Palo Alto training Agenda

1 - Palo Alto Networks Portfolio and Architecture

2 - Configuring Initial Firewall Settings

3 - Managing Firewall Configurations

4 - Managing Firewall Administrator Accounts

5 - Connecting the Firewall to Production Networks with Security Zones

6 - Creating and Managing Security Policy Rules

7 - Creating and Managing NAT Policy Rules

8 - Controlling Application Usage with App-ID

9 - Blocking Known Threats Using Security Profiles

10 - Blocking Inappropriate Web Traffic with URL Filtering

11 - Blocking Unknown Threats with Wildfire

12 - Controlling Access to Network Resources with User-ID

13 - Using Decryption to Block Threats in Encrypted Traffic

14 - Locating Valuable Information Using Logs and Reports

While covering the above operation related task, following common troubleshooting steps must be included:

1. Troubleshooting interface and zone mapping mistakes.

2.Inspecting ARP, routing issues, and interface status.

3.Using CLI and packet capture tools to diagnose dropped or misrouted packets

4. Troubleshoot Panorama connectivity (port, certificate, time sync)

5. How to resolve traffic drops/performance issues by packet captures, and packet-diagnostic logs

6. Inspecting and testing specific policy rules using traffic logs

7. Validate interface configuration like speed, duplex, VLAN tags.

8. Troubleshooting peer device connectivity issue.

Also, some common use cases required for day-to-day operations should be included:

1. Routing Problems & Network Reachability

2. Network connectivity issue due interface misconfigurations, Bonding, LACP configuration, incorrect VLAN assignments, trunk configuration

3.Firewall rules and NAT are properly configured but packet drop on out interface.

4.Application is not responding or slowness in loading due to Packet drop, latency, Network Congestion

5. Genuine applications blocked or misidentified due to App-ID & Content-ID

6. Syslog, SNMP, Log Forwarding and Monitoring Failures

7. Firewall cluster, HA Failover and Redundancy Issues

8. Identifying Misconfigured Firewall Rules, NAT, Zones

Following firewall operation related points need to be discussed during training:

1. How to use ACC tab for generating reports and logs
2. How to create custom report as per the requirement
3. How to take packet captures
4. Brief idea on traffic, threat, configuration, system, unified logs in monitor tab
5. How can we use the session browser for troubleshooting
6. How can we create a decryption policy
7. Guidance on OBJECT < REGION (will VPN can change these IPs)
8. Brief on security profiles
9. How to troubleshoot the log forwarding
10. How to apply scheduler on the policies and how to create a scheduler
11. How to configure interface/ vlan/ aggregate port/ sub interface/ management profile
12. What is the purpose of zone protection and how to configure it
13. What is the purpose of virtual router, how to check the routes on CLI and GUI
14. What is the use of MORE RUN TIME in routers
15. How to use interface management under network tab
16. How to take the backup of firewall
17. How to generate and download the tech support file
18. How to troubleshoot if fw don’t make communication with the updates.paloaltonetworks.com for latest updates, DNS etc
19. How to check if NTP is in sync or not
20. Complete understanding on high availability tab
21. How to create a password profile
22. What is the use of administrator tab for define the roles for user
23. How to handle certificates in the firewall
24. How to configure syslog profile
25. How to carry the log settings
26. How to upgrade the firewall and what precautions should we take
27. What is the use of dynamic updates, how to troubleshoot if this does not update on time.
28. What’s management server? And how do we restart in case of management plane or daemon crash issues.

29. How to disconnect firewall from panorama temporarily so that we can manage firewall locally for a while.
30. How to generate and add certificate to firewall locally?