PaloAltoNetworks.PCNSE.v2023-10-19.q136

Exam Code:	PCNSE
Exam Name:	Palo Alto Networks Certified Network Security Engineer Exam
Certification Provider:	Palo Alto Networks
Free Question Number:	136
Version:	v2023-10-19
# of views:	5004
# of Questions views:	1360
https://www.freepdfdumps.com/PaloAltoNetworks.PCNSE.v2023-10-19.q136.html	

NEW QUESTION: 1
Cortex XDR notifies an administrator about grayware on the endpoints. There are no entries about grayware in any of the logs of the corresponding firewall. Which setting can the administrator configure on the firewall to log grayware verdicts?
A. within the log forwarding profile attached to the Security policy rule
B. within the log settings option in the Device tab
C. in WildFire General Settings, select "Report Grayware Files"
D. in Threat General Settings, select "Report Grayware Files"
Answer: C (LEAVE A REPLY)
Explanation
https://docs.paloaltonetworks.com/wildfire/10-2/wildfire-admin/monitor-wildfire-activity/use-the-firewall-to-mo

NEW QUESTION: 2
A network administrator plans a Prisma Access deployment with three service connections, each with a BGP peering to a CPE. The administrator needs to minimize the BGP configuration and management overhead on on-prem network devices.
What should the administrator implement?
A. target service connection for traffic steering
B. summarized BGP routes before advertising
C. hot potato routing
D. default routing
Answer: B (LEAVE A REPLY)
Explanation
The best way to minimize the BGP configuration and management overhead on on-prem network devices is to summarize BGP routes before advertising them. Route summarization is a technique that reduces the number of routes in a routing table by aggregating multiple routes into

a single route with a less specific prefix. This reduces the size of routing updates and the memory and CPU usage of routers. Prisma Access supports route summarization for service connections and remote network connections that use BGP routing1. You should not implement target service connection for traffic steering, as this is a feature that allows you to select a specific service connection for traffic from a remote network connection or a mobile user based on destination IP address or application. This does not affect the BGP configuration ormanagement on on-prem network devices2. You should not implement hot potato routing, as this is a routing technique that selects the closest exit point to the destination network based on the number of hops or the lowest IGP metric. This does not affect the BGP configuration or management on on-prem network devices3. You should not implement default routing, as this is a routing technique that uses a default route to forward packets to an unknown destination. This does not affect the BGP configuration or management on on-prem network devices, and it may not provide optimal routing for Prisma Access traffic4. References: 1:
https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-panorama-admin/prepare-the-prisma-acc
2:
https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-panorama-admin/prepare-the-prisma-acc
3:
https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-cloud-managed-admin/prisma-access-ser
4:
https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-cloud-managed-admin/prisma-access-ser

NEW QUESTION: 3
Information Security is enforcing group-based policies by using security-event monitoring on Windows User-ID agents for IP-to-User mapping in the network. During the rollout, Information Security identified a gap for users authenticating to their VPN and wireless networks.
Root cause analysis showed that users were authenticating via RADIUS and that authentication events were not captured on the domain controllers that were being monitored Information Security found that authentication events existed on the Identity Management solution (IDM). There did not appear to be direct integration between PAN-OS and the IDM solution How can Information Security extract and learn iP-to-user mapping information from authentication events for VPN and wireless users?
A. Add domain controllers that might be missing to perform security-event monitoring for VPN and wireless users.
B. Configure the integrated User-ID agent on PAN-OS to accept Syslog messages over TLS.
C. Configure the User-ID XML API on PAN-OS firewalls to pull the authentication events directly from the IDM solution

D. Configure the Windows User-ID agents to monitor the VPN concentrators and wireless controllers for IP-to-User mapping.

Answer: C (LEAVE A REPLY)

Explanation

According to the Palo Alto Networks documentation , the User-ID XML API is a feature that allows external systems to send user mapping information to the firewall or Panorama using XML messages over HTTPS. The User-ID XML API can be used to integrate with third-party identity management solutions (IDM) that can provide authentication events for VPN and wireless users. Therefore, the correct answer is C.

The other options are not effective or relevant for extracting and learning IP-to-user mapping information from authentication events for VPN and wireless users:

Add domain controllers that might be missing to perform security-event monitoring for VPN and wireless users: This option would not help because the root cause analysis showed that authentication events were not captured on the domain controllers that were being monitored. Adding more domain controllers would not change this fact, unless they were configured to receive authentication events from RADIUS servers, which is not mentioned in the scenario.

Configure the integrated User-ID agent on PAN-OS to accept Syslog messages over TLS: This option would not help because it assumes that the IDM solution can send Syslog messages over TLS, which is not mentioned in the scenario. Moreover, Syslog messages are less reliable and secure than XML messages for user mapping information.

Configure the Windows User-ID agents to monitor the VPN concentrators and wireless controllers for IP-to-User mapping: This option would not help because it assumes that the VPN concentrators and wireless controllers can provide IP-to-User mapping information, which is not mentioned in the scenario. Moreover, this option would require additional configuration and maintenance of Windows User-ID agents, which may not be feasible or scalable.

References: 1:

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/user-id/map-ip-addresses-to-users/send-user-mappin

NEW QUESTION: 4

Given the following snippet of a WildFire submission log did the end-user get access to the requested information and why or why not?

A. Yes, because the action is set to alert

B. No, because this is an example from a defeated phishing attack

C. No, because the severity is high and the verdict is malicious.

D. Yes, because the action is set to allow.

Answer: (SHOW ANSWER)

Explanation

As long as the action is set to allow, then it will still allow it. Threats that have the ability to become critical but have mitigating factors; for example, they may be difficult to exploit, do not

result in elevated privileges, or do not have a large victim pool. WildFire Submissions log entries with a malicious verdict and an action set to allow are logged as High.
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/monitoring/view-and-manage-logs/log-types-and-s

NEW QUESTION: 5
An engineer is tasked with configuring a Zone Protection profile on the untrust zone.
Which three settings can be configured on a Zone Protection profile? (Choose three.)
A. Ethernet SGT Protection
B. Protocol Protection
C. DoS Protection
D. Reconnaissance Protection
E. Resource Protection
Answer: (SHOW ANSWER)
Explanation
B: Protocol Protection: Protocol protection is used to limit or block traffic that uses certain protocols or application functions. For example, a Zone Protection profile can be configured to block traffic that uses non-standard protocols, such as IP-in-IP, or to limit the number of concurrent sessions for certain protocols, such as SIP.
C: DoS Protection: DoS protection is used to protect against various types of denial-of-service (DoS) attacks, such as SYN floods, UDP floods, ICMP floods, and others. A Zone Protection profile can be configured to limit the rate of traffic for certain protocols or to drop traffic that matches specific patterns, such as malformed packets or packets with invalid headers.
D: Reconnaissance Protection: Reconnaissance protection is used to prevent attackers from gathering information about the network, such as by using port scans or other techniques. A Zone Protection profile can be configured to limit the rate of traffic for certain types of reconnaissance, such as port scans or OS fingerprinting, or to drop traffic that matches specific patterns, such as packets with invalid flags or payloads.

NEW QUESTION: 6
An engineer is creating a template and wants to use variables to standardize the configuration across a large number of devices Which Mo variable types can be defined? (Choose two.)
A. Path group
B. Zone
C. IP netmask
D. FQDN
Answer: C,D (LEAVE A REPLY)
Explanation
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/panorama-web-interface/panorama-tem

NEW QUESTION: 7
Which configuration is backed up using the Scheduled Config Export feature in Panorama?
A. Panorama running configuration
B. Panorama candidate configuration
C. Panorama candidate configuration and candidate configuration of all managed devices
D. Panorama running configuration and running configuration of all managed devices
Answer: D (LEAVE A REPLY)
Explanation
https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/administer-panorama/manage-panorama-and

NEW QUESTION: 8
What are two best practices for incorporating new and modified App-IDs? (Choose two)
A. Configure a security policy rule to allow new App-IDs that might have network-wide impact
B. Study the release notes and install new App-IDs if they are determined to have low impact
C. Perform a Best Practice Assessment to evaluate the impact or the new or modified App-IDs
D. Run the latest PAN-OS version in a supported release tree to have the best performance for the new App-IDs
Answer: A,B (LEAVE A REPLY)
Explanation
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-upgrade/software-and-content-updates/best-practices-for-

NEW QUESTION: 9
An administrator needs to evaluate a recent policy change that was committed and pushed to a firewall device group.
How should the administrator identify the configuration changes?
A. review the configuration logs on the Monitor tab
B. click Preview Changes under Push Scope
C. use Test Policy Match to review the policies in Panorama
D. context-switch to the affected firewall and use the configuration audit tool
Answer: (SHOW ANSWER)
Explanation
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface-help/panorama-web-interface/panorama-com

NEW QUESTION: 10
The manager of the network security team has asked you to help configure the company's Security Profiles according to Palo Alto Networks best practice As part of that effort, the manager has assigned you the Vulnerability Protection profile for the internet gateway firewall.

Which action and packet-capture setting for items of high severity and critical severity best matches Palo Alto Networks best practice?

A. action 'reset-both' and packet capture 'extended-capture'

B. action 'default' and packet capture 'single-packet'

C. action 'reset-both' and packet capture 'single-packet'

D. action 'reset-server' and packet capture 'disable'

Answer: C (LEAVE A REPLY)

Explanation

https://docs.paloaltonetworks.com/best-practices/10-2/internet-gateway-best-practices/best-practice-internet-gate

"Enable extended-capture for critical, high, and medium severity events and single-packet capture for low severity events. "

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/objects/objects-security-profiles-vulner

NEW QUESTION: 11

A bootstrap USB flash drive has been prepared using a Windows workstation to load the initial configuration of a Palo Alto Networks firewall that was previously being used in a lab. The USB flash drive was formatted using file system FAT32 and the initial configuration is stored in a file named init-cfg txt. The firewall is currently running PAN-OS 10.0 and using a lab config The contents of init-cfg txi in the USB flash drive are as follows:

The USB flash drive has been inserted in the firewalls' USB port, and the firewall has been restarted using command:> request resort system Upon restart, the firewall fails to begin the bootstrapping process. The failure is caused because

A. Firewall must be in factory default state or have all private data deleted for bootstrapping

B. The hostname is a required parameter, but it is missing in init-cfg txt

C. The USB must be formatted using the ext3 file system, FAT32 is not supported

D. PANOS version must be 91.x at a minimum but the firewall is running 10.0.x

E. The bootstrap.xml file is a required file but it is missing

Answer: (SHOW ANSWER)

Explanation

https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/firewall-administration/bootstrap-the-firewall/bootst

NEW QUESTION: 12

A firewall administrator is investigating high packet buffer utilization in the company firewall. After looking at the threat logs and seeing many flood attacks coming from a single source that are dropped a by the firewall, the administrator decides to enable packet butter protection to protect against similar attacks.

The administrator enables packet buffer protection globally in the firewall but still sees a high packet buffer utilization rate.

What else should the administrator do to stop packet buffers from being overflowed?
A. Add the default Vulnerability Protection profile to all security rules that allow traffic from outside.
B. Enable packet buffer protection for the affected zones.
C. Add a Zone Protection profile to the affected zones.
D. Apply DOS profile to security rules allow traffic from outside.
Answer: B (LEAVE A REPLY)
Explanation
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/zone-protection-and-dos-protection/zone-defense/p

NEW QUESTION: 13
Which steps should an engineer take to forward system logs to email?
A. Create a new email profile under Device > server profiles; then navigate to Objects > Log Forwarding profile > set log type to system and the add email profile.
B. Enable log forwarding under the email profile in the Objects tab.
C. Create a new email profile under Device > server profiles: then navigate to Device > Log Settings > System and add the email profile under email.
D. Enable log forwarding under the email profile in the Device tab.
Answer: C (LEAVE A REPLY)
Explanation
An email profile defines the email server and sender address for sending email notifications from the firewall or Panorama. To forward system logs to email, the engineer needs to create a new email profile under Device
> Server Profiles > Email and configure the required settings, such as SMTP server, sender email address, and recipient email address. Then, the engineer needs to navigate to Device > Log Settings > System and select the email profile under Email for each severity level of system logs that need to be forwarded. Enabling log forwarding under the email profile in the Objects tab or in the Device tab is not possible, as log forwarding profiles are configured under Objects > Log Forwarding. Log forwarding profiles are used for forwarding threat, traffic, URL filtering, data filtering, HIP match, configuration, and correlation logs, not system logs.
References:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/monitoring/configure-email-alerts
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/monitoring/configure-log-forwarding

NEW QUESTION: 14
How can Panorama help with troubleshooting problems such as high CPU or resource exhaustion on a managed firewall?
A. Firewalls send SNMP traps to Panorama when resource exhaustion is detected Panorama generates a system log and can send email alerts

B. Panorama provides visibility into all the system and traffic logs received from firewalls it does not offer any ability to see or monitor resource utilization on managed firewalls
C. Panorama monitors all firewalls using SNMP It generates a system log and can send email alerts when resource exhaustion is detected on a managed firewall
D. Panorama provides information about system resources of the managed devices in the Managed Devices
> Health menu
Answer: D (LEAVE A REPLY)
Explanation
Panorama can help with troubleshooting problems such as high CPU or resource exhaustion on a managed firewall by providing information about system resources of the managed devices in the Managed Devices > Health menu. This is explained in the Palo Alto Networks PCNSE Study Guide in Chapter 13: Panorama, under the section "Monitoring Managed Firewalls with Panorama":
"The Panorama web interface provides information about the system resources of the managed devices. In the Managed Devices > Health menu, you can view the CPU, memory, and disk usage of each managed device.
This information can help you troubleshoot problems such as high CPU or resource exhaustion on a managed firewall."

NEW QUESTION: 15
Where can an administrator see both the management-plane and data-plane CPU utilization in the WebUI?
A. System Resources widget
B. System Logs widget
C. Session Browser
D. General Information widget
Answer: A (LEAVE A REPLY)
Explanation
The System Resources widget of the Exadata WebUI, displays a real-time overview of the various resources like CPU, Memory, and I/O usage across the entire Exadata Database Machine. It shows the usage of both management-plane and data-plane CPU utilization.
System Resources Widget Displays the Management CPU usage, Data Plane usage, and the Session Count (the number of sessions established through the firewall or Panorama).
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/dashboard/dashboard-widgets.html

NEW QUESTION: 16
A company with already deployed Palo Alto firewalls has purchased their first Panorama server. The security team has already configured all firewalls with the Panorama IP address and added

all the firewall serial numbers in Panorama. What are the next steps to migrate configuration from the firewalls to Panorama?

A. Use API calls to retrieve the configuration directly from the managed devices

B. Export Named Configuration Snapshot on each firewall followed by Import Named Configuration Snapshot in Panorama

C. import Device Configuration to Panorama followed by Export or Push Device Config Bundle

D. Use the Firewall Migration plugin to retrieve the configuration directly from the managed devices

Answer: C (LEAVE A REPLY)

Explanation

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CloRCAS

NEW QUESTION: 17

A firewall administrator notices that many Host Sweep scan attacks are being allowed through the firewall sourced from the outside zone. What should the firewall administrator do to mitigate this type of attack?

A. Create a DOS Protection profile with SYN Flood protection enabled and apply it to all rules allowing traffic from the outside zone

B. Enable packet buffer protection in the outside zone.

C. Create a Security rule to deny all ICMP traffic from the outside zone.

D. Create a Zone Protection profile, enable reconnaissance protection, set action to Block, and apply it to the outside zone.

Answer: D (LEAVE A REPLY)

Explanation

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

NEW QUESTION: 18

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
Answer: A,B,E (LEAVE A REPLY)
Explanation
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 admins3.
References: 1:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/authentication/authentication-types/external-authent
2:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/authentication/authentication-types/kerberos-authen
3:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/user-id/map-ip-addresses-to-users/map-ip-addresses

NEW QUESTION: 19
An administrator needs to build Security rules in a Device Group that allow traffic to specific users and groups defined in Active Directory What must be configured in order to select users and groups for those rules from Panorama?
A. The Security rules must be targeted to a firewall in the device group and have Group Mapping configured
B. A master device with Group Mapping configured must be set in the device group where the Security rules are configured
C. User-ID Redistribution must be configured on Panorama to ensure that all firewalls have the same mappings

D. A User-ID Certificate profile must be configured on Panorama

Answer: (SHOW ANSWER)

Explanation

https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/panorama-web-interface/panorama-de

NEW QUESTION: 20

An auditor is evaluating the configuration of Panorama and notices a discrep-ancy between the Panorama template and the local firewall configuration.

When overriding the firewall configuration pushed from Panorama, what should you consider?

A. The modification will not be visible in Panorama.

B. The firewall template will show that it is out of sync within Panorama.

C. Panorama will update the template with the overridden value.

D. Only Panorama can revert the override.

Answer: A (LEAVE A REPLY)

Explanation

When overriding the firewall configuration pushed from Panorama, the modification will not be visible in Panorama. The firewall will show an override icon next to the modified setting and will display a warning message that the local configuration differs from Panorama. The override icon will also appear on Panorama next to the firewall name in the Device Groups and Templates tabs1. The other options are not correct. The firewall template will not show that it is out of sync within Panorama, because the template itself is not modified. Panorama will not update the template with the overridden value, because the template is read-only on the firewall. The override can be reverted either from Panorama or from the firewall2. References: 1: https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/firewall-administration/manage-configuration/over

2: https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/firewall-administration/manage-configuration/reve

NEW QUESTION: 21

Which two actions would be part of an automatic solution that would block sites with untrusted certificates without enabling SSL Forward Proxy? (Choose two.)

A. Create a no-decrypt Decryption Policy rule.

B. Configure an EDL to pull IP addresses of known sites resolved from a CRL.

C. Create a Dynamic Address Group for untrusted sites

D. Create a Security Policy rule with vulnerability Security Profile attached.

E. Enable the "Block sessions with untrusted issuers" setting.

Answer: A,D (LEAVE A REPLY)

Explanation

You can use the No Decryption tab to enable settings to block traffic that is matched to a decryption policy configured with the No Decrypt action (Policies > Decryption > Action). Use these options to control server certificates for the session, though the firewall does not decrypt and inspect the session traffic.
https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-web-interface-help/objects/objects-decryption-profile

NEW QUESTION: 22
You have upgraded your Panorama and Log Collectors lo 10.2 x. Before upgrading your firewalls using Panorama, what do you need do?
A. Refresh your licenses with Palo Alto Network Support - Panorama/Licenses/Retrieve License Keys from License Server.
B. Re-associate the firewalls in Panorama/Managed Devices/Summary.
C. Commit and Push the configurations to the firewalls.
D. Refresh the Mastor Key in Panorama/Master Key and Diagnostic
Answer: C (LEAVE A REPLY)
Explanation
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-upgrade/upgrade-pan-os/upgrade-the-firewall-pan-os/upg

NEW QUESTION: 23
The UDP-4501 protocol-port is used between which two GlobalProtect components?
A. GlobalProtect app and GlobalProtect gateway
B. GlobalProtect portal and GlobalProtect gateway
C. GlobalProtect app and GlobalProtect satellite
D. GlobalProtect app and GlobalProtect portal
Answer: A (LEAVE A REPLY)
Explanation
UDP 4501 Used for IPSec tunnel connections between GlobalProtect apps and gateways.
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/firewall-administration/reference-port-number-usag

NEW QUESTION: 24
An administrator is seeing one of the firewalls in a HA active/passive pair moved to 'suspended" state due to Non-functional loop. Which three actions will help the administrator troubleshool this issue? (Choose three.)
A. Use the CLI command show high-availability flap-statistics
B. Check the HA Link Monitoring interface cables.
C. Check the High Availability > Link and Path Monitoring settings.
D. Check High Availability > Active/Passive Settings > Passive Link State
E. Check the High Availability > HA Communications > Packet Forwarding settings.

Answer: (SHOW ANSWER)

Explanation

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClhJCAS&lang=ja&refURL=

NEW QUESTION: 25

Refer to the exhibit.

Review the screenshots and consider the following information:

* FW-1 is assigned to the FW-1_DG device group, and FW-2 is assigned to OFFICE_FW_DG.
* There are no objects configured in REGIONAL_DG and OFFICE_FW_DG device groups.

Which IP address will be pushed to the firewalls inside Address Object Server-1?

A. Server-1 on FW-1 will have IP 1.1.1.1. Server-1 will not be pushed to FW-2.

B. Server-1 on FW-1 will have IP 3.3.3.3. Server-1 will not be pushed to FW-2.

C. Server-1 on FW-1 will have IP 2.2.2.2. Server-1 will not be pushed to FW-2.

D. Server-1 on FW-1 will have IP 4.4.4.4. Server-1 on FW-2 will have IP 1.1.1.1.

Answer: D (LEAVE A REPLY)

Explanation

FW-1 will get the value from FW-DG1 while FW-2 will get the value from the Shared DG since no values are present in its parent DGs.

https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/manage-firewalls/manage-device-groups/man

NEW QUESTION: 26

An administrator needs to gather information about the firewall CPU utiliza-tion on both the management plane and the data plane.

Where does the administrator view the desired data?

A. Application Command and Control Center

B. Monitor > Utilization

C. Support > Resources

D. System Resources Widget on the Dashboard

Answer: D (LEAVE A REPLY)

Explanation

The System Resources widget on the Dashboard in the WebUI shows both the management plane and data plane CPU utilization as well as other system resources such as memory, disk, and session1. The other options do not show both the management plane and data plane CPU utilization. The Application Command and Control Center (ACC) shows the network activity and application usage based on traffic logs2. The Monitor > Utilization page shows the interface utilization and packet buffer utilization3. The Support > Resources page shows the system resources for Panorama only4. References: 1: https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/dashboard/dashboard-widgets 2:

https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/acc/acc-overview 3: https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/monitor/monitor-utilization 4: https://docs.paloaltonetworks.com/panorama/10-2/panorama-web-interface-help/support/support-resources

NEW QUESTION: 27
Which configuration task is best for reducing load on the management plane?
A. Disable logging on the default deny rule
B. Enable session logging at start
C. Disable pre-defined reports
D. Set the URL filtering action to send alerts
Answer: C (LEAVE A REPLY)
Explanation
Report generation can also consume considerable resources, while some pre-defined reports may not be useful to the organization, or they've been replaced by a custom report. These pre-defined reports can be disabled from Device > Setup > Logging and Reporting Settings https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClSvCAK

NEW QUESTION: 28
The following objects and policies are defined in a device group hierarchy
A)
B)
C)
Address Objects
-Shared Address 1
-Branch Address2
Policies -Shared Polic1
l -Branch Policyl
D)
Address Objects -Shared Addressl -Shared Address2 -Branch Addressl Policies -Shared Policyl -Shared Policy2 -Branch Policyl
A. Option A
B. Option D
C. Option C
D. Option B
Answer: (SHOW ANSWER)

NEW QUESTION: 29

In an existing deployment, an administrator with numerous firewalls and Panorama does not see any WildFire logs in Panorama. Each firewall has an active WildFire subscription On each firewall. WildFire togs are available.
This issue is occurring because forwarding of which type of logs from the firewalls to Panorama is missing?
A. Threat logs
B. Traffic togs
C. System logs
D. WildFire logs
Answer: A (LEAVE A REPLY)
Explanation
Access to the WildFire logs from Panorama requires the following: a WildFire subscription, a File Blocking profile that is attached to a Security rule, and Threat log forwarding to Panorama.
https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/monitor-network-activity/use-case-respond-t

NEW QUESTION: 30
In a Panorama template which three types of objects are configurable? (Choose three)
A. certificate profiles
B. HIP objects
C. QoS profiles
D. security profiles
E. interface management profiles
Answer: (SHOW ANSWER)
Explanation
https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/manage-firewalls/use-case-configure-firewall

NEW QUESTION: 31
An engineer is pushing configuration from Panorama lo a managed firewall.
What happens when the pushed Panorama configuration has Address Object names that duplicate the Address Objects already configured on the firewall?
A. The firewall rejects the pushed configuration, and the commit fails.
B. The firewall renames the duplicate local objects with "-1" at the end signifying they are clones; it will update the references to the objects accordingly and fully commit the pushed configuration.
C. The firewall fully commits all of the pushed configuration and overwrites its locally configured objects
D. The firewall ignores only the pushed objects that have the same name as the locally configured objects, and it will commit the rest of the pushed configuration.
Answer: A (LEAVE A REPLY)
Explanation

it fails the commit should the local FW has the same object as the Panorama. on this docs it say "shared"
https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/manage-firewalls/transition-a-firewall-to-pano

NEW QUESTION: 32
Which three multi-factor authentication methods can be used to authenticate access to the firewall? (Choose three.)
A. One-time password
B. User certificate
C. Voice
D. SMS
E. Fingerprint
Answer: A,B,D (LEAVE A REPLY)
Explanation
These three methods are examples of multi-factor authentication that can be used to authenticate access to the firewall. A one-time password is a code that is generated by an authentication app or sent by email or SMS and expires after a single use. A user certificate is a digital credential that is issued by a trusted authority and stored on the user's device. SMS is a text message that is sent to the user's phone number with a code or a link to verify their identity1. The other methods are not supported by the firewall for multi-factor authentication. Voice and fingerprint are biometric factors that require special hardware and software to capture and analyze. References:
1:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/authentication/configure-multi-factor-authenticatio

NEW QUESTION: 33
An engineer troubleshooting a VPN issue needs to manually initiate a VPN tunnel from the CLI. Which CLI command can the engineer use?
A. test vpn flow
B. test vpn Ike-sa
C. test vpn tunnel

D. test vpn gateway

Answer: D (LEAVE A REPLY)

Explanation

The engineer can use the test vpn gateway CLI command to manually initiate a VPN tunnel from the CLI.

This command allows the engineer to specify the name of the VPN gateway and the IP address of the peer to initiate an IKE negotiation and establish a VPN tunnel. Option A is incorrect because test vpn flow is not a valid CLI command. Option B is incorrect because test vpn ike-sa is a CLI command that displays information about the IKE security associations, not initiates a VPN tunnel. Option C is incorrect because test vpn tunnel is a CLI command that displays information about the IPSec security associations, not initiates a VPN tunnel.

NEW QUESTION: 34

A company is looking to increase redundancy in their network. Which interface type could help accomplish this?

A. Layer 2

B. Virtual wire

C. Tap

D. Aggregate ethernet

Answer: (SHOW ANSWER)

Explanation

An aggregate group increases the bandwidth between peers by load balancing traffic across the combined interfaces. It also provides redundancy

https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-networking-admin/configure-interfaces/configure-an-aggr

NEW QUESTION: 35

A firewall has been assigned to a new template stack that contains both "Global" and "Local" templates in Panorama, and a successful commit and push has been performed. While validating the configuration on the local firewall, the engineer discovers that some settings are not being applied as intended.

The setting values from the "Global" template are applied to the firewall instead of the "Local" template that has different values for the same settings.

What should be done to ensure that the settings in the "Local" template are applied while maintaining settings from both templates?

A. Move the "Global" template above the "Local" template in the template stack.

B. Perform a commit and push with the "Force Template Values" option selected.

C. Move the "Local" template above the "Global" template in the template stack.

D. Override the values on the local firewall and apply the correct settings for each value.

Answer: C (LEAVE A REPLY)

Explanation

https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/panorama-overview/centralized-firewall-con

NEW QUESTION: 36
A company wants to install a PA-3060 firewall between two core switches on a VLAN trunk link. They need to assign each VLAN to its own zone and to assign untagged (native) traffic to its own zone which options differentiates multiple VLAN into separate zones?
A. Create V-Wire objects with two V-Wire interfaces and define a range of "0-4096 in the "Tag Allowed" field of the V-Wire object.
B. Create V-Wire objects with two V-Wire subinterfaces and assign only a single VLAN ID to the Tag Allowed" field of the V-Wire object. Repeat for every additional VLAN and use a VLAN ID of 0 for untagged traffic. Assign each interface/sub interface to a unique zone.
C. Create Layer 3 subinterfaces that are each assigned to a single VLAN ID and a common virtual router.
The physical Layer 3 interface would handle untagged traffic. Assign each interface/subinterface tA.
unique zone. Do not assign any interface an IP address.
D. Create VLAN objects for each VLAN and assign VLAN interfaces matching each VLAN ID. Repeat for every additional VLAN and use a VLAN ID of 0 for untagged traffic. Assign each interface/sub interface to a unique zone.
Answer: B (LEAVE A REPLY)
Explanation
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/networking/configure-interfaces/virtual-wire-interfa Virtual wire interfaces by default allow all untagged traffic. You can, however, use a virtual wire to connect two interfaces and configure either interface to block or allow traffic based on the virtual LAN (VLAN) tags.
VLAN tag 0 indicates untagged traffic.You can also create multiple subinterfaces, add them into different zones, and then classify traffic according to a VLAN tag or a combination of a VLAN tag with IP classifiers (address, range, or subnet) to apply granular policy control for specific VLAN tags or for VLAN tags from a specific source IP address, range, or subnet.

NEW QUESTION: 37
The Aggregate Ethernet interface is showing down on a passive PA-7050 firewall of an active/passive HA pair. The HA Passive Link State is set to "Auto" under Device > High Availability > General > Active/Passive Settings. The AE interface is configured with LACP enabled and is up only on the active firewall.
Why is the AE interface showing down on the passive firewall?
A. It does not perform pre-negotiation LACP unless "Enable in HA Passive State" is selected under the High Availability Options on the LACP tab of the AE Interface.
B. It does not participate in LACP negotiation unless Fast Failover is selected under the Enable LACP selection on the LACP tab of the AE Interface.

C. It participates in LACP negotiation when Fast is selected for Transmission Rate under the Enable LACP selection on the LACP tab of the AE Interface.
D. It performs pre-negotiation of LACP when the mode Passive is selected under the Enable LACP selection on the LACP tab of the AE Interface.
Answer: A (LEAVE A REPLY)
Explanation
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/high-availability/set-up-activepassive-ha/configure

NEW QUESTION: 38
How would an administrator monitor/capture traffic on the management interface of the Palo Alto Networks NGFW?
A. Use the debug dataplane packet-diag set capture stage firewall file command.
B. Use the debug dataplane packet-diag set capture stage management file command.
C. Enable all four stages of traffic capture (TX, RX, DROP, Firewall).
D. Use the tcpdump command.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 39
SSL Forward Proxy decryption is configured but the firewall uses Untrusted-CA to sign the website https
//www important-website com certificate End-users are receiving me "security certificate is not trusted is warning Without SSL decryption the web browser shows that the website certificate is trusted and signed by a well-known certificate chain Well-Known-Intermediate and Well-Known-Root- CA.
The network security administrator who represents the customer requires the following two behaviors when SSL Forward Proxy is enabled:
1 End-users must not get the warning for the https://www.very-important-website.com website.
2 End-users should get the warning for any other untrusted website
Which approach meets the two customer requirements?
A. Navigate to Device > Certificate Management > Certificates > Device Certificates import Well-Known-Intermediate-CA and Well-Known-Root-CA select the Trusted Root CA checkbox and commit the configuration
B. Install the Well-Known-Intermediate-CA and Well-Known-Root-CA certificates on all end-user systems m the user and local computer stores
C. Navigate to Device > Certificate Management - Certificates s Default Trusted Certificate Authorities import Well-Known-intermediate-CA and Well-Known-Root-CA select the Trusted Root CA check box and commit the configuration
D. Clear the Forward Untrust Certificate check box on the Untrusted-CA certificate and commit the configuration
Answer: C (LEAVE A REPLY)

Explanation
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/device/device-certificate-management-c

NEW QUESTION: 40
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
Answer: D (LEAVE A REPLY)
Explanation
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.

NEW QUESTION: 41
Which three actions can Panorama perform when deploying PAN-OS images to its managed devices? (Choose three.)
A. upload-only
B. upload and install and reboot
C. verify and install
D. upload and install

E. install and reboot

Answer: A,B,D (LEAVE A REPLY)

Explanation

Panorama can perform three actions when deploying PAN-OS images to its managed devices: upload-only, upload and install, and upload and install and reboot. Upload-only transfers the PAN-OS image from Panorama to the managed device without installing it. Upload and install transfers the PAN-OS image from Panorama to the managed device and installs it, but does not reboot the device. Upload and install and reboot transfers the PAN-OS image from Panorama to the managed device, installs it, and reboots the device. Verify and install is not a valid action for deploying PAN-OS images from Panorama. Install and reboot is not a valid action for deploying PAN-OS images from Panorama, as the image needs to be uploaded first. References: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/panorama/panorama-device-deployment/mana

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Cles

NEW QUESTION: 42

A firewall administrator wants to have visibility on one segment of the company network. The traffic on the segment is routed on the Backbone switch. The administrator is planning to apply Security rules on segment X after getting the visibility.

There is already a PAN-OS firewall used in L3 mode as an internet gateway, and there are enough system resources to get extra traffic on the firewall. The administrator needs to complete this operation with minimum service interruptions and without making any IP changes.

What is the best option for the administrator to take?

A. Configure the TAP interface for segment X on the firewall.

B. Configure vwire interfaces for segment X on the firewall.

C. Configure a Layer 3 interface for segment X on the firewall.

D. Configure a new vsys for segment X on the firewall.

Answer: A (LEAVE A REPLY)

Explanation

A TAP interface is a dedicated interface on the firewall that can be connected to a switch SPAN or mirror port to passively monitor traffic flows across a network. A TAP interface provides application visibility and threat detection without being in the flow of network traffic. A TAP interface does not require any IP changes or service interruptions on the network segment . Option B is incorrect because vwire interfaces are used to create virtual wires that transparently connect two network segments. Vwire interfaces require physical cabling changes and may cause service interruptions on the network segment . Option C is incorrect because a Layer 3 interface is used to route traffic between different subnets. A Layer 3 interface requires IP changes and may cause service interruptions on the network segment . Option D is incorrect because a new vsys is used to create a virtual system that can have its own set of policies and objects. A new vsys does not provide visibility or security for a specific network segment

NEW QUESTION: 43
Where is information about packet buffer protection logged?
A. Alert entries are in the Alarms log. Entries for dropped traffic, discarded sessions, and blocked IP address are in the Threat log
B. All entries are in the System log
C. Alert entries are in the System log. Entries for dropped traffic, discarded sessions and blocked IP addresses are in the Threat log
D. All entries are in the Alarms log
Answer: D (LEAVE A REPLY)
Explanation
Graphical user interface, text, application Description automatically generated

NEW QUESTION: 44
Before an administrator of a VM-500 can enable DoS and zone protection, what actions need to be taken?
A. Measure and monitor the CPU consumption of the firewall data plane to ensure that each firewall is properly sized to support DoS and zone protection
B. Add a WildFire subscription to activate DoS and zone protection features
C. Create a zone protection profile with flood protection configured to defend an entire egress zone against SYN. ICMP ICMPv6, UDP. and other IP flood attacks
D. Replace the hardware firewall because DoS and zone protection are not available with VM-Series systems
Answer: A (LEAVE A REPLY)

NEW QUESTION: 45
An engineer creates a set of rules in a Device Group (Panorama) to permit traffic to various services for a specific LDAP user group.
What needs to be configured to ensure Panorama can retrieve user and group information for use in these rules?
A. A service route to the LDAP server
B. A Master Device
C. Authentication Portal
D. A User-ID agent on the LDAP server
Answer: (SHOW ANSWER)
Explanation
To configure LDAP authentication on Panorama, you need to
Define an LDAP server profile that specifies the connection details and credentials for accessing the LDAP server.
Define an authentication profile that references the LDAP server profile and defines how users authenticate to Panorama (such as username format and password expiration).

Define an authentication sequence (optional) that allows users to authenticate using multiple methods (such as local database, LDAP, RADIUS, etc.).
Assign the authentication profile or sequence to a Panorama administrator role or a device group role.

NEW QUESTION: 46
A firewall has Security policies from three sources
1. locally created policies
2. shared device group policies as pre-rules
3. the firewall's device group as post-rules
How will the rule order populate once pushed to the firewall?
A. shared device group policies, firewall device group policies. local policies.
B. firewall device group policies, local policies. shared device group policies
C. shared device group policies. local policies, firewall device group policies
D. local policies, firewall device group policies, shared device group policies
Answer: C (LEAVE A REPLY)
Explanation
https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/manage-firewalls/manage-device-groups/ma

NEW QUESTION: 47
Before you upgrade a Palo Alto Networks NGFW, what must you do?
A. Make sure that the PAN-OS support contract is valid for at least another year
B. Export a device state of the firewall
C. Make sure that the firewall is running a version of antivirus software and a version of WildFire that support the licensed subscriptions.
D. Make sure that the firewall is running a supported version of the app + threat update
Answer: D (LEAVE A REPLY)
Explanation
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-upgrade/upgrade-pan-os/pan-os-upgrade-checklist#id53a2
"Verify the minimum content release version."

Before you upgrade, make sure the firewall is running a version of app + threat (content version) that meets the minimum requirement of the new PAN-OS
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClRrCAK

NEW QUESTION: 48
A client wants to detect the use of weak and manufacturer-default passwords for IoT devices. Which option will help the customer?
A. Configure a Data Filtering profile with alert mode.
B. Configure an Antivirus profile with alert mode.
C. Configure a Vulnerability Protection profile with alert mode
D. Configure an Anti-Spyware profile with alert mode.
Answer: C (LEAVE A REPLY)
Explanation
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/policy/security-profiles

NEW QUESTION: 49
A network security administrator wants to enable Packet-Based Attack Protection in a Zone Protection profile.
What are two valid ways to enable Packet-Based Attack Protection? (Choose two.)
A. TCP Drop
B. SYN Random Early Drop
C. ICMP Drop
D. TCP Port Scan Block
Answer: A,B (LEAVE A REPLY)
Explanation
Packet-Based Attack Protection is a feature of Zone Protection Profiles that allows the firewall to drop packets that are malformed, spoofed, or part of a port scan. TCP Drop and SYN Random Early Drop are two options under Packet-Based Attack Protection that can be enabled to protect against TCP-based attacks. TCP Drop enables the firewall to check for spoofed IP addresses, mismatched overlapping TCP segments, and invalid IP options. SYN Random Early Drop enables the firewall to drop SYN packets randomly when the SYN queue is full, preventing SYN flood attacks. ICMP Drop and TCP Port Scan Block are not valid options under Packet-Based Attack Protection

NEW QUESTION: 50
An administrator needs to optimize traffic to prefer business-critical applications over non-critical applications QoS natively integrates with which feature to provide service quality?
A. certificate revocation
B. Content-ID
C. App-ID
D. port inspection

Answer: C (LEAVE A REPLY)

Explanation

QoS natively integrates with App-ID, which is a feature that identifies applications based on their unique characteristics and behaviors, regardless of port, protocol, encryption, or evasive tactics. By using App-ID, QoS can prioritize or limit traffic based on the application name, category, subcategory, technology, or risk level. Certificate revocation is a process of invalidating digital certificates that are no longer trusted or secure.

Content-ID is a feature that scans content and data within allowed applications for threats and sensitive data.

Port inspection is a method of identifying applications based on the TCP or UDP port numbers they use, which is not reliable or granular enough for QoS purposes. References:

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/quality-of-service/configure-qos

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/app-id

NEW QUESTION: 51

Review the images. A firewall policy that permits web traffic includes the What is the result of traffic that matches the "Alert - Threats" Profile Match List?

A. The source address of SMTP traffic that matches a threat is automatically blocked as BadGuys for 180 minutes.

B. The source address of traffic that matches a threat is automatically blocked as BadGuys for 180 minutes.

C. The source address of traffic that matches a threat is automatically tagged as BadGuys for 180 minutes.

D. The source address of SMTP traffic that matches a threat is automatically tagged as BadGuys for 180 minutes.

Answer: C (LEAVE A REPLY)

Explanation

The threat profile has the action set to "alert" which means that the traffic is allowed but logged. The profile also has the "Tag Source IP" option enabled with the tag name "BadGuys" and the timeout value of 180 minutes. This means that any source IP address that matches a threat signature will be tagged with "BadGuys" for 180 minutes. The tag can be used for dynamic address groups or external dynamic lists to enforce policy actions based on the tag. References: :

https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/threat-prevention/set-up-antivirus-anti-spyware-an

NEW QUESTION: 52

In the New App Viewer under Policy Optimizer, what does the compare option for a specific rule allow an administrator to compare?

A. The running configuration with the candidate configuration of the firewall

B. Applications configured in the rule with their dependencies

C. Applications configured in the rule with applications seen from traffic matching the same rule

D. The security rule with any other security rule selected

Answer: C (LEAVE A REPLY)

Explanation

The compare option for a specific rule in the New App Viewer under Policy Optimizer allows an administrator to compare the applications configured in the rule with the applications seen from traffic matching the same rule. This option helps the administrator to identify any discrepancies between the intended and actual applications allowed by the rule. The administrator can thenoptimize the rule by adding or removing applications as needed1. Option A is incorrect because the compare option does not compare the running configuration with the candidate configuration of the firewall. That is done by using the Commit > Commit and Push option2. Option B is incorrect because the compare option does not compare applications configured in the rule with their dependencies. That is done by using the App Dependencies tab under Policy Optimizer1.

Option D is incorrect because the compare option does not compare the security rule with any other security rule selected. That is done by using the Compare Rules option under Policies > Security3.

NEW QUESTION: 53

A network-security engineer attempted to configure a bootstrap package on Microsoft Azure, but the virtual machine provisioning process failed. In reviewing the bootstrap package, the engineer only had the following directories: /config, /license and /software Why did the bootstrap process fail for the VM-Series firewall in Azure?

A. All public cloud deployments require the /plugins folder to support proper firewall native integrations

B. The /content folder is missing from the bootstrap package

C. The VM-Series firewall was not pre-registered in Panorama and prevented the bootstrap process from successfully completing

D. The /config or /software folders were missing mandatory files to successfully bootstrap

Answer: B (LEAVE A REPLY)

Explanation

https://docs.paloaltonetworks.com/vm-series/10-2/vm-series-deployment/bootstrap-the-vm-series-firewall/bootst The bootstrap process failed for the VM-Series firewall in Azure because the /content folder is missing from the bootstrap package 1. References: 1: Bootstrap the VM-Series Firewall on Azure - Palo Alto Networks

NEW QUESTION: 54

An engineer is tasked with enabling SSL decryption across the environment. What are three valid parameters of an SSL Decryption policy? (Choose three.)

A. URL categories

B. source users

C. source and destination IP addresses

D. App-ID
E. GlobalProtect HIP
Answer: A,B,C (LEAVE A REPLY)
Explanation
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClEZCA0
https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/decryption/define-traffic-to-decrypt/create-a-decry

NEW QUESTION: 55
To ensure that a Security policy has the highest priority, how should an administrator configure a Security policy in the device group hierarchy?
A. Add the policy to the target device group and apply a master device to the device group.
B. Reference the targeted device's templates in the target device group.
C. Clone the security policy and add it to the other device groups.
D. Add the policy in the shared device group as a pre-rule
Answer: D (LEAVE A REPLY)
Explanation
According to the Palo Alto Networks documentation , the shared device group is a special device group that contains policies and objects that apply to all firewalls managed by Panorama. The policies in the shared device group can be configured as pre-rules or post-rules, which determine their priority relative to the policies in other device groups. Pre-rules have higher priority than the policies in other device groups, while post-rules have lower priority. Therefore, to ensure that a Security policy has the highest priority, the administrator should configure it in the shared device group as a pre-rule. Therefore, the correct answer is D.
The other options are not relevant or effective for ensuring that a Security policy has the highest priority:
Add the policy to the target device group and apply a master device to the device group: This option would add the policy to a specific device group, which is a subset of firewalls managed by Panorama.
The policy would only apply to the firewalls in that device group, not to all firewalls. Moreover, applying a master device to the device group does not affect the priority of the policy, but only allows synchronizing configuration changes across devices in the same device group2.
Reference the targeted device's templates in the target device group: This option would reference the templates that contain network and device settings for the targeted devices in the target device group. It does not affect the Security policy or its priority, but only allows applying consistent configuration settings across devices in the same device group3.
Clone the security policy and add it to the other device groups: This option would create copies of the security policy and add them to different device groups. However, this would not ensure that the policy has the highest priority, because it would still depend on whether it is configured as a pre-rule or a post-rule within each device group. Moreover, this option would create redundant and potentially conflicting policies across different device groups.

References: 1:
https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/panorama-overview/centralized-firewall-conf
2:
https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/panorama-overview/centralized-firewall-conf
3:
https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/panorama-overview/centralized-firewall-conf

NEW QUESTION: 56
During the implementation of SSL Forward Proxy decryption, an administrator imports the company's Enterprise Root CA and Intermediate CA certificates onto the firewall. The company's Root and Intermediate CA certificates are also distributed to trusted devices using Group Policy and GlobalProtect. Additional device certificates and/or Subordinate certificates requiring an Enterprise CA chain of trust are signed by the company's Intermediate CA.
Which method should the administrator use when creating Forward Trust and Forward Untrust certificates on the firewall for use with decryption?
A. Generate a single subordinate CA certificate for both Forward Trust and Forward Untrust.
B. Generate a CA certificate for Forward Trust and a self-signed CA for Forward Untrust.
C. Generate a single self-signed CA certificate for Forward Trust and another for Forward Untrust
D. Generate two subordinate CA certificates, one for Forward Trust and one for Forward Untrust.
Answer: B (LEAVE A REPLY)
Explanation
Generate a CA certificate for Forward Trust (step 2) a self-signed CA for Forward Untrust (step 4)
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/configure-ssl-forward-proxy

NEW QUESTION: 57
A company is deploying User-ID in their network. The firewall learn needs to have the ability to see and choose from a list of usernames and user groups directly inside the Panorama policies when creating new security rules How can this be achieved?
A. By configuring Data Redistribution Client in Panorama > Data Redistribution
B. By configuring User-ID source device in Panorama > Managed Devices
C. By configuring User-ID group mapping in Panorama > User Identification
D. By configuring Master Device in Panorama > Device Groups
Answer: C (LEAVE A REPLY)
Explanation
User-ID group mapping is a feature that allows Panorama to retrieve user and group information from directory services such as LDAP or Active Directory . This information can be used to enforce security policies based on user identity and group membership.

To configure User-ID group mapping on Panorama, you need to perform the following steps1:
Select Panorama > User Identification > Group Mapping Settings
Click Add and enter a name for the server profile
Select a Server Type (LDAP or Active Directory)
Click Add and enter the server details (IP address, port number, etc.)
Click OK
Select Group Include List and click Add
Select the groups that you want to include in the group mapping
Click OK
Commit your changes
By configuring User-ID group mapping on Panorama, you can see and choose from a list of usernames and user groups directly inside the Panorama policies when creating new security rules2.

NEW QUESTION: 58
An engineer receives reports from users that applications are not working and that websites are only partially loading in an asymmetric environment. After investigating, the engineer observes the flow_tcp_non_syn_drop counter increasing in the show counters global output.
Which troubleshooting command should the engineer use to work around this issue?
A. set deviceconfig setting tcp asymmetric-path drop
B. set deviceconfig setting session tcp-reject-non-syn no
C. set session tcp-reject-non-syn yes
D. set deviceconfig setting tcp asymmetric-path bypass
Answer: B (LEAVE A REPLY)
Explanation
To work around this issue, one possible troubleshooting command is set deviceconfig setting session tcp-reject-non-syn no which disables TCP reject non-SYN temporarily (until reboot)4. This command allows non-SYN first packet through without dropping it.
The flow_tcp_non_syn_drop counter increases when the firewall receives packets with the ACK flag set, but not the SYN flag, which indicates asymmetric traffic flow. The tcp-reject-non-syn option enables or disables the firewall to drop non-SYN TCP packets. In this case, disabling the tcp-reject-non-syn option using the "set deviceconfig setting session tcp-reject-non-syn no" command can help work around the issue. This allows the firewall to accept non-SYN packets and create a session for the existing flow.

NEW QUESTION: 59
An administrator is building Security rules within a device group to block traffic to and from malicious locations How should those rules be configured to ensure that they are evaluated with a high priority?
A. Create the appropriate rules with a Block action and apply them at the top of the Default Rules

B. Create the appropriate rules with a Block action and apply them at the top of the Security Post-Rules.
C. Create the appropriate rules with a Block action and apply them at the top of the local firewall Security rules.
D. Create the appropriate rules with a Block action and apply them at the top of the Security Pre-Rules
Answer: D (LEAVE A REPLY)
Explanation
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/panorama-web-interface/defining-poli

NEW QUESTION: 60
What are three valid qualifiers for a Decryption Policy Rule match? (Choose three.)
A. Destination Zone
B. App-ID
C. Custom URL Category
D. User-ID
E. Source Interface
Answer: A,C,D (LEAVE A REPLY)
Explanation
The valid qualifiers for a Decryption Policy Rule match are:
* Source Zone
* Destination Zone
* Source Address
* Destination Address
* Source User
* Destination User
* Source Region
* Destination Region
* Service/URL Category
* Custom URL Category
* URL Filtering Profile
Therefore, out of the options given, Destination Zone, Custom URL Category, and User-ID are valid qualifiers. References:
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/decryption/configure-decryption-policies.html

NEW QUESTION: 61
An organization wishes to roll out decryption but gets some resistance from engineering leadership regarding the guest network.
What is a common obstacle for decrypting traffic from guest devices?

A. Guest devices may not trust the CA certificate used for the forward untrust certificate.
B. Guests may use operating systems that can't be decrypted.
C. The organization has no legal authority to decrypt their traffic.
D. Guest devices may not trust the CA certificate used for the forward trust certificate.
Answer: D (LEAVE A REPLY)
Explanation
https://docs.paloaltonetworks.com/best-practices/10-2/decryption-best-practices/decryption-best-practices/plan-s
https://live.paloaltonetworks.com/t5/general-topics/decrypt-guest-network-traffic/td-p/119388

NEW QUESTION: 62
Which log type would provide information about traffic blocked by a Zone Protection profile?
A. Data Filtering
B. IP-Tag
C. Traffic
D. Threat
Answer: (SHOW ANSWER)
Explanation
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Clm9CAC Zone Protection profile is a set of security policies that you can apply to an interface or zone to protect it from reconnaissance, flooding, brute force, and other types of attacks.
The log type that would provide information about traffic blocked by a Zone Protection profile is Threat4.
This log type records events such as packet-based attacks, spyware, viruses, vulnerability exploits, and URL filtering.

NEW QUESTION: 63
Which time determines how long the passive firewall will wait before taking over as the active firewall alter losing communications with the HA peer?
A. Heartbeat Interval
B. Additional Master Hold Up Time
C. Promotion Hold Time

D. Monitor Fall Hold Up Time

Answer: (SHOW ANSWER)

Explanation

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/high-availability/ha-concepts/ha-timers

NEW QUESTION: 64

Which three methods are supported for split tunneling in the GlobalProtect Gateway? (Choose three.)

A. Video Streaming Application

B. Destination Domain

C. Client Application Process

D. Source Domain

E. URL Category

Answer: (SHOW ANSWER)

Explanation

The GlobalProtect Gateway supports three methods for split tunneling23:

Access Route - You can define a list of IP addresses or subnets that are accessible through the VPN tunnel. All other traffic goes directly to the internet.

Domain and Application - You can define a list of domains or applications that are accessible through the VPN tunnel. All other traffic goes directly to the internet. You can also use this method to exclude specific domains or applications from the VPN tunnel.

Video Traffic - You can exclude video streaming traffic from the VPN tunnel based on predefined categories or custom URLs. This method reduces latency and jitter for video streaming applications.

NEW QUESTION: 65

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.

Answer: B (LEAVE A REPLY)

Explanation

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Cm1OCAS 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.

NEW QUESTION: 66
What is considered the best practice with regards to zone protection?
A. Review DoS threat activity (ACC > Block Activity) and look for patterns of abuse
B. Use separate log-forwarding profiles to forward DoS and zone threshold event logs separately from other threat logs
C. If the levels of zone and DoS protection consume too many firewall resources, disable zone protection
D. Set the Alarm Rate threshold for event-log messages to high severity or critical severity
Answer: (SHOW ANSWER)
Explanation
The best practice with regards to zone protection is to review DoS threat activity (ACC > Block Activity) and look for patterns of abuse. This way, you can identify the sources and types of DoS attacks that target your network zones and adjust your zone protection profiles and policies accordingly1. You can also use the DoS Protection dashboard widget to monitor the number of sessions that match DoS protection policies2. You do not need to use separate log-forwarding profiles to forward DoS and zone threshold event logs separately from other threat logs, as you can use a single log-forwarding profile to forward different types of logs to different destinations3. You should not disable zone protection if the levels of zone and DoS protection consume too many firewall resources, as this would expose your network zones to potential DoS attacks. Instead, you should optimize your zone protection profiles and policies to reduce the resource consumption4. You should not set the Alarm Rate threshold for event-log messages to high severity or critical severity, as this would limit the visibility into DoS attacks that have lower severity levels. Instead, you should set the Alarm Rate threshold to a value that is appropriate for your network environment and traffic patterns. References: 1:
https://docs.paloaltonetworks.com/best-practices/dos-and-zone-protection-best-practices/dos-and-zone-protection
2:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/monitoring/use-the-acc-to-monitor-network-activit
3:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/monitoring/configure-log-forwarding/log-forwardi
4:
https://docs.paloaltonetworks.com/best-practices/dos-and-zone-protection-best-practices/dos-and-zone-protection
:

https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/networking/network-profiles/zone-protection-profi

NEW QUESTION: 67
Which benefit do policy rule UUIDs provide?
A. An audit trail across a policy's lifespan
B. Functionality for scheduling policy actions
C. The use of user IP mapping and groups in policies
D. Cloning of policies between device-groups
Answer: A (LEAVE A REPLY)
Explanation
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/policy/enumeration-of-rules-within-a-rulebase To keep track of rules within a rulebase, you can refer to the rule number, which changes depending on the order of a rule in the rulebase. The rule number determines the order in which the firewall applies the rule. The universally unique identifier (UUID) for a rule never changes even if you modify the rule, such as when you change the rule name. The UUID allows you to track the rule across rule bases even after you deleted the rule.

NEW QUESTION: 68
Which three firewall multi-factor authentication factors are supported by PAN-OS? (Choose three)
A. SSH key
B. User logon
C. Short message service
D. One-Time Password
E. Push
Answer: B,D,E (LEAVE A REPLY)
Explanation
According to Palo Alto Networks documentation123, multi-factor authentication (MFA) is a method of verifying a user's identity using two or more factors, such as something they know, something they have, or something they are.
The firewall supports MFA for administrative access, GlobalProtect VPN access, and Captive Portal access.
The firewall can integrate with external MFA providers such as RSA SecurID, Duo Security, or Okta Verify.
The three firewall MFA factors that are supported by PAN-OS are:
User logon: This is something the user knows, such as a username and password.
One-Time Password: This is something the user has, such as a code generated by an app or sent by email or SMS.
Push: This is something the user is, such as a biometric verification or a device approval.

NEW QUESTION: 69

What can an engineer use with GlobalProtect to distribute user-specific client certificates to each GlobalProtect user?

A. Certificate profile

B. SSL/TLS Service profile

C. OCSP Responder

D. SCEP

Answer: (SHOW ANSWER)

Explanation

If you have a Simple Certificate Enrollment Protocol (SCEP) server in your enterprise PKI, you can configure a SCEP profile to automate the generation and distribution of unique client certificates.

https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/certificate-management/obtain-certificates/deploy-

NEW QUESTION: 70

A network administrator wants to use a certificate for the SSL/TLS Service Profile.

Which type of certificate should the administrator use?

A. certificate authority (CA) certificate

B. client certificate

C. machine certificate

D. server certificate

Answer: D (LEAVE A REPLY)

Explanation

Use only signed certificates, not CA certificates, in SSL/TLS service profiles.

https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/certificate-management/configure-an-ssltls-service A server certificate is used for the SSL/TLS Service Profile. The server certificate identifies the firewall to clients that initiate SSL/TLS connections to it. References:

https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/certificate-management/certificates-and-keys/serve

NEW QUESTION: 71

Which statement regarding HA timer settings is true?

A. Use the Recommended profile for typical failover timer settings

B. Use the Moderate profile for typical failover timer settings

C. Use the Aggressive profile for slower failover timer settings.

D. Use the Critical profile for faster failover timer settings.

Answer: (SHOW ANSWER)

Explanation

The Recommended profile is the default profile that provides typical failover timer settings for most deployments. The other profiles are designed for specific scenarios where faster or slower failover is desired.

References:
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/high-availability/ha-concepts/ha-timers

NEW QUESTION: 72
When using certificate authentication for firewall administration, which method is used for authorization?
A. Radius
B. LDAP
C. Kerberos
D. Local
Answer: D (LEAVE A REPLY)
Explanation
Authentication: Certificates Authorization: Local The administrative accounts are local to the firewall, but authentication to the web interface is based on client certificates. You use the firewall to manage role assignments but access domains are not supported.

NEW QUESTION: 73
Which two profiles should be configured when sharing tags from threat logs with a remote User-ID agent?
(Choose two.)
A. Log Forwarding
B. Log Ingestion
C. LDAP
D. HTTP
Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 74
What is a correct statement regarding administrative authentication using external services with a local authorization method?
A. Prior to PAN-OS 10.2. an administrator used the firewall to manage role assignments, but access domains have not been supported by this method.
B. Starting with PAN-OS 10.2. an administrator needs to configure Cloud Identity Engine to use external authentication services for administrative authentication.
C. The administrative accounts you define locally on the firewall serve as references to the accounts defined on an external authentication server.
D. The administrative accounts you define on an external authentication server serve as references to the accounts defined locally on the firewall.
Answer: (SHOW ANSWER)
Explanation

https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/firewall-administration/manage-firewall-administra

NEW QUESTION: 75
What is the best description of the HA4 Keep-Alive Threshold (ms)?
A. the maximum interval between hello packets that are sent to verify that the HA functionality on the other firewall is operational.
B. The time that a passive or active-secondary firewall will wait before taking over as the active or active-primary firewall
C. the timeframe within which the firewall must receive keepalives from a cluster member to know that the cluster member is functional.
D. The timeframe that the local firewall wait before going to Active state when another cluster member is preventing the cluster from fully synchronizing.
Answer: C (LEAVE A REPLY)
Explanation
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/high-availability/configure-ha-clustering

NEW QUESTION: 76
A firewall administrator has been tasked with ensuring that all Panorama configuration is committed and pushed to the devices at the end of the day at a certain time. How can they achieve this?
A. Use the Scheduled Config Export to schedule Commit to Panorama and also Push to Devices.
B. Use the Scheduled Config Push to schedule Push lo Devices and separately schedule an API call to commit all Panorama changes.
C. Use the Scheduled Config Export to schedule Push to Devices and separately schedule an API call to commit all Panorama changes.
D. Use the Scheduled Config Push to schedule Commit to Panorama and also Push to Devices.
Answer: (SHOW ANSWER)
Explanation
https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/manage-firewalls/schedule-a-configuration-p Log in to the PanoramaWeb Interface. Create a scheduled configuration push. Select PanoramaScheduled Config Push and Add a new scheduled configuration push. You can also schedule a configuration push to managed firewalls when you push to devices (CommitPush to Devices).

NEW QUESTION: 77
What happens when an A/P firewall cluster synchronizes IPsec tunnel security associations (SAs)?
A. Phase 1 and Phase 2 SAs are synchronized over HA3 links.
B. Phase 1 SAs are synchronized over HA1 links.
C. Phase 2 SAs are synchronized over HA2 links.
D. Phase 1 and Phase 2 SAs are synchronized over HA2 links.
Answer: C (LEAVE A REPLY)
Explanation
From the Palo Alto documentation below, "when a VPN is terminated on a Palo Alto firewall HA pair, not all IPSEC related information is synchronized between the firewalls... This is an expected behavior. IKE phase 1 SA information is NOT synchronized between the HA firewalls." And from the second link, "Data link (HA2) is used to sync sessions, forwarding tables, IPSec security associations, and ARP tables between firewalls in the HA pair. Data flow on the HA2 link is always unidirectional (except for the HA2 keep-alive). It flows from the active firewall to the passive firewall."
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000HAuZCAW&lang=en_US%E
https://help.aryaka.com/display/public/KNOW/Palo+Alto+Networks+NFV+Technical+Brief

NEW QUESTION: 78
A network security engineer is attempting to peer a virtual router on a PAN-OS firewall with an external router using the BGP protocol. The peer relationship is not establishing.
What command could the engineer run to see the current state of the BGP state between the two devices?
A. show routing protocol bgp state
B. show routing protocol bgp peer
C. show routing protocol bgp summary
D. show routing protocol bgp rib-out
Answer: C (LEAVE A REPLY)
Explanation
The show routing protocol bgp summary command displays the current state of the BGP peer relationship between the firewall and other BGP routers. The output includes the peer IP address, AS number, uptime, prefix count, state, and status codes. References:
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-cli-quick-start/use-the-cli/show-the-routing-table-and-stat

NEW QUESTION: 79
While analyzing the Traffic log, you see that some entries show "unknown-tcp" in the Application column What best explains these occurrences?
A. A handshake took place, but no data packets were sent prior to the timeout.
B. A handshake took place; however, there were not enough packets to identify the application.
C. A handshake did take place, but the application could not be identified.
D. A handshake did not take place, and the application could not be identified.
Answer: C (LEAVE A REPLY)
Explanation
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClibCAC#:~:text=unknown% Unknown-tcp means the firewall captured the three-way TCP handshake, but the application was not identified. This may be due to the use of a custom application for which the firewall does not have signatures

NEW QUESTION: 80
An administrator connected a new fiber cable and transceiver to interface Ethernetl/l on a Palo Alto Networks firewall. However, the link does not seem to be coming up.
If an administrator were to troubleshoot, how would they confirm the transceiver type, tx-power, rx-power, vendor name, and part number via the CLI?
A. show system state filter sw.dev.interface.config
B. show chassis status slot s1
C. show system state filter-pretty sys.s1.*
D. show system state filter ethernet1/1
Answer: D (LEAVE A REPLY)
Explanation
According to the Palo Alto Networks documentation , the command show system state filter displays the current state of the system and allows you to filter the output by a specific keyword. The keyword ethernet1/1 matches the interface name that the administrator wants to troubleshoot. The output of this command will show information about the transceiver type, tx-power, rx-power, vendor name, and part number for that interface2. Therefore, the correct answer is D. References:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-cli-quick-start/use-the-cli/find-a-command 2 :https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClFmCAK

NEW QUESTION: 81
An administrator device-group commit push is tailing due to a new URL category How should the administrator correct this issue?
A. verify that the URL seed Tile has been downloaded and activated on the firewall
B. change the new category action to alert" and push the configuration again
C. update the Firewall Apps and Threat version to match the version of Panorama
D. ensure that the firewall can communicate with the URL cloud

Answer: C (LEAVE A REPLY)
Explanation
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PNqw

NEW QUESTION: 82
As a best practice, logging at session start should be used in which case?
A. On all Allow rules
B. While troubleshooting
C. Only when log at session end is enabled
D. Only on Deny rules
Answer: (SHOW ANSWER)
Explanation
Logging at session start should be used as a best practice while troubleshooting. Logging at session start allows the administrator to see the logs for sessions that are initiated but not completed, such as sessions that are dropped or blocked by the firewall. This can help the administrator to identify and resolve issues with network connectivity or firewall configuration. Logging at session start should not be used for normal operations because it generates more logs and consumes more resources on the firewall. Option A is incorrect because logging at session start should not be used on all Allow rules. Logging at session end is sufficient for Allow rules because it provides information about the completed sessions, such as bytes and packets transferred, application, user, and threat information. Option C is incorrect because logging at session start can be used independently of logging at session end. Logging at session start and logging at session end are not mutually exclusive options. Option D is incorrect because logging at session start should not be used only on Deny rules. Logging at session end is sufficient for Deny rules because it provides information about the denied sessions, such as source and destination IP addresses, ports, and protocol.

NEW QUESTION: 83
You need to allow users to access the office-suite applications of their choice. How should you configure the firewall to allow access to any office-suite application?
A. Create an Application Group and add Office 365, Evernote Google Docs and Libre Office
B. Create an Application Group and add business-systems to it.
C. Create an Application Filter and name it Office Programs, then filter it on the office programs subcategory.
D. Create an Application Filter and name it Office Programs then filter on the business-systems category.
Answer: C (LEAVE A REPLY)
Explanation
According to the Palo Alto Networks documentation, "Application filters enable you to create groups of applications based on specific characteristics such as subcategory, technology, risk factor, and so on. You can then use these groups in Security policy rules to allow or block access

to the applications. For example, you can create an application filter that includes all applications in the office-programs subcategory and use it in a Security policy rule to allow access to any office-suite application." References: https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/app-id/manage-applications-in-a-policy/use-applic

NEW QUESTION: 84
A user at an internal system queries the DNS server for their web server with a private IP of 10 250 241 131 in the. The DNS server returns an address of the web server's public address, 200.1.1.10.
In order to reach the web server, which security rule and U-Turn NAT rule must be configured on the firewall?
A.
B.
C.
D.
Answer: A (LEAVE A REPLY)
Explanation
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClEiCAK

NEW QUESTION: 85
A prospect is eager to conduct a Security Lifecycle Review (SLR) with the aid of the Palo Alto Networks NGFW.
Which interface type is best suited to provide the raw data for an SLR from the network in a way that is minimally invasive?
A. Layer 3
B. Virtual Wire
C. Tap
D. Layer 2
Answer: C (LEAVE A REPLY)
Explanation
A tap interface is best suited to provide the raw data for an SLR from the network in a way that is minimally invasive. A tap interface allows the firewall to passively monitor network traffic without affecting the flow of traffic. The firewall can analyze the traffic and generate reports based on the application, user, content, and threat information. References: https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/networking/configure-interfaces/configure-a-tap-in

NEW QUESTION: 86
An engineer decides to use Panorama to upgrade devices to PAN-OS 10.2.
Which three platforms support PAN-OS 10 2? (Choose three.)

A. PA-5000 Series
B. PA-500
C. PA-800 Series
D. PA-220
E. PA-3400 Series
Answer: C,D,E (LEAVE A REPLY)
Explanation
According to the Palo Alto Networks Compatibility Matrix , the three platforms that support PAN-OS 10.2 are:
PA-800 Series2
PA-2202
PA-3400 Series2
The PA-5000 Series and PA-500 do not support PAN-OS 10.2
To upgrade devices to PAN-OS 10.2 using Panorama, you need to determine the upgrade path3, upgrade Panorama itself4, and then upgrade the firewalls using Panorama

NEW QUESTION: 87
Which User-ID mapping method should be used in a high-security environment where all IP address-to-user mappings should always be explicitly known?
A. PAN-OS integrated User-ID agent
B. GlobalProtect
C. Windows-based User-ID agent
D. LDAP Server Profile configuration
Answer: (SHOW ANSWER)
Explanation
Because GlobalProtect users must authenticate to gain access to the network, the IP address-to-username mapping is explicitly known. This is the best solution in sensitive environments where you must be certain of who a user is in order to allow access to an application or service.
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/user-id/user-id-concepts/user-mapping/globalprote

NEW QUESTION: 88
An administrator Just enabled HA Heartbeat Backup on two devices However, the status on tie firewall's dashboard is showing as down High Availability.
What could an administrator do to troubleshoot the issue?
A. Go to Device > High Availability> General > HA Pair Settings > Setup and configuring the peer IP for heartbeat backup
B. Check peer IP address In the permit list In Device > Setup > Management > Interfaces > Management Interface Settings
C. Go to Device > High Availability > HA Communications> General> and check the Heartbeat Backup under Election Settings

D. Check peer IP address for heartbeat backup to Device > High Availability > HA Communications > Packet Forwarding settings.

Answer: B (LEAVE A REPLY)

Explanation

If the HA status is showing as down after enabling HA Heartbeat Backup on two devices, an administrator could troubleshoot the issue by checking the peer IP address in the permit list in Device > Setup > Management > Interfaces > Management Interface Settings. This is described in the Palo Alto Networks PCNSE Study Guide in Chapter 7: High Availability, under the section "Configure Heartbeat Backup for Redundancy":

"Verify that the management interface's permitted IP addresses on each peer includes the IP address of the other peer's Heartbeat Backup interface."

NEW QUESTION: 89

A network administrator wants to deploy SSL Forward Proxy decryption. What two attributes should a forward trust certificate have? (Choose two.)

A. A subject alternative name

B. A private key

C. A server certificate

D. A certificate authority (CA) certificate

Answer: (SHOW ANSWER)

Explanation

When deploying SSL Forward Proxy decryption, a forward trust certificate must have a subject alternative name (SAN) and be a server certificate. SAN is an extension to the X.509 standard that allows multiple domain names to be protected by a single SSL/TLS certificate. It is used to identify the domain names or IP addresses that the certificate should be valid for. A private key is also required but it is not mentioned in the options. A certificate authority (CA) certificate is not required as the forward trust certificate itself is a CA certificate.

NEW QUESTION: 90

Which statement is true regarding a Best Practice Assessment?

A. It shows how your current configuration compares to Palo Alto Networks recommendations

B. It runs only on firewalls

C. When guided by an authorized sales engineer, it helps determine the areas of greatest risk where you should focus prevention activities.

D. It provides a set of questionnaires that help uncover security risk prevention gaps across all areas of network and security architecture

Answer: A (LEAVE A REPLY)

Explanation

The Best Practice Assessment (BPA) tool compares the configuration of firewalls and Panorama to the Palo Alto Networks best practice recommendations. Run the BPA periodically to identify

security weaknesses, see the best practice settings, and implement them to improve your security posture.
https://docs.paloaltonetworks.com/best-practices/10-2/bpa-getting-started

NEW QUESTION: 91
Given the following snippet of a WildFire submission log. did the end-user get access to the requested information and why or why not?
A. Yes. because the action is set to "allow "
B. No because WildFire categorized a file with the verdict "malicious"
C. Yes because the action is set to "alert"
D. No because WildFire classified the seventy as "high."
Answer: (SHOW ANSWER)
Explanation
Threats that have the ability to become critical but have mitigating factors; for example, they may be difficult to exploit, do not result in elevated privileges, or do not have a large victim pool.
WildFire Submissions log entries with a malicious verdict and an action set to allow are logged as High.
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/monitoring/view-and-manage-logs/log-types-and-s

NEW QUESTION: 92
A network administrator troubleshoots a VPN issue and suspects an IKE Crypto mismatch between peers.
Where can the administrator find the corresponding logs after running a test command to initiate the VPN?
A. Configuration logs
B. System logs
C. Traffic logs
D. Tunnel Inspection logs
Answer: (SHOW ANSWER)
Explanation

According to the Palo Alto Networks documentation, "To view IKE and IPSec Crypto profiles in the logs, filter the System log for eventid equal to vpn (Monitor > Logs > System)." References: https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/vpn/set-up-site-to-site-vpn/set-up-ike-crypto-profil

NEW QUESTION: 93
What can you use with Global Protect to assign user-specific client certificates to each GlobalProtect user?
A. SSL/TLS Service profile
B. Certificate profile
C. SCEP
D. OCSP Responder
Answer: C (LEAVE A REPLY)
Explanation
If you have a Simple Certificate Enrollment Protocol (SCEP) server in your enterprise PKI, you can configure a SCEP profile to automate the generation and distribution of unique client certificates.
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/certificate-management/obtain-certificates/deploy-

NEW QUESTION: 94
An administrator wants multiple web servers In the DMZ to receive connections initiated from the internet.
Traffic destined for 206.15.22.9 port 80/TCP needs to be forwarded to the server at 10.1.1.22.
Based on the image, which NAT rule will forward web-browsing traffic correctly?
A.
B.
C.
D.
Answer: (SHOW ANSWER)
Explanation
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/networking/nat/nat-configuration-examples/destinat

NEW QUESTION: 95
An engineer needs to redistribute User-ID mappings from multiple data centers. Which data flow best describes redistribution of user mappings?
A. Domain Controller to User-ID agent
B. User-ID agent to Panorama
C. User-ID agent to firewall
D. firewall to firewall

Answer: D (LEAVE A REPLY)
Explanation
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/user-id/deploy-user-id-in-a-large-scale-network/red

NEW QUESTION: 96
A network security administrator wants to begin inspecting bulk user HTTPS traffic flows egressing out of the internet edge firewall. Which certificate is the best choice to configure as an SSL Forward Trust certificate?
A. A self-signed Certificate Authority certificate generated by the firewall
B. A Machine Certificate for the firewall signed by the organization's PKI
C. A web server certificate signed by the organization's PKI
D. A subordinate Certificate Authority certificate signed by the organization's PKI
Answer: D (LEAVE A REPLY)
Explanation
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/configure-ssl-forward-proxy

NEW QUESTION: 97
Refer to the image.
An administrator is tasked with correcting an NTP service configuration for firewalls that cannot use the Global template NTP servers. The administrator needs to change the IP address to a preferable server for this template stack but cannot impact other template stacks.
How can the issue be corrected?
A. Override the value on the NYCFW template.
B. Override a template value using a template stack variable.
C. Override the value on the Global template.
D. Enable "objects defined in ancestors will take higher precedence" under Panorama settings.
Answer: B (LEAVE A REPLY)
Explanation
Both templates and template stacks support variables. Variables allow you to create placeholder objects with their value specified in the template or template stack based on your configuration needs. Create a template or template stack variable to replace IP addresses, Group IDs, and interfaces in your configurations.
https://docs.paloaltonetworks.com/panorama/10-0/panorama-admin/manage-firewalls/manage-templates-and-tem

NEW QUESTION: 98
An administrator wants to configure the Palo Alto Networks Windows User-ID agent to map IP addresses to usernames. The company uses four Microsoft Active Directory servers and two Microsoft Exchange servers, which can provide logs for login events.

All six servers have IP addresses assigned from the following subnet: 192.168 28.32/27. The Microsoft Active Directory servers reside in 192.168.28.32/28. and the Microsoft Exchange servers resideL in 192.168.28 48/28 What information does the administrator need to provide in the User Identification > Discovery section?

A. The IP-address and corresponding server type (Microsoft Active Directory or Microsoft Exchange) for each of the six servers

B. Network 192 168.28.32/28 with server type Microsoft Active Directory and network 192.168.28.48/28 with server type Microsoft Exchange

C. Network 192 168 28.32/27 with server type Microsoft

D. One IP address of a Microsoft Active Directory server and "Auto Discover" enabled to automatically obtain all five of the other servers

Answer: A (LEAVE A REPLY)

Explanation

The administrator needs to provide the IP address and corresponding server type (Microsoft Active Directory or Microsoft Exchange) for each of the six servers in the User Identification > Discovery section. The administrator should enter the network address of 192.168.28.32/28 and select "Microsoft Active Directory" as the server type for the four Active Directory servers and enter the network address of 192.168.28.48/28 and select "Microsoft Exchange" as the server type for the two Exchange servers. This will allow the User-ID agent to discover and map the IP address of each server to the corresponding username.

NEW QUESTION: 99

An engineer is bootstrapping a VM-Series Firewall Other than the 'config folder, which three directories are mandatory as part of the bootstrap package directory structure? (Choose three.)

A. /software

B. /opt

C. /license

D. /content

E. /plugins

Answer: (SHOW ANSWER)

Explanation

https://docs.paloaltonetworks.com/vm-series/9-1/vm-series-deployment/bootstrap-the-vm-series-firewall/prepare

NEW QUESTION: 100

An engineer has been asked to limit which routes are shared by running two different areas within an OSPF implementation. However, the devices share a common link for communication. Which virtual router configuration supports running multiple instances of the OSPF protocol over a single link?

A. ASBR

B. ECMP

C. OSPFv3
D. OSPF
Answer: C (LEAVE A REPLY)
Explanation
Support for multiple instances per link-With OSPFv3, you can run multiple instances of the OSPF protocol over a single link. This is accomplished by assigning an OSPFv3 instance ID number. An interface that is assigned to an instance ID drops packets that contain a different ID.
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-networking-admin/ospf/ospf-concepts/ospfv3

NEW QUESTION: 101
A firewall administrator has been tasked with ensuring that all Panorama-managed firewalls forward traffic logs to Panorama. In which section is this configured?
A. Panorama > Managed Devices
B. Monitor > Logs > Traffic
C. Device Groups > Objects > Log Forwarding
D. Templates > Device > Log Settings
Answer: C (LEAVE A REPLY)
Explanation
https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/manage-log-collection/configure-log-forwar

NEW QUESTION: 102
What steps should a user take to increase the NAT oversubscription rate from the default platform setting?
A. Navigate to Device > Setup > TCP Settings > NAT Oversubscription Rate
B. Navigate to Policies > NAT > Destination Address Translation > Dynamic IP (with session distribution)
C. Navigate to Policies > NAT > Source Address Translation > Dynamic IP (with session distribution)
D. Navigate to Device > Setup > Session Settings > NAT Oversubscription Rate
Answer: D (LEAVE A REPLY)
Explanation
NAT oversubscription is a feature that allows you to reuse a translated IP address and port for multiple source devices. This can help you conserve public IP addresses and increase the number of sessions that can be translated by a NAT rule.

NEW QUESTION: 103
A super user is tasked with creating administrator accounts for three contractors. For compliance purposes, all three contractors will be working with different device-groups m their hierarchy to deploy policies and objects.

Which type of role-based access is most appropriate for this project?
A. Create a Dynamic Admin with the Panorama Administrator role.
B. Create a Device Group and Template Admin.
C. Create a Custom Panorama Admin.
D. Create a Dynamic Read only superuser
Answer: (SHOW ANSWER)
Explanation
A Device Group and Template Admin is a type of role-based access that allows the administrator to assign different privileges for different device groups and templates. This is useful for managing multiple firewalls with different configuration needs. For example, the administrator can create a Device Group and Template Admin role that allows the contractors to deploy policies and objects only to their assigned device groups and templates1. The other options are not suitable for this project. A Dynamic Admin with the Panorama Administrator role has full access to all device groups and templates2. A Custom Panorama Admin can have limited access to device groups and templates, but cannot have different privileges for different device groups and templates3. A Dynamic Read only superuser can only view the configuration and logs, but cannot deploy policies and objects. References: 1:
https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/panorama-overview/role-based-access-contr
2:
https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/panorama-overview/role-based-access-contr
3:
https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/panorama-overview/role-based-access-contr
:
https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/panorama-overview/role-based-access-contr

NEW QUESTION: 104
WildFire will submit for analysis blocked files that match which profile settings?
A. files matching Anti-Spyware signatures
B. files that are blocked by URL filtering
C. files that are blocked by a File Blocking profile
D. files matching Anti-Virus signatures
Answer: D (LEAVE A REPLY)
Explanation
https://docs.paloaltonetworks.com/wildfire/u-v/wildfire-whats-new/latest-wildfire-cloud-features/wildfire-analys

NEW QUESTION: 105

The administrator for a small company has recently enabled decryption on their Palo Alto Networks firewall using a self-signed root certificate. They have also created a Forward Trust and Forward Untrust certificate and set them as such The admin has not yet installed the root certificate onto client systems What effect would this have on decryption functionality?

A. Decryption will function and there will be no effect to end users

B. Decryption will not function because self-signed root certificates are not supported

C. Decryption will not function until the certificate is installed on client systems

D. Decryption will function but users will see certificate warnings for each SSL site they visit

Answer: (SHOW ANSWER)

Explanation

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIEZCA0

NEW QUESTION: 106

A network security administrator wants to enable Packet-Based Attack Protection in a Zone Protection profile.

What are two valid ways to enable Packet-Based Attack Protection? (Choose two.)

A. ICMP Drop

B. TCP Drop

C. TCP Port Scan Block

D. SYN Random Early Drop

Answer: B,D (LEAVE A REPLY)

Explanation

Packet-Based Attack Protection is a feature of Zone Protection Profiles that allows the firewall to drop packets that are malformed, spoofed, or part of a port scan. TCP Drop and SYN Random Early Drop are two options under Packet-Based Attack Protection that can be enabled to protect against TCP-based attacks. TCP Drop enables the firewall to check for spoofed IP addresses, mismatched overlapping TCP segments, and invalid IP options. SYN Random Early Drop enables the firewall to drop SYN packets randomly when the SYN queue is full, preventing SYN flood attacks. ICMP Drop and TCP Port Scan Block are not valid options under Packet-Based Attack Protection

NEW QUESTION: 107

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?
A. Syslog listener
B. agentless User-ID with redistribution
C. standalone User-ID agent
D. captive portal
Answer: (SHOW ANSWER)
Explanation
A syslog listener is a User-ID agent that listens for syslog messages from network devices that contain user mapping information, such as network access control systems, domain controllers, or MDM solutions. By configuring a syslog listener on the firewall or Panorama and specifying the syslog format and filters, User-ID can parse the syslog messages and extract user mapping information from multiple sources. Agentless User-ID with redistribution is a method of using an existing firewall as a User-ID agent that redistributes user mappings to other firewalls or Panorama. This method does not involve syslog messages. A standalone User-ID agent is a software application that runs on a Windows server and collects user mappings from Active Directory servers or other sources. This method requires installing and managing a separate agent software. A captive portal is a web page that prompts users to authenticate before accessing certain network resources. This method does not involve syslog messages.
References:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/user-id/map-ip-addresses-to-users/syslog-mon
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/user-id/map-ip-addresses-to-users/user-id-age

NEW QUESTION: 108
An administrator has purchased WildFire subscriptions for 90 firewalls globally.
What should the administrator consider with regards to the WildFire infra-structure?
A. To comply with data privacy regulations, WildFire signatures and ver-dicts are not shared globally.
B. Palo Alto Networks owns and maintains one global cloud and four WildFire regional clouds.
C. Each WildFire cloud analyzes samples and generates malware signatures and verdicts independently of the other WildFire clouds.
D. The WildFire Global Cloud only provides bare metal analysis.
Answer: B (LEAVE A REPLY)
Explanation

According to the Palo Alto Networks website1, there are five WildFire public clouds that customers can choose from based on their location and data privacy requirements: WildFire Global Cloud (U.S.), WildFire Europe Cloud, WildFire Japan Cloud, WildFire Singapore Cloud, and WildFire United Kingdom Cloud. Additionally, there are three more regional public clouds that are available as of PAN-OS 10.0:
WildFire Canada Cloud, WildFire Australia Cloud, and WildFire Germany Cloud2. Therefore, the correct answer is B. References: 1: https://www.paloaltonetworks.com/network-security/wildfire 2: https://docs.paloaltonetworks.com/wildfire/9-1/wildfire-admin/wildfire-overview/wildfire-deployments/wildfire-

NEW QUESTION: 109
Given the screenshot, how did the firewall handle the traffic?
A. Traffic was allowed by policy but denied by profile as encrypted.
B. Traffic was allowed by policy but denied by profile as a threat.
C. Traffic was allowed by profile but denied by policy as a threat.
D. Traffic was allowed by policy but denied by profile as a nonstandard port.
Answer: B (LEAVE A REPLY)
Explanation
The screenshot shows the threat log which records the traffic that matches a threat signature or is blocked by a security profile. The log entry indicates that the traffic was allowed by the security policy rule "Allow-All" but was denied by the vulnerability protection profile "strict" as a threat. The threat name is "Microsoft Windows SMBv1 Multiple Vulnerabilities (MS17-010: EternalBlue)" and the action is "reset-both" which means that the firewall reset both the client and server connections. References: :
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/monitoring/use-syslog-for-monitoring/syslog-field

NEW QUESTION: 110
An administrator is configuring SSL decryption and needs 10 ensure that all certificates for both SSL Inbound inspection and SSL Forward Proxy are installed properly on the firewall. When certificates are being imported to the firewall for these purposes, which three certificates require a private key? (Choose three.)
A. Forward Untrust certificate
B. Forward Trust certificate
C. Enterprise Root CA certificate
D. End-entity (leaf) certificate
E. Intermediate certificate(s)
Answer: (SHOW ANSWER)
Explanation
This is discussed in the Palo Alto Networks PCNSE Study Guide in Chapter 9: Decryption, under the section

"SSL Forward Proxy and Inbound Inspection Certificates":
"When importing SSL decryption certificates, you need to provide private keys for the forward trust, forward untrust, and end-entity (leaf) certificates. You do not need to provide private keys for the root CA and intermediate certificates."

NEW QUESTION: 111
A firewall engineer creates a destination static NAT rule to allow traffic from the internet to a webserver hosted behind the edge firewall. The pre-NAT IP address of the server is 153.6 12.10, and the post-NAT IP address is 192.168.10.10. Refer to the routing and interfaces information below.
What should the NAT rule destination zone be set to?
A. None
B. Outside
C. DMZ
D. Inside
Answer: (SHOW ANSWER)
Explanation
The destination zone in the NAT rule is determined after the route lookup of the destination IP address in the original packet (that is, the pre-NAT destination IP address).
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-networking-admin/nat/nat-configuration-examples/destina The NAT rule destination zone should be set to the zone where the traffic is destined before NAT. In this case, the traffic from the internet is destined to the pre-NAT IP address of the server, which is 153.6.12.10. This IP address belongs to the Outside zone, as shown in the routing and interfaces information. Therefore, the NAT rule destination zone should be set to Outside. The other options are not correct. None is not a valid option for the NAT rule destination zone. Inside and DMZ are the zones where the traffic is destined after NAT, which is 192.168.10.10. References: :
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/networking/nat/source-and-destination-nat/configu

NEW QUESTION: 112
An engineer is tasked with configuring SSL forward proxy for traffic going to external sites.
Which of the following statements is consistent with SSL decryption best practices?
A. The forward trust certificate should not be stored on an HSM.
B. The forward untrust certificate should be signed by a certificate authority that is trusted by the clients.
C. Check both the Forward Trust and Forward Untrust boxes when adding a certificate for use with SSL decryption
D. The forward untrust certificate should not be signed by a Trusted Root CA
Answer: B (LEAVE A REPLY)
Explanation

According to the PCNSE Study Guide , SSL forward proxy is a feature that allows the firewall to decrypt and inspect SSL traffic going to external sites. The firewall acts as a proxy between the client and the server, generating a certificate on the fly for each site.
The best practices for configuring SSL forward proxy are
Use a forward trust certificate that is signed by a certificate authority (CA) that is trusted by the clients.
This certificate is used to sign certificates for sites that have valid certificates from trusted CAs. The clients will not see any certificate errors if they trust the forward trust certificate.
Use a forward untrust certificate that is not signed by a trusted CA. This certificate is used to sign certificates for sites that have invalid or untrusted certificates. The clients will see certificate errors if they do not trust the forward untrust certificate. This helps alert users of potential risks and prevent man-in-the-middle attacks.
Do not store the forward trust or untrust certificates on an HSM (hardware security module). The HSM does not support on-the-fly signing of certificates, which is required for SSL forward proxy.

NEW QUESTION: 113
A user at an external system with the IP address 65.124.57.5 queries the DNS server at 4. 2.2.2 for the IP address of the web server, www,xyz.com. The DNS server returns an address of 172.16.15.1 In order to reach Ire web server, which Security rule and NAT rule must be configured on the firewall?
A.
B.
C.
D.
Answer: C (LEAVE A REPLY)
Explanation
The addresses used in destination NAT rules always refer to the original IP address in the packet (that is, the pre-translated address). The destination zone in the NAT rule is determined after the route lookup of the destination IP address in the original packet (that is, the pre-NAT destination IP address). The addresses in the security policy also refer to the IP address in the original packet (that is, the pre-NAT address). However, the destination zone is the zone where the end host is physically connected. In other words, the destination zone in the security rule is determined after the route lookup of the post-NAT destination IP address.
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/networking/nat/nat-configuration-examples/destinat

NEW QUESTION: 114
Which data flow describes redistribution of user mappings?
A. User-ID agent to firewall
B. firewall to firewall
C. Domain Controller to User-ID agent

D. User-ID agent to Panorama

Answer: B (LEAVE A REPLY)

Explanation

https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/user-id/configure-firewalls-to-redistribute-u

https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/user-id/deploy-user-id-in-a-large-scale-network/redi

NEW QUESTION: 115

What type of address object would be useful for internal devices where the addressing structure assigns meaning to certain bits in the address, as illustrated in the diagram?

A. IP Netmask

B. IP Wildcard Mask

C. IP Address

D. IP Range

Answer: B (LEAVE A REPLY)

Explanation

https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/policy/use-address-object-to-represent-ip-addresse An IP Wildcard Mask address object is useful for internal devices where the addressing structure assigns meaning to certain bits in the address, as illustrated in the diagram. An IP Wildcard Mask address object specifies which source or destination addresses are subject to a Security policy rule. A zero (0) bit in the mask indicates that the bit being compared must match the bit in the IP address that is covered by the zero. A one (1) bit in the mask (a wildcard bit) indicates that the bit being compared need not match the bit in the IP address1. For example, if you want to match all cash registers in the northeastern U.S., you can use an IP Wildcard Mask address object of 10.132.1.0/0.0.2.255, which will match any IP address from 10.132.1.0 to

10.132.3.255. References: 1:

https://docs.paloaltonetworks.com/network-security/security-policy/objects/addresses

NEW QUESTION: 116

Which three items are import considerations during SD-WAN configuration planning? (Choose three.)

A. link requirements

B. the name of the ISP

C. IP Addresses

D. branch and hub locations

Answer: (SHOW ANSWER)

Explanation

https://docs.paloaltonetworks.com/sd-wan/1-0/sd-wan-admin/sd-wan-overview/plan-sd-wan-configuration

NEW QUESTION: 117
Which statement best describes the Automated Commit Recovery feature?
A. It performs a connectivity check between the firewall and Panorama after every configuration commit on the firewall. It reverts the configuration changes on the firewall if the check fails.
B. It restores the running configuration on a firewall and Panorama if the last configuration commit fails.
C. It performs a connectivity check between the firewall and Panorama after every configuration commit on the firewall. It reverts the configuration changes on the firewall and on Panorama if the check fails.
D. It restores the running configuration on a firewall if the last configuration commit fails.
Answer: A (LEAVE A REPLY)
Explanation
https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/administer-panorama/enable-automated-com The Automated Commit Recovery feature enables the firewall to automatically revert to a previous configuration if a commit operation causes connectivity loss between the firewall and Panorama. The feature performs a connectivity check between the firewall and Panorama after every configuration commit on the firewall. If the check fails, the firewall reverts to the last known good configuration and restores connectivity with Panorama. The feature does not restore the running configuration on a firewall or Panorama if the last commit fails, as this would require manual intervention. The feature does not revert the configuration changes on Panorama, as Panorama is not affected by the commit operation on the firewall. References:
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-new-features/panorama-features/automatic-panoram
https://docs.paloaltonetworks.com/panorama/10-1/panorama-admin/administer-panorama/enable-automate

NEW QUESTION: 118
An administrator analyzes the following portion of a VPN system log and notices the following issue
"Received local id 10 10 1 4/24 type IPv4 address protocol 0 port 0, received remote id 10.1.10.4/24 type IPv4 address protocol 0 port 0." What is the cause of the issue?
A. IPSec crypto profile mismatch
B. IPSec protocol mismatch
C. mismatched Proxy-IDs
D. bad local and peer identification IP addresses in the IKE gateway
Answer: (SHOW ANSWER)
Explanation
According to the Palo Alto Networks documentation, "A successful phase 2 negotiation requires not only that the security proposals match, but also the proxy-ids on either peer, be a mirror

image of each other. So it is mandatory to configure the proxy-IDs whenever you establish a tunnel between the Palo Alto Network firewall and the firewalls configured for policy-based VPNs." The log message indicates that the local and remote IDs are identical, which means they are not mirrored.
References: https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClW8CAK

NEW QUESTION: 119
A company has configured GlobalProtect to allow their users to work from home. A decrease in performance for remote workers has been reported during peak-use hours.
Which two steps are likely to mitigate the issue? (Choose TWO)
A. Exclude video traffic
B. Enable decryption
C. Block traffic that is not work-related
D. Create a Tunnel Inspection policy
Answer: (SHOW ANSWER)
Explanation
This is because excluding video traffic from being sent over the VPN will reduce the amount of bandwidth being used during peak hours, allowing more bandwidth to be available for other types of traffic. Blocking non-work related traffic will also reduce the amount of bandwidth being used, further freeing up bandwidth for work-related traffic.
Enabling decryption and creating a Tunnel Inspection policy are not likely to mitigate the issue of decreased performance during peak-use hours, as they do not directly address the issue of limited bandwidth availability during these times.
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PP3ICAW

NEW QUESTION: 120
A company requires that a specific set of ciphers be used when remotely managing their Palo Alto Networks appliances. Which profile should be configured in order to achieve this?
A. SSH Service profile
B. SSL/TLS Service profile
C. Decryption profile
D. Certificate profile
Answer: A (LEAVE A REPLY)
Explanation
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/certificate-management/configure-an-ssh-service-p

NEW QUESTION: 121

An administrator has 750 firewalls. The administrator's central-management Panorama instance deploys dynamic updates to the firewalls. The administrator notices that the dynamic updates from Panorama do not appear on some of the firewalls.
If Panorama pushes the configuration of a dynamic update schedule to managed firewalls, but the configuration does not appear, what is the root cause?
A. Panorama does not have valid licenses to push the dynamic updates.
B. Panorama has no connection to Palo Alto Networks update servers.
C. No service route is configured on the firewalls to Palo Alto Networks update servers.
D. Locally-defined dynamic update settings take precedence over the settings that Panorama pushed.
Answer: D (LEAVE A REPLY)
Explanation
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClKQCA0
"Locally defined dynamic updates setting on a managed Palo Alto Networks firewall take preference over the Panorama pushed setting."

NEW QUESTION: 122
An administrator needs firewall access on a trusted interface. Which two components are required to configure certificate based, secure authentication to the web UI? (Choose two)
A. certificate profile
B. server certificate
C. SSH Service Profile
D. SSL/TLS Service Profile
Answer: (SHOW ANSWER)
Explanation
To configure certificate-based, secure authentication to the web UI, two components are required: a certificate profile and a server certificate. A certificate profile defines the trusted certificate authorities (CAs) for verifying client certificates and server certificates . A server certificate is a digital certificate that identifies the firewall to clients and servers2. The firewall can use a self-signed certificate or a certificate signed by an external CA as the server certificate for web UI access3. The server certificate must be assigned to an SSL/TLS service profile, which specifies the SSL/TLS protocol version and cipher suites for secure communication4. The SSL/TLS service

profile must be selected in the general settings of the firewall management interface. References: 1: https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/certificate-management/certificate-profiles 2: https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/certificate-management/generate-a-certificate-on-th
3: https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClFGCA0 4: https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/certificate-management/ssl-tls-service-profiles : https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/firewall-administration/manage-firewall-administra

NEW QUESTION: 123
What happens when an A/P firewall cluster synchronies IPsec tunnel security associations (SAs)?
A. Phase 2 SAs are synchronized over HA2 links
B. Phase 1 and Phase 2 SAs are synchronized over HA2 links
C. Phase 1 SAs are synchronized over HA1 links
D. Phase 1 and Phase 2 SAs are synchronized over HA3 links
Answer: (SHOW ANSWER)
Explanation
From the Palo Alto documentation below, "when a VPN is terminated on a Palo Alto firewall HA pair, not all IPSEC related information is synchronized between the firewalls... This is an expected behavior. IKE phase 1 SA information is NOT synchronized between the HA firewalls." And from the second link, "Data link (HA2) is used to sync sessions, forwarding tables, IPSec security associations, and ARP tables between firewalls in the HA pair. Data flow on the HA2 link is always unidirectional (except for the HA2 keep-alive). It flows from the active firewall to the passive firewall."
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000HAuZCAW&lang=en_US%E

NEW QUESTION: 124
During the process of developing a decryption strategy and evaluating which websites are required for corporate users to access, several sites have been identified that cannot be decrypted due to technical reasons.
In this case, the technical reason is unsupported ciphers. Traffic to these sites will therefore be blocked if decrypted How should the engineer proceed?
A. Allow the firewall to block the sites to improve the security posture
B. Add the sites to the SSL Decryption Exclusion list to exempt them from decryption
C. Install the unsupported cipher into the firewall to allow the sites to be decrypted
D. Create a Security policy to allow access to those sites
Answer: B (LEAVE A REPLY)

Explanation
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/decryption-exclusions
Traffic that breaks decryption for technical reasons, such as using a pinned certificate, an incomplete certificate chain, unsupported ciphers, or mutual authentication (attempting to decrypt the traffic results in blocking the traffic).
Palo Alto Networks provides a predefined SSL Decryption Exclusion list (DeviceCertificate ManagementSSL Decryption Exclusion) that excludes hosts with applications and services that are known to break decryption technically from SSL Decryption by default. If you encounter sites that break decryption technically and are not on the SSL Decryption Exclusion list, you can add them to list manually by server hostname. The firewall blocks sites whose applications and services break decryption technically unless you add them to the SSL Decryption Exclusion list.

NEW QUESTION: 125
A customer is replacing their legacy remote access VPN solution The current solution is in place to secure only internet egress for the connected clients Prisma Access has been selected to replace the current remote access VPN solution During onboarding the following options and licenses were selected and enabled
- Prisma Access for Remote Networks 300Mbps
- Prisma Access for Mobile Users 1500 Users
- Cortex Data Lake 2TB
- Trusted Zones trust
- Untrusted Zones untrust
- Parent Device Group shared
How can you configure Prisma Access to provide the same level of access as the current VPN solution?
A. Configure mobile users with trust-to-untrust Security policy rules to allow the desired traffic outbound to the internet
B. Configure mobile users with a service connection and trust-to-trust Security policy rules to allow the desired traffic outbound to the internet
C. Configure remote networks with a service connection and trust-to-untrust Security policy rules to allow the desired traffic outbound to the internet
D. Configure remote networks with trust-to-trust Security policy rules to allow the desired traffic outbound to the internet
Answer: (SHOW ANSWER)
Explanation
To provide the same level of access as the current VPN solution, which is to secure only Internet egress for the connected clients, you can configure mobile users with trust-to-untrust Security policy rules to allow the desired traffic outbound to the Internet. This way, the mobile users will be assigned an IP address from a pool that belongs to the trust zone, and they will be able to access the Internet through Prisma Access using a gateway that belongs to the untrust zone1. You do

not need to configure a service connection for this scenario, as a service connection is used to enable access between mobile users and remote networks or private apps2
. You also do not need to configure trust-to-trust Security policy rules, as they are used to enable access between mobile users and other trusted resources
https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-panorama-admin/prepare-the-prisma-acc
2:
https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-cloud-managed-admin/prisma-access-ser
3:
https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-cloud-managed-admin/prisma-access-mo

NEW QUESTION: 126
Which log type will help the engineer verify whether packet buffer protection was activated?
A. Data Filtering
B. Configuration
C. Threat
D. Traffic
Answer: C (LEAVE A REPLY)
Explanation
The log type that will help the engineer verify whether packet buffer protection was activated is Threat Logs.
Threat Logs are logs generated by the Palo Alto Networks firewall when it detects a malicious activity on the network. These logs contain information about the source, destination, and type of threat detected. They also contain information about the packet buffer protection that was activated in response to the detected threat.
This information can help the engineer verify that packet buffer protection was activated and determine which actions were taken in response to the detected threat.
Packet buffer protection is a feature that prevents packet buffer exhaustion by dropping packets, discarding sessions, or blocking source IP addresses when the packet buffer utilization exceeds a certain threshold. The firewall records these events in the threat log with different threat IDs and names1. The system log also records an alert event when the packet buffer congestion reaches the alert threshold2. The other types of logs do not show packet buffer protection events.
References:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/zone-protection-and-dos-protection/zone-defense/p
2:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/monitoring/use-syslog-for-monitoring/syslog-field

NEW QUESTION: 127
An engineer wants to implement the Palo Alto Networks firewall in VWire mode on the internet gateway and wants to be sure of the functions that are supported on the vwire interface What are three supported functions on the VWire interface? (Choose three)
A. NAT
B. QoS
C. IPSec
D. OSPF
E. SSL Decryption
Answer: (SHOW ANSWER)
Explanation
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/networking/configure-interfaces/virtual-wire-interfa
"The virtual wire supports blocking or allowing traffic based on virtual LAN (VLAN) tags, in addition to supporting security policy rules, App-ID, Content-ID, User-ID, decryption, LLDP, active/passive and active/active HA, QoS, zone protection (with some exceptions), non-IP protocol protection, DoS protection, packet buffer protection, tunnel content inspection, and NAT."

NEW QUESTION: 128
Which feature of Panorama allows an administrator to create a single network configuration that can be reused repeatedly for large-scale deployments even if values of configured objects, such as routes and interface addresses, change?
A. Template stacks
B. Template variables
C. The Shared device group
D. A device group
Answer: B (LEAVE A REPLY)
Explanation
Template variables are placeholders that you can use in a template or a template stack to represent values that differ across firewalls, such as IP addresses, hostnames, or interface names. Template variables allow you to create a single network configuration that can be reused repeatedly for large-scale deployments even if values of configured objects change1. Option A is incorrect because template stacks are used to group multiple templates together and apply them to firewalls or device groups. Template stacks do not allow you to use variables for different values2. Option C is incorrect because the Shared device group is used to push policies and objects that are common across all firewalls managed by Panorama. The Shared device group does not allow you to use variables for different values . Option D is incorrect because a device group is used to group firewalls that require similar policies and objects. A device group does not allow you to use variables for different values3.

NEW QUESTION: 129

A network engineer has discovered that asymmetric routing is causing a Palo Alto Networks firewall to drop traffic. The network architecture cannot be changed to correct this.
Which two actions can be taken on the firewall to allow the dropped traffic permanently? (Choose two.)
A. Navigate to Network > Zone Protection Click Add
Select Packet Based Attack Protection > TCP/IP Drop Set "Reject Non-syn-TCP" to No Set "Asymmetric Path" to Bypass
B. > set session tcp-reject-non-syn no
C. Navigate to Network > Zone Protection Click Add
Select Packet Based Attack Protection > TCP/IP Drop Set "Reject Non-syn-TCP" to Global Set "Asymmetric Path" to Global
D. # set deviceconfig setting session tcp-reject-non-syn no
Answer: A,D (LEAVE A REPLY)
Explanation
Option A is correct because setting "Reject Non-syn-TCP" to No and "Asymmetric Path" to Bypass in the Zone Protection profile disables the TCP checks that can cause the firewall to drop packets due to asymmetric routing. This allows the firewall to accept non-SYN TCP packets without a session match and packets that are out of sequence or out of window.
Option D is correct because setting session tcp-reject-non-syn to no in the CLI also disables the TCP checks that can cause the firewall to drop packets due to asymmetric routing. This allows the firewall to accept non-SYN TCP packets without a session match and packets that are out of sequence or out of window.
Option B is incorrect because setting session tcp-reject-non-syn to no in the CLI has the same effect as setting "Reject Non-syn-TCP" to No in the Zone Protection profile, so there is no need to do both. Also, setting "Asymmetric Path" to Global in the Zone Protection profile does not disable the TCP checks that can cause the firewall to drop packets due to asymmetric routing. It only allows the firewall to use a global timer for asymmetric path detection instead of a per-session timer.
Option C is incorrect because setting "Reject Non-syn-TCP" to Global and "Asymmetric Path" to Global in the Zone Protection profile does not disable the TCP checks that can cause the firewall to drop packets due to asymmetric routing. It only allows the firewall to use a global timer for both non-SYN TCP rejection and asymmetric path detection instead of a per-session timer.
References:
1 https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClReCAK
2 https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClSHCA0

NEW QUESTION: 130
A remote administrator needs firewall access on an untrusted interface. Which two components are required on the firewall to configure certificate-based administrator authentication to the web UI? (Choose two)
A. client certificate

B. certificate profile
C. certificate authority (CA) certificate
D. server certificate
Answer: B,C (LEAVE A REPLY)
Explanation
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/firewall-administration/manage-firewall-administrat

NEW QUESTION: 131
What are two best practices for incorporating new and modified App-IDs? (Choose two.)
A. Run the latest PAN-OS version in a supported release tree to have the best performance for the new App-IDs
B. Configure a security policy rule to allow new App-IDs that might have network-wide impact
C. Perform a Best Practice Assessment to evaluate the impact of the new or modified App-IDs
D. Study the release notes and install new App-IDs if they are determined to have low impact
Answer: B,D (LEAVE A REPLY)
Explanation
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/app-id/manage-new-app-ids-introduced-in-content-r

NEW QUESTION: 132
Where can a service route be configured for a specific destination IP?
A. Use Network > Virtual Routers, select the Virtual Router > Static Routes > IPv4
B. Use Device > Setup > Services > Services
C. Use Device > Setup > Services > Service Route Configuration > Customize > Destination
D. Use Device > Setup > Services > Service Route Configuration > Customize > IPv4
Answer: (SHOW ANSWER)
Explanation
A service route is the path from the interface to the service on a server. By default, the firewall uses the management interface to communicate to various servers, including DNS, Email, Palo Alto Updates, User-ID agent, Syslog, Panorama, dynamic updates, URL updates, licenses, and AutoFocus. etc. Sometimes, it is necessary to use an alternative path other than Firewall management IP due to many restrictions. To configure service routes for non-predefined services, the destination addresses can be manually entered in the Destination section under Device > Setup > Services > Service Route Configuration > Customize1. Option A is incorrect because it is used to configure static routes for network traffic, not service routes for firewall services. Option B is incorrect because it is used to configure general service settings such as NTP server and proxy server, not service routes for specific destinations. Option D is incorrect because it is used to configure service routes for predefined services such as DNS and Syslog, not service routes for non-predefined services2
.

NEW QUESTION: 133
Which profile generates a packet threat type found in threat logs?
A. Zone Protection
B. WildFire
C. Anti-Spyware
D. Antivirus
Answer: A (LEAVE A REPLY)
Explanation
"Threat/Content Type (subtype) Subtype of threat log." "packet-Packet-based attack protection triggered by a Zone Protection profile."
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/monitoring/use-syslog-for-monitoring/syslog-field
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/monitoring/use-syslog-for-monitoring/syslog-field packet-Packet-based attack protection triggered by a Zone Protection profile.

NEW QUESTION: 134
View the screenshots. A QoS profile and policy rules are configured as shown. Based on this information, which two statements are correct? (Choose two.)
A. DNS has a higher priority and more bandwidth than SSH.
B. Google-video has a higher priority and more bandwidth than WebEx.
C. SMTP has a higher priority but lower bandwidth than Zoom.
D. Facetime has a higher priority but lower bandwidth than Zoom.
Answer: A,B (LEAVE A REPLY)
Explanation
The QoS profile assigns different classes and guaranteed bandwidth percentages to different applications. The QoS policy rules apply the QoS profile to the traffic based on the source and destination zones. The priority of a class is determined by its number, with lower numbers having higher priority. The bandwidth of a class is determined by its guaranteed percentage, with higher percentages having more bandwidth. Based on this information, DNS belongs to class 1 which has the highest priority (1) and the most bandwidth (40%). SSH belongs to class 4 which has the lowest priority (4) and the least bandwidth (5%). Therefore, DNS has a higher priority and more bandwidth than SSH. Similarly, Google-video belongs to class 2 which has the second highest priority (2) and the second most bandwidth (30%). WebEx belongs to class 3 which has the third highest priority (3) and the third most bandwidth (25%). Therefore, Google-video has a higher priority and more bandwidth than WebEx. References: :
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/quality-of-service/qos-concepts/qos-profiles

NEW QUESTION: 135

An engineer needs to see how many existing SSL decryption sessions are traversing a firewall What command should be used?

A. show dataplane pool statistics I match proxy

B. debug dataplane pool statistics I match proxy

C. debug sessions I match proxy

D. show sessions all

Answer: B (LEAVE A REPLY)

Explanation

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClhdCAC

NEW QUESTION: 136

What happens, by default, when the GlobalProtect app fails to establish an IPSec tunnel to the GlobalProtect gateway?

A. It stops the tunnel-establishment processing to the GlobalProtect gateway immediately.

B. It tries to establish a tunnel to the GlobalProtect gateway using SSL/TLS.

C. It keeps trying to establish an IPSec tunnel to the GlobalProtect gateway.

D. It tries to establish a tunnel to the GlobalProtect portal using SSL/TLS.

Answer: (SHOW ANSWER)

Explanation

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClfoCAC

"Should the IPSec connection fail, VPN will fall back to SSL protocol."

Valid PCNSE Dumps shared by Actual4test.com for Helping Passing PCNSE Exam! Actual4test.com now offer the **newest PCNSE exam dumps**, the Actual4test.com PCNSE exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com PCNSE dumps with Test Engine here: https://www.actual4test.com/PCNSE_examcollection.html (**375** Q&As Dumps, **30%OFF** **Special Discount: Freepdfdumps**)