PCNSE Q&As

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

Pass Palo Alto Networks PCNSE Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/pcnse.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Palo Alto Networks Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

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

QUESTION 2

When you configure an active/active high availability pair which two links can you use? (Choose two)

A. HA2 backup

B. HA3

C. Console Backup

D. HSCI-C

Correct Answer: AB

QUESTION 3

A web server is hosted in the DMZ, and the server is configured to listen for incoming connections only on TCP port 8080. A Security policy rule allowing access from the Trust zone to the DMZ zone need to be configured to enable we browsing access to the server.

Which application and service need to be configured to allow only cleartext web-browsing traffic to thins server on tcp/8080.

A. application: web-browsing; service: application-default

B. application: web-browsing; service: service-https

C. application: ssl; service: any

D. application: web-browsing; service: (custom with destination TCP port 8080)

Correct Answer: D

If you check in the FW the default port for web-browsing is TCP 80, so you will need a custom app. admin@PA-LAB-01# show predefined application web-browsing web-browsing { category general-internet; subcategory internet-utility; technology browser- based; analysis \\'Web browsing continues to evolve. Initially used to simply view HTML formatted information, web browsers have become the client, through which, users can access new applications that provide functionality far beyond simple information browsing. These applications include web mail, instant messaging, streaming media, web conferencing, blogs, file sharing and other social networkingapplications. Much of the plain web-browsing activities has effectively been overshadowed by all the other applications. } default { port tcp/80; } tunnel-applications http-proxy; risk 4; } [edit]

QUESTION 4

A company requires the firewall to block expired certificates issued by internet-hosted websites. The company plans to implement decryption in the future, but it does not perform SSL Forward Proxy decryption at this time. Without the use of SSL Forward Proxy decryption, how is the firewall still able to identify and block expired certificates issued by internet-hosted websites?

A. By having a Certificate profile that contains the website\\'s Root CA assigned to the respective Security policy rule.

B. By using SSL Forward Proxy to decrypt SSL and TLS handshake communication and the server/client session keys in order to validate a certificate\\'s authenticity and expiration.

C. By using SSL Forward Proxy to decrypt SSL and TLS handshake communication in order to validate a certificates

authenticity and expiration.

D. By having a Decryption profile that blocks sessions with expired certificates in the No Decryption section and assigning it to a No Decrypt policy rule.

Correct Answer: D

https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/decryption/troubleshoot-and-monitor-decryption/decryption-troubleshooting-workflow-examples/troubleshoot-certificate-expiration-issues

QUESTION 5

An ISP manages a Palo Alto Networks firewall with multiple virtual systems for its tenants.

Where on this firewall can the ISP configure unique service routes for different tenants?

A. Setup > Services > Virtual Systems > Set Location > Service Route Configuration > Inherit Global Service Route Configuration

B. Setup > Services > Global > Service Route Configuration > Customize

C. Setup > Services > Virtual Systems > Set Location > Service Route Configuration > Customize

D. Setup > Services > Global > Service Route Configuration > Use Management Interface for all

Correct Answer: C

The best option for the ISP to configure unique service routes for different tenants is to use the Setup > Services > Virtual Systems > Set Location > Service Route Configuration > Customize option on the firewall. This option allows the ISP to customize the service routes for each virtual system that represents a tenant. A service route is the path from the interface to the service on a server, such as DNS, email, or Panorama. By customizing the service routes for each virtual system, the ISP can ensure that each tenant uses a different interface or IP address to access these services. Option A is incorrect because it is used to inherit the global service route configuration for a virtual system, not to customize it. Option B is incorrect because it is used to customize the global service route configuration for all virtual systems, not for a specific one. Option D is incorrect because it is used to use the management interface for all service routes, not to customize them.