Quarantine
  - o Authentication
  - o Encryption
- HTTP decryption on Cisco FTD, Cisco WSA, & Umbrella
- Cisco SMA for centralized content security management:

Zetlan Technologies

# LEARN REMOTELY!!

The efficiency of online learning in terms of time management, flexibility, and the ability to access resources anytime, anywhere can be compelling.

## ZETLAN TECHNOLOGIES

www.zetlantech.com

For contact: +91 8680961847
+91 9600579474