Security-All-in-One

Security Appliance 1: Check Point

Module 1: Platforms and Architecture

- Understand meaning of next generation firewall [NGFW].
- Introduction to different firewalls models in the market and market ranking of Checkpoint.
- Parameters for deciding firewall for a network
- Architecture of GAiA OS and firewall platforms covering VM firewalls and hardware firewalls.
- Application of various platforms suiting to different network environments.

Module 2: Checkpoint Fundamentals

- Types of deployments- Standalone and Distributed.
- Installation of GAiA OS in Checkpoint Security Gateway.
- Designing network topology for the course.
- Linking the firewall with the manager.
- Verify SIC establishment between the Security Management Server and the Gateway using SmartDashboard.

Module 3: Pushing Policy and NAT.

- Create rules in SmartDashboard for administrative and internal LAN access.
- Evaluate policies and optimize them for a corporate network.
- Push policies on firewall.
- Configuring static and hide NAT for servers and internal users.
- Verify NAT using SmartView Tracker.

Module 4: Policy Packages and Database Version.

- Optimize policy rule base for corporate network.
- Understand Database Revision Control for policy backup.
- Practical verification of database versions.

Module 5: SmartView Tracker and Monitor.

- Check different types of log files in SmartView Tracker and understand traffic flow and changes on the firewall.
- Use Queries in SmartView Tracker to monitor common network traffic and troubleshoot events.
- Using SmartView Monitor, configure alerts and traffic counters, view a Gateway's status, monitor suspicious activity.

Module 6: Application Control and URL Filtering.

- Layer-7 visibility of checkpoint.
- Understanding how URLs are filtered.
- Configure URL filtering and application control.
- Verification using SmartView Tracker.
- Understanding HTTPS inspection in GAiA and use cases.

Module 7: Identity Awareness

- Use Identity Awareness to provide granular level access to network resources.
- Acquire user information used by the Security Gateway to control access.
- Define Access Roles for use in an Identity Awareness rule.
- Implementing Identity Awareness in the Firewall Rule Base.

Module 8: IPSec Site-to-Site VPN.

- Understanding of IPSec site to site VPNs.
- Configuration and verification of IPSec VPN between checkpoint firewalls.
- Configure and verify IPSec VPN between checkpoint and other vendor firewall.
- Configure a pre-shared secret site-to-site VPN with partner sites.

Module 9: Backup and CLI

- Understand the type of backups available in checkpoint.
- Given network specifications, perform a backup and restore the current Gateway installation from the command line and WebUI.
- Identify files needed to backup, import and export users and add or delete administrators from the command line.
- Remove or fetch a policy from the command line interface.
- Traffic monitoring using CLI.

Security Appliance 2: Palo Alto Firewall

Module 1: Platforms and Architecture

- Understand meaning of next generation firewall [NGFW].
- Introduction to different firewalls models in the market and market ranking of Palo Alto.
- Parameters for deciding firewall for a network
- Architecture of Palo-Alto OS and firewall platforms covering VM firewalls and hardware firewalls.
- Application of various platforms suiting to different network environments.

Module 2: Initial Configuration

- Introduction to WebUI and CLI of Palo Alto.
- Configuration of initial parameters.
- Setting up passwords.
- Setting up of the basic network.

Module 3: Interface Configuration

- Types of interfaces available in firewall.
- Choosing type of interface for particular network design.
- Configuring interfaces depending on network design.

Module 4: Security and NAT Policies

- Types of security policies.
- Configuration and logical design of policies.
- Order of processing the policies by the firewall.
- Understanding and configuration of types of NAT- static, dynamic and PAT.

Module 5: App-ID

- Understand TCP packets and how NGFW firewalls process them.
- Drawbacks faced by traditional firewalls in understanding Layer-7 applications
- Application awareness by Palo Alto
- Configure App-ID in PAN-OS.

Module 6: Basic Content-ID

- What is Content-ID?
- Understanding SP3 architecture of PAN-OS for Content-ID.
- Different profiles available in firewall for network security.
- Application and design of profiles in security policies.

Module 7: URL Filtering

- How URLs are filtered?
- Understanding of URL filtering by PAN-OS.
- Configuration of URL filtering.

Module 8: Decryption

- Working of SSL.
- Why SSL decryption is needed.
- How PAN-OS does SSL decryption.

Module 9: WildFire

- What is wildfire?
- Why is Wildfire so important?
- Understanding of wildfire reports.

Module 10: GlobalProtect and User-ID

- Configure and manage GlobalProtect and User-ID to protect systems that are located outside of the data center perimeter.

Module 11: Site-to-Site VPNs

- Understanding of IPSec site to site VPNs.
- Features offered by Palo Alto to secure IPSec VPNs from intruders.
- Configuration of IPSec VPN.

Module 12: Monitoring and Reporting

- Monitor network traffic using the interactive web interface and firewall reports

Module 13: Active/Passive High Availability

- Benefits of High Availability.
- Need for High Availability.
- Differences between Active/Active and Active/Passive scenarios
- Configuration of high availability in PAN-OS

Security Appliance 3: Fortigate Firewall

Module 1: Routing

- Routing table elements
- How FortiGate matches each packet with a route
- Static routes, policy routes, and dynamic routing
- Equal cost multi-path (ECMP)
- Link health monitor
- Loose and strict reverse path forwarding (RPF)
- Link aggregation
- Loopback interfaces and black hole routes
- WAN link load balancing
- How to diagnose broken routes

Module 2: Virtual Domains VLANs and VLAN tagging

- Virtual Domains (VDOMs)
- Global and per-VDOM resources
- Per-VDOM administrative accounts
- Inter-VDOM Links
- Monitoring per-VDOM resources
- VDOM topologies

Module 3: Transparent Mode

- Transparent mode vs. NAT mode
- Transparent bridging
- Forwarding domains
- Port pairing
- STP configuration
- Monitoring the MAC address table

Module 4: High Availability

- Active-passive vs. active-active mode
- How and HA cluster elects the primary
- Active-active traffic balancing
- HA failover
- Configuration synchronization
- Session synchronization
- Virtual clustering
- Checking the status of a HA cluster

Module 5: Advanced IPSec

- VPN Main vs. aggressive mode negotiations
- Static vs. dynamic peers
- Benefits and cost of VPN technologies
- Dialup VPN configuration
- Redundant VPNs
- Troubleshooting

Module 6: Data Leak Prevention (DLP)

- Why use DLP?
- Files vs. messages
- Sensors and filters
- Document fingerprinting
- Summary vs. full content archiving

Module 7: Diagnostics

- Why do you need to know precisely what is normal?
- Network diagrams
- Monitoring network usage & system resource usage
- Physical layer troubleshooting
- Network layer troubleshooting
- Transport layer troubleshooting

Security Appliance 4: Juniper SRX

Module:1: Junos Security Overview

- Identify concepts, general features and functionality of Junos OS security
  - Junos security architecture
  - Branch vs. high-end platforms
  - Major hardware components of SRX Series services gateways
  - Packet flow
  - Packet-based vs. session-based forwarding

Module:2: Zones

- Identify concepts, benefits and operation of zones
  - Zone types
  - Dependencies
  - Host inbound packet behavior
  - Transit packet behavior

- Demonstrate knowledge of how to configure, monitor and troubleshoot zones
  - Zone configuration steps
  - Hierarchy priority (Inheritance)
  - Monitoring and troubleshooting

Module:3: Security Policies

- Identify the concepts, benefits and operation of security policies
  - Policy types (default policy)
  - Policy components
  - Policy ordering
  - Host inbound traffic examination
  - Transit traffic examination
  - Scheduling
  - Rematching
  - ALGs
  - Address books
  - Applications

- Demonstrate knowledge of how to configure, monitor and troubleshoot security policies
  - Policies
  - ALGs
  - Address books
  - Custom applications
  - Monitoring and troubleshooting

Module:4: Authentication

- Describe the concepts, benefits and operation of firewall user authentication
  - User Firewall
  - User authentication types
  - Authentication server support
  - Client groups

Module:5: Network Address Translation

- Identify the concepts, benefits and operation of NAT
  - NAT types
  - NAT/PAT processing
  - Address persistence
  - NAT proxy ARP
  - Configuration guidelines

- Demonstrate knowledge of how to configure, monitor and troubleshoot NAT
  - NAT configuration steps
  - Monitoring and troubleshooting

Module:6: IPSec VPNs

- Identify the concepts, benefits and operation of IPSec VPNs
  - Secure VPN characteristics and components
  - IPSec tunnel establishment
  - IPSec traffic processing
  - Junos OS IPSec implementation options

- Demonstrate knowledge of how to configure, monitor and troubleshoot IPSec VPNs
  - IPSec VPN configuration steps
  - Monitoring and troubleshooting

Module:7: High Availability

- Identify the concepts, benefits and operation of HA
  - HA features and characteristics
  - Deployment requirements and considerations
  - Chassis cluster characteristics and operation
  - Cluster modes
  - Cluster and node IDs
  - Redundancy groups
  - Cluster interfaces
  - Real-time objects
  - State synchronization
  - Ethernet switching considerations
  - IPSec considerations
  - Manual failover

- Demonstrate knowledge of how to configure, monitor and troubleshoot clustering
  - Cluster preparation
  - Cluster configuration steps
  - Monitoring and troubleshooting

Module:8: Unified Threat Management

- Identify concepts, general features and functionality of UTM
  - Packet flow and processing
  - Design considerations
  - Policy flow
  - Platform support
  - Licensing

- Describe the purpose, configuration and operation of antispam filtering
  - Methods
  - Whitelists vs. blacklists
  - Order of operations
  - Traffic examination

- Configuration steps using the CLI
- Monitoring and troubleshooting

- Describe the purpose, configuration and operation of antivirus protection
  - Scanning methods
  - Antivirus flow process
  - Scanning options and actions
  - Configuration steps using the CLI
  - Monitoring and troubleshooting

- Describe the concepts, benefits and operation of content and Web filtering
  - Filtering features and solutions
  - Configuration steps using the CLI
  - Monitoring and troubleshooting

Security Appliance 5: Cisco ASA

Module 1: Basic of Cisco ASA

- What does a firewall do?
- Security Appliance Overview
- Models and features of Cisco Security Appliances
- Licensing of ASA

Module 2: Initial Configuration

- User Interface
- File Management
- Security Appliance security levels
- ASDM overview and requirements
- Navigating ASDM windows

Module 3: ASA Management Features

- Basic settings and password encryption
- Enabling Management Access Methods
- Authentication, Authorization and Accounting [AAA]
- Privilege levels and Local User Database
- Packet Tracer
- Managing ASA configuration and images

Module 4: ACL and NAT on ASA

- Interface ACL
- Global ACL
- Time Based ACL
- Object Groups
- Static and Dynamic NAT

- Port Address Translation
- NAT Exemption
- Auto NAT and Manual NAT

Module 5 : Routing on ASA

- Static Routing
- EIGRP on ASA
- OSPF on ASA
- ASA Multicast Routing Support

Module 6: Advanced Network Protections

- Blocking and Threat level
- Black list and white list
- Dynamic Database Updates
- DNS Inspection

Module 7: Virtual Private Networks

- Encryption, authentication and hashing algorithms
- IKE Phase 1 and Phase 2
- Configure IPSec Site-to-Site VPNs
- Configure Cisco ANYCONNECT VPN
- Create SSL Web based VPN

Module 8: High Availability

- Implement Stateful ASA Failover
- Active/Standby Mode
- Active/Active Mode
- Dynamic Routing Protocol Failover