Palo Alto Interview Questions for Freshers

1. In Palo Alto, identify the various deployment modes?

In Palo Alto, several different deployment modes are observed. The company operates in different modes as per its benefits and suitability. Those include virtual wire mode, tap mode, layer two, and layer three deployment modes. The different deployment modes are leveraged to satisfy different security requirements.

2. Is the firewall at Palo alto stateful?

Yes, the firewall of Palo Alto is stateful. It means that the entire traffic passing through the firewall is matched against the session, and every session is matched against the security policy.

3. In Palo Alto, what is the difference between virtual routers and virtual systems?

The virtual systems in Palo Alto are called logical, multiple firewall instances in a single network of Palo Alto physical firewalls. Every virtual system is an independent and individually managed logical firewall with its traffic kept separate from others. On the contrary virtual routers are used to add another dedicated virtual system in the entire system when required with the other vendors.

4. What is the purpose of Palo Alto Autofocus?

The AutoFocus of Palo Alto is a cloud-based threat intelligence service allowing users to conveniently determine all critical attacks. This way, the user can triage effectively and take the necessary actions without the need for additional IT resources.

5. What are the different failover scenarios?

A failover gets triggered when a monitored metric fails on the active Panorama. There are two significant scenarios when a failover gets triggered;

- The peers in the Panorama cannot communicate with each other, and the active peer is not responding to status polls and health.
- One or more of the destinations specified on the active peer is unreachable.

6. In Palo Alto, what is a U-Turn Nat?

The U-turn NAT refers to the logical path that traffic travels when accessing an internal resource when its external address is resolved. The U-turn NAT is often used in a network where internal users are required to access an internal DMZ server.

7. Explain Active/Passive and Active/Active modes in Palo Alto?

In the active/passive mode, one firewall manages traffic while the other is ready and synchronized to move to the active state if there is a failure. In this mode, both the firewalls share the same settings, and one is responsible for actively managing the traffic until there is a failure.
In the active/active mode, several firewalls are grouped in the form of a cluster and contain multiple active units processing traffic. They share the network load and do DPI as well, together.

8. What is a zone protection profile?

The zone protection profile is one of the best ways to help protect the network from attacks. The attacks can be in the form of reconnaissance attacks, common floods, and similar other packet-based attacks.

9. What is the Application Command Centre (Acc)?

The ACC or Application Command Centre from Panorama offers the users a graphical view of an application that is highly interactive as well. Furthermore, it also provides URL, threat, and data (files and patterns) traversing the Palo Alto network firewalls.

10. What is Waf (Web Application Firewall)?

A WAF or a web application firewall helps protect web applications of all kinds by monitoring and filtering the HTTP traffic between the internet and a web application.

11. What do Ha, Ha1, and Ha2 mean in Palo Alto?

HA is an acronym for high availability port. A dedicated HA link port connects the auxiliary and primary devices physically. It allows the user to place two firewalls in a group and synchronize their configuration.
The HA1 port is used for clear text communication and encrypted communication. On the other hand, the H2 link is used to forward tables, synchronize sessions, IPsec security associations, and the ARP tables.

12. What is Palo Alto's architectural style?

The architectural style of Palo Alto is known as the Queen Anne style. The coastal Northern California community of Palo Alto includes multiple incredible examples from the style of Queen Anne architecture that was built between 1880 and 1905.

13. What exactly is an App-Id?

The app ID allows the users to see the applications available on the network and also learn how they work, their behavioral characteristics, and their relative risk. The applications and application functions can be determined using several techniques, including decryption, application signatures, protocol decoding, and heuristics.

14. How does an App-Id work?

APP ID uses several identification techniques that help determine the exact ID Of the applications traversing your network. It also includes those who try evading detection by masquerading as legitimate traffic, using encryption, or by hopping ports.

15. What are the advantages of panorama in Palo Alto?

Panorama offers centralized, easy-to-implement management features that provide insight into the network-wide traffic and simplify configurations. It is a centralized management system that controls various Palo Alto Network's next-generation firewalls via a web-based interface. It helps the administrators view the device-specific or aggregate application, content, and user data and manage Palo Alto Networks firewalls.

16. What are the possibilities for forwarding log messages on The Palo Alto firewall?

Every firewall stores the log file locally by default. Panorama supports forwarding log messages to a log collector, a cortex data lake, or simultaneously both. One can even use external services for notification, archiving, or analysis by forwarding logs to the services from panorama or firewalls.

17. What is the procedure for adding a license to the Palo Alto firewall?

Go to the web interface of the firewall. Navigate to the device, and license, and click on the activate feature using the Auth code. Then click on the download authorization file and download the autirizationfile.txt file. Then copy this file to a computer that has access to the internet and log in to the support panel.
Click on my VM series auth codes and select the applicable auth code from the list. Now click on register VM. Select the authorization file from the pop-up. Now the registration process is completed, the serial number of the VM series firewall will be attached to the records on the support site.

18. What is Globalprotect in Palo Alto?

GlobalPortect allows organizations to protect the mobile workforce by extending the next-generation security platforms to all users, irrespective of the location. Global protection secures the traffic by applying the platform's capabilities to understand the application's use, associate the traffic with devices and users and enforce security policies with next-generation policies.

19. In Palo Alto, what do you mean by endpoint security?

Endpoint security is the technology necessary to secure various endpoints across organizations like laptops, desktops, servers, and tablets. IoT has created a host of devices that could be compromised, and protection on endpoints should be in place to ensure that the devices are secure.

20. Mention the various linkages used to establish Ha or the Ha Introduction?

The firewall in HA pair uses HA Lin’s to synchronize data and maintain state information. However, some models of the firewall also dedicate the HA ports- Data link (HA2) and Control link (HA1).

21. What are Backup Links?

Backup links provide redundancy for the HA2 and HA1 links. In-brand ports can be used for backup links for HA1 and HA2 connections when dedicated backup links aren’t available.

22. Mention the various port numbers used in Ha?

There are two major types of ports used in HA. One is the TCP port 28769 and 28260 to ensure clear text communication between two ends. Another port number is Port 28, which is used for encrypted communication.

23. What functionalities does Palo Alto Support in Virtual Wire Mode?

A virtual wire interface supports App ID, user ID, content ID, NAT, and decryption

24. Can you tell me which virtualization platform fully supports Palo Alto Network Deployments?

To meet the growing need for inline security across the virtualization use cases and diverse cloud, one can deploy the network across the firewalls on a vast range of public and private cloud computing environments. Such environments include Cisco ACI, OpenStack, Microsoft Public, ENCS, Vmware, etc.

25. Can you find out which command is used to show the maximum size of the log file? Give a quick overview of how panorama handles new logs once the storage limit has been reached.

To determine the maximum size of a log file, run the following command.
show logdb-quota on the system.
When the log storage limit is reached, Panorama automatically deletes old logs to create a way for new entries.
The panorama contains an automated feature that may check and, if necessary, remove the storage restriction.