PCNSE$^{Q\&As}$

Palo Alto Networks Certified Security Engineer (PCNSE) PAN-OS 11.x

Pass Palo Alto Networks PCNSE Exam with 100% Guarantee

QUESTION 1

An administrator has enabled OSPF on a virtual router on the NGFW. OSPF is not adding new routes to the virtual router. Which two options enable the administrator to troubleshoot this issue? (Choose two.)

A. View Runtime Stats in the virtual router.

B. View System logs.

C. Add a redistribution profile to forward as BGP updates.

D. Perform a traffic pcap at the routing stage.

Correct Answer: AB

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CldcCAC

QUESTION 2

A company is using wireless controllers to authenticate users. Which source should be used for User-ID mappings?

A. Syslog

B. XFF headers

C. server monitoring

D. client probing

Correct Answer: A

QUESTION 3

An organization is interested in migrating from their existing web proxy architecture to the Web Proxy feature of their PAN-OS 11.0 firewalls. Currently. HTTP and SSL requests contain the c IP address of the web server and the client browser is redirected to the proxy

Which PAN-OS proxy method should be configured to maintain this type of traffic flow?

A. DNS proxy

B. Explicit proxy

C. SSL forward proxy

D. Transparent proxy

Correct Answer: D

A transparent proxy is a type of web proxy that intercepts and redirects HTTP and HTTPS requests without requiring any configuration on the client browser1. The firewall acts as a gateway between the client and the web server, and performs security checks on the traffic. A transparent proxy can be configured on PAN-OS 11.0 firewalls by performing the following steps1: Enable Web Proxy under Device > Setup > Services Select Transparent Proxy as the Proxy Type Configure a Service Route for Web Proxy Configure SSL/TLS Service Profile for Web Proxy Configure Security Policy Rules for Web Proxy Traffic By configuring a transparent proxy on PAN-OS 11.0 firewalls, an organization can migrate from their existing web proxy architecture without changing their network topology or client settings2. The firewall will maintain the same type of traffic flow as before, where HTTP and HTTPS requests contain the IP address of the web server and the client browser is redirected to the proxy1. Answer A is not correct because DNS proxy is a type of web proxy that intercepts DNS queries from clients and resolves them using an external DNS server3. This type of proxy does not redirect HTTP or HTTPS requests to the firewall.

QUESTION 4

An administrator has two pairs of firewalls within the same subnet. Both pairs of firewalls have been configured to use High Availability mode with Active/Passive. The ARP tables for upstream routes display the same MAC address being shared for some of these firewalls.

What can be configured on one pair of firewalls to modify the MAC addresses so they are no longer in conflict?

A. Configure a floating IP between the firewall pairs.

B. Change the Group IDs in the High Availability settings to be different from the other firewall pair on the same subnet.

C. Change the interface type on the interfaces that have conflicting MAC addresses from L3 to VLAN.

D. On one pair of firewalls, run the CLI command: set network interface vlan arp.

Correct Answer: B

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Cm1OCA S change the Group IDs in the High Availability settings to be different from the other firewall pair on the same subnet. This will prevent the MAC addresses from conflicting and allow the firewalls to properly route traffic. You can also configure a floating IP between the firewall pairs if necessary.

QUESTION 5

Which three external authentication services can the firewall use to authenticate admins into the Palo Alto Networks NGFW without creating administrator account on the firewall? (Choose three.)

A. RADIUS

B. TACACS+

C. Kerberos

D. LDAP

E. SAML

Correct Answer: ABE

According to the Palo Alto Networks documentation1, the firewall can use three external authentication services to authenticate admins into the Palo Alto Networks NGFW without creating administrator accounts on the firewall: RADIUS, TACACS+, and SAML. These services allow the firewall to verify the credentials of admins against an external server and grant them access based on their assigned roles and permissions.

Therefore, the correct answer is A, B, and E.

The other options are not external authentication services that the firewall can use to authenticate admins:

Kerberos: This option is not an external authentication service that the firewall can use to authenticate admins. Kerberos is a protocol that allows users to access network resources using a single sign-on mechanism. The firewall can use

Kerberos to authenticate users for GlobalProtect VPN or Captive Portal, but not for admin access.

LDAP: This option is not an external authentication service that the firewall can use to authenticate admins. LDAP is a protocol that allows querying and modifying directory services over a network. The firewall can use LDAP to retrieve user

and group information from an external server, but not to authenticate admins.

References:

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/authentication/authentication-types/external-authentication-services

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/authentication/authentication-types/kerberos-authentication

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/user-id/map-ip-addresses-to-users/map-ip-addresses-to-users-using-an-ldap-server