Free Questions for PCNSE

Shared by Doyle on 29-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A network security administrator has an environment with multiple forms of authentication. There is a network access control system in place that authenticates and restricts access for wireless users, multiple Windows domain controllers, and an MDM solution for company-provided smartphones. All of these devices have their authentication events logged.

Given the information, what is the best choice for deploying User-ID to ensure maximum coverage?

Options:

A- Captive portal
B- Standalone User-ID agent
C- Syslog listener
D- Agentless User-ID with redistribution

Answer:

C

Explanation:

A syslog listener is the best choice for deploying User-ID to ensure maximum coverage in an environment with multiple forms of authentication. A syslog listener is a feature that enables the firewall or Panorama to receive syslog messages from other systems and parse them for IP address-to-username mappings.A syslog listener can collect user mapping information from a variety of sources, such as network access control systems, domain controllers, MDM solutions, VPN gateways, wireless controllers, proxies, and more2.A syslog listener can also support multiple platforms and operating systems, such as Windows, Linux, macOS, iOS, Android, etc3. Therefore, a syslog listener can provide a comprehensive and flexible solution for User-ID deployment in a large-scale network.Reference:Configure a Syslog Listener for User Mapping,User-ID Agent Deployment Guide, PCNSE Study Guide (page 48)

Question 2

Question Type: MultipleChoice

A firewall administrator is changing a packet capture filter to troubleshoot a specific traffic flow

Upon opening the newly created packet capture, the administrator still sees traffic for the previous fitter What can the administrator do to limit the captured traffic to the newly configured filter?

Options:

A- Command line > debug dataplane packet-diag clear filter-marked-session all
B- In the GLH under Monitor > Packet Capture > Manage Filters under Ingress Interface select an interface
C- Command line> debug dataplane packet-diag clear filter all
D- In the GUI under Monitor > Packet Capture > Manage Filters under the Non-IP field, select 'exclude'

Answer:

C

Question 3

Question Type: MultipleChoice

Which function does the HA4 interface provide when implementing a firewall cluster which contains firewalls configured as active-passive pairs?

Options:

A- Perform packet forwarding to the active-passive peer during session setup and asymmetric traffic flow.
B- Perform synchronization of routes, IPSec security associations, and User-ID information.
C- Perform session cache synchronization for all HA cluster members with the same cluster ID.
D- Perform synchronization of sessions, forwarding tables, and IPSec security associations between firewalls in an HA pair.

Answer:

D

Explanation:

In a High Availability (HA) configuration, particularly in an active-passive setup, it's crucial that the passive unit is kept up to date with the current state of the active unit. This ensures a

seamless transition in the event of a failover. The HA4 interface is dedicated to this synchronization task.

D . Perform synchronization of sessions, forwarding tables, and IPSec security associations between firewalls in an HA pair:

The HA4 interface is responsible for the synchronization of critical stateful information between the active and passive units in an HA pair. This includes session information, ensuring that the passive unit can continue existing sessions without interruption if it needs to become active.

In addition to session information, HA4 also synchronizes forwarding tables, which contain information on how to route packets, and IPSec security associations, which are necessary for maintaining secure VPN tunnels.

This synchronization ensures that both units in an HA pair have identical information regarding the current state of the network, sessions, and security associations, enabling a smooth and immediate transition to the passive unit in case the active unit fails.

Question 4

Question Type: MultipleChoice

Which two components are required to configure certificate-based authentication to the web UI when an administrator needs firewall access on a trusted interface'? (Choose two.)

Options:

A- Server certificate
B- SSL/TLS Service Profile
C- Certificate Profile
D- CA certificate

Answer:

C, D

Question 5

Question Type: MultipleChoice

An organization wants to begin decrypting guest and BYOD traffic.

Which NGFW feature can be used to identify guests and BYOD users, instruct them how to download and install the CA certificate, and clearly notify them that their traffic will be decrypted?

Options:

A- Authentication Portal
B- SSL Decryption profile
C- SSL decryption policy
D- comfort pages

Answer:

A

Explanation:

An authentication portal is a feature that can be used to identify guests and BYOD users, instruct them how to download and install the CA certificate, and clearly notify them that their traffic will be decrypted. An authentication portal is a web page that the firewall displays to users who need to authenticate before accessing the network or the internet. The authentication portal can be customized to include a welcome message, a login prompt, a disclaimer, a certificate download link, and a logout button.The authentication portal can also be configured to use different authentication methods, such as local database, RADIUS, LDAP, Kerberos, or SAML1.By using an authentication portal, the firewall can redirect BYOD users to a web page where they can learn about the decryption policy, download and install the CA certificate, and agree to the terms of use before accessing the network or the internet2.

An SSL decryption profile is not a feature that can be used to identify guests and BYOD users, instruct them how to download and install the CA certificate, and clearly notify them that their traffic will be decrypted. An SSL decryption profile is a set of options that define how the firewall handles SSL/TLS traffic that it decrypts.An SSL decryption profile can include settings such as certificate verification, unsupported protocol handling, session caching, session resumption, algorithm selection, etc3. An SSL decryption profile does not provide any user identification or notification functions.

An SSL decryption policy is not a feature that can be used to identify guests and BYOD users, instruct them how to download and install the CA certificate, and clearly notify them that their traffic will be decrypted. An SSL decryption policy is a set of rules that determine which traffic the firewall decrypts based on various criteria, such as source and destination zones, addresses, users, applications, services, etc.An SSL decryption policy can also specify which type of decryption to apply to the traffic, such as SSL Forward Proxy, SSL Inbound Inspection, or SSH Proxy4. An SSL decryption policy does not provide any user identification or notification functions.

Comfort pages are not a feature that can be used to identify guests and BYOD users, instruct them how to download and install the CA certificate, and clearly notify them that their traffic will be decrypted. Comfort pages are web pages that the firewall displays to users when it blocks or fails to decrypt certain traffic due to security policy or technical reasons.Comfort pages can include information such as the reason for blocking or failing to decrypt the traffic, the URL of the original site, the firewall serial number, etc5. Comfort pages do not provide any user identification or notification functions before decrypting the traffic.

Question 6

Question Type: MultipleChoice

A firewall administrator is configuring an IPSec tunnel between a company's HQ and a remote location. On the HQ firewall, the interface used to terminate the IPSec tunnel has a static IP. At the remote location, the interface used to terminate the IPSec tunnel has a DHCP assigned IP address.

Which two actions are required for this scenario to work? (Choose two.)

Options:

A- On the HQ firewall select peer IP address type FQDN
B- On the remote location firewall select peer IP address type Dynamic
C- On the HQ firewall enable DDNS under the interface used for the IPSec tunnel
D- On the remote location firewall enable DONS under the interface used for the IPSec tunnel

Answer:

A, C

Question 7

Question Type: MultipleChoice

An enterprise Information Security team has deployed policies based on AD groups to restrict user access to critical infrastructure systems. However, a recent phishing campaign against the organization has prompted Information Security to look for more controls that can secure access to critical assets. For users that need to access these systems. Information Security wants to use PAN-OS multi-factor authentication (MFA) integration to enforce MFA.

What should the enterprise do to use PAN-OS MFA?

Options:

A- Configure a Captive Portal authentication policy that uses an authentication sequence.
B- Configure a Captive Portal authentication policy that uses an authentication profile that references a RADIUS profile.
C- Create an authentication profile and assign another authentication factor to be used by a Captive Portal authentication policy.
D- Use a Credential Phishing agent to detect, prevent, and mitigate credential phishing campaigns.

Answer:

C

Question 8

Question Type: MultipleChoice

The decision to upgrade PAN-OS has been approved. The engineer begins the process by upgrading the Panorama servers, but gets an error when attempting the install.

When performing an upgrade on Panorama to PAN-OS. what is the potential cause of a failed install?

Options:

A- Outdated plugins
B- Global Protect agent version
C- Expired certificates
D- Management only mode

Answer:

A

Explanation:

One of the potential causes of a failed install when upgrading Panorama to PAN-OS is having outdated plugins. Plugins are software extensions that enable Panorama to interact with Palo Alto Networks cloud services and third-party services.Plugins have dependencies on specific PAN-OS versions, so they must be updated before or after upgrading Panorama, depending on the plugin compatibility matrix2.If the plugins are not updated accordingly, the upgrade process may fail or

cause issues with Panorama functionality3.Reference:Panorama Plugins Upgrade/Downgrade Considerations,Troubleshoot Your Panorama Upgrade, PCNSE Study Guide (page 54)

Question 9

Question Type: MultipleChoice

A firewall administrator has confirm reports of a website is not displaying as expected, and wants to ensure that decryption is not causing the issue. Which three methods can the administrator use to determine if decryption is causing the website to fail? (Choose three.)

Options:

A- Disable SSL handshake logging
B- Investigate decryption logs of the specific traffic to determine reasons for failure.
C- Temporarily disable SSL decryption for all websites to troubleshoot the issue
D- Create a policy-based 'No Decrypt' rule in the decryption policy to include specific traffic from decryption.
E- Move the policy with action decrypt to the top of the decryption policy rulebase.

Answer:

B, C, D

Question 10

Question Type: MultipleChoice

An engineer is configuring Packet Buffer Protection on ingress zones to protect from single-session DoS attacks.

Which sessions does Packet Buffer Protection apply to?

Options:

A- It applies to existing sessions and is global.
B- It applies to new sessions and is not global.
C- It applies to existing sessions and is not global.
D- It applies to new sessions and is global.

Answer:

A

Explanation:

https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/zone-protection-and-dos-protection/zone-defense/packet-buffer-protection