Palo Alto Essentials 2 [205]

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

- Integrate the Firewall into Your Management Network
- Register the Firewall
- Activate Licenses and Subscriptions
- Install Content and Software Updates
- Segment Your Network Using Interfaces and Zones
- Set Up a Basic Security Policy
- Assess Network Traffic
- Enable Basic WildFire Forwarding
- Control Access to Web Content
- Enable AutoFocus Threat Intelligence
- Best Practices for Completing the Firewall Deployment

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

- Policy Types
- Security Policy
- Policy Objects
- Security Profiles
- Best Practice Internet Gateway Security Policy
- Enumeration of Rules Within a Rulebase
- Move or Clone a Policy Rule or Object to a Different Virtual System
- Use Tags to Group and Visually Distinguish Objects
- Use an External Dynamic List in Policy
- Register IP Addresses and Tags Dynamically
- Monitor Changes in the Virtual Environment
- CLI Commands for Dynamic IP Addresses and Tags
- Identify Users Connected through a Proxy Server
- Policy-Based Forwarding
- 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.
- Identify how to create security rules to implement App-ID
- Manage Custom or Unknown Applications
- Manage New App-IDs Introduced in Content Releases
- Use Application Objects in Policy
- Applications with Implicit Support
- Application Level Gateways
- Disable the SIP Application-level Gateway (ALG)

Module 6: 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.
- Set Up Data Filtering
- Set Up File Blocking
- Prevent Brute Force Attacks
- Customize the Action and Trigger Conditions for a Brute Force Signature
- Best Practices for Securing Your Network from Layer 4 and Layer 7 Evasions
- Enable Evasion Signatures
- Best Practices for Application and Threat Content Updates
- Prevent Credential Phishing

Module 7: URL Filtering

- How URLs are filtered?
- Understanding of URL filtering by PAN-OS.
- Configuration of URL filtering.
- PAN-DB Categorization
- Determine URL Filtering Policy Requirements
- Configure URL Filtering
- Use an External Dynamic List in a URL Filtering Profile
- Customize the URL Filtering Response Pages
- Allow Password Access to Certain Sites
- Safe Search Enforcement
- Monitor Web Activity
- URL Filtering Use Cases
- Troubleshoot URL Filtering

Module 8: Decryption

- Working of SSL.
- Why SSL decryption is needed
- Define Traffic to Decrypt
- Configure SSL Forward Proxy
- Configure SSL Inbound Inspection
- Configure SSH Proxy
- Decryption Exclusions
- Enable Users to Opt Out of SSL Decryption
- Configure Decryption Port Mirroring
- Temporarily Disable SSL Decryption

Module 9: WildFire

- What is wildfire?
- Why is Wildfire so important?
- Understanding of wildfire reports.
- Log forwarding to Wildfire Servers.

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
- Enable User-ID
- Map Users to Groups
- Map IP Addresses to Users
- Enable User- and Group-Based Policy
- Enable Policy for Users with Multiple Accounts
- Verify the User-ID Configuration
- Deploy User-ID in a Large-Scale Network

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
- Use the Application Command Center
- Use the App Scope Reports
- Take Packet Captures
- Monitor Applications and Threats
- View and Manage Logs
- View and Manage Reports
- Use External Services for Monitoring
- Configure Log Forwarding
- Configure Email Alerts
- Use Syslog for Monitoring
- SNMP Monitoring and Traps
- Forward Logs to an HTTP(S) Destination
- NetFlow Monitoring
- Introduction to AutoFocus

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
- Set Up Active/Passive HA
- Set Up Active/Active HA
- HA Firewall States
- HA Synchronization

Module 14 : Quality of Service

- QoS Overview
- QoS Concepts Configure QoS
- Configure QoS for a Virtual System
- Enforce QoS Based on DSCP Classification
- QoS Use Cases

Module 15 : Panorama

- Overview
- Initial Configuration
- Templates and device groups
- High Availability