PaloAltoNetworks.PCNSE.v2023-06-02.q103

Exam Code:	PCNSE
Exam Name:	Palo Alto Networks Certified Network Security Engineer Exam
Certification Provider:	Palo Alto Networks
Free Question Number:	103
Version:	v2023-06-02
# of views:	4198
# of Questions views:	1030
https://www.freepdfdumps.com/PaloAltoNetworks.PCNSE.v2023-06-02.q103.html	

NEW QUESTION: 1
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. Install the unsupported cipher into the firewall to allow the sites to be decrypted
B. Add the sites to the SSL Decryption Exclusion list to exempt them from decryption
C. Create a Security policy to allow access to those sites
D. Allow the firewall to block the sites to improve the security posture
Answer: D (LEAVE A REPLY)

NEW QUESTION: 2
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. App-ID
C. source and destination IP addresses
D. source users
E. GlobalProtect HIP
Answer: A,C,D (LEAVE A REPLY)

NEW QUESTION: 3
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: D (LEAVE A REPLY)

Explanation

When an administrator has numerous firewalls and Panorama, WildFire logs need to be forwarded from the firewalls to Panorama in order for them to be visible in Panorama. WildFire logs contain information about malicious files that have been detected by WildFire and provide detailed information such as the file's hash value, severity, and other attributes. This information can then be used to help identify threats and take appropriate security measures. Proper configuration of forwarding WildFire logs is essential for monitoring malicious activity and ensuring the security of the network.

NEW QUESTION: 4

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. default routing

B. summarized BGP routes before advertising

C. hot potato routing

D. target service connection for traffic steering

Answer: C (LEAVE A REPLY)

NEW QUESTION: 5

A network security administrator has been tasked with deploying User-ID in their organization.

What are three valid methods of collecting User-ID information in a network? (Choose three.)

A. Windows User-ID agent

B. GlobalProtect

C. XMLAPI

D. External dynamic list

E. Dynamic user groups

Answer: (SHOW ANSWER)

Explanation

User-ID is a feature that enables the firewall to identify users and groups based on their IP addresses, usernames, or other attributes.

There are three valid methods of collecting User-ID information in a network:

* Windows User-ID agent: This is a software agent that runs on a Windows server and collects user mapping information from Active Directory, Exchange servers, or other sources.
* GlobalProtect: This is a VPN solution that provides secure remote access for users and devices. It also collects user mapping information from endpoints that connect to the firewall using GlobalProtect.
* XMLAPI: This is an application programming interface that allows third-party applications or scripts to send user mapping information to the firewall using XML format.

NEW QUESTION: 6
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: (SHOW ANSWER)
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: 7
An administrator is receiving complaints about application performance degradation. After checking the ACC.
the administrator observes that there Is an excessive amount of SSL traffic Which three elements should the administrator configure to address this issue? (Choose three.)
A. QoS on the ingress Interface for the traffic flows
B. A QoS policy for each application ID
C. QoS on the egress interface for the traffic flows
D. A QoS profile defining traffic classes
E. An Application Override policy for the SSL traffic
Answer: B,D,E (LEAVE A REPLY)

NEW QUESTION: 8

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: 9

A firewall engineer creates a new App-ID report under Monitor > Reports > Application Reports > New Application to monitor new applications on the network and better assess any Security policy updates the engineer might want to make.

How does the firewall identify the New App-ID characteristic?

A. It matches to the New App-IDs downloaded in the last 30 days.

B. It matches to the New App-IDs downloaded in the last 90 days

C. It matches to the New App-IDs installed since the last time the firewall was rebooted

D. It matches to the New App-IDs in the most recently installed content releases.

Answer: D (LEAVE A REPLY)

Explanation

When creating a new App-ID report under Monitor > Reports > Application Reports > New Application, the firewall identifies new applications based on the New App-IDs in the most recently installed content releases.

The New App-IDs are the application signatures that have been added in the latest content release, which can be found under Objects > Security Profiles > Application. This allows the engineer to monitor any new applications that have been added to the firewall's database and evaluate whether to allow or block them with a Security policy update.

NEW QUESTION: 10

An engineer needs to collect User-ID mappings from the company's existing proxies.

What two methods can be used to pull this data from third party proxies? (Choose two.)

A. Syslog

B. Client probing
C. Server Monitoring
D. XFF Headers
Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 11
An engineer configures SSL decryption in order to have more visibility to the internal users' traffic when it is regressing the firewall.
Which three types of interfaces support SSL Forward Proxy? (Choose three.)
A. High availability (HA)
B. Layer
C. Virtual Wire
D. Tap
E. Layer 3
Answer: (SHOW ANSWER)
Explanation
SSL Forward Proxy is a feature that allows the firewall to decrypt and inspect outbound SSL traffic from internal users to external servers1. The firewall acts as a proxy (MITM) generating a new certificate for the accessed URL and presenting it to the client during SSL handshake2.
SSL Forward Proxy can be configured on any interface type that supports security policies, which are Layer 2, Virtual Wire, and Layer 3 interfaces1. These interface types allow the firewall to apply security profiles and URL filtering on the decrypted SSL traffic.

NEW QUESTION: 12
An engineer must configure the Decryption Broker feature. To which router must the engineer assign the decryption forwarding interfaces that are used in Decryption Broker security chain?
A. A virtual router that has no additional interfaces for passing data-type traffic and no other configured routes than those used for the security chain.
B. The default virtual router. If there is no default virtual router , the engineer must create one during setup.
C. A virtual router that is configured with at least one dynamic routing protocol and has at least one entry in the RIB
D. The virtual router that routes the traffic that the Decryption Broker security chain inspects.
Answer: D (LEAVE A REPLY)
Explanation
Decryption Broker is a feature that allows you to use a Palo Alto Networks firewall as a decryption broker for other security devices in your network . It works by decrypting traffic on one interface and forwarding it to another interface where it can be inspected by other devices before being re-encrypted and sent to its destination2. The firewall acts as a transparent bridge between the two interfaces and does not change the source or destination IP addresses of the traffic To configure Decryption Broker, you need to assign decryption forwarding interfaces (DFIs) to the virtual router

that routes the traffic that you want to inspect. The DFIs are used to forward decrypted traffic from one interface to another in a security chain3. A security chain is a set of devices that perform different security functions on the same traffic flow3. You can have multiple security chains for different types of traffic or different segments of your network3.
The reason why you need to assign DFIs to the virtual router that routes the traffic is because Decryption Broker uses routing tables to determine which DFI belongs to which security chain and how to forward traffic between them2. If you assign DFIs to a different virtual router than the one that routes the traffic, Decryption Broker will not be able to find them or forward traffic correctly2.

NEW QUESTION: 13
In SSL Forward Proxy decryption, which two certificates can be used for certificate signing? (Choose two.)
A. wildcard server certificate
B. enterprise CA certificate
C. client certificate
D. server certificate
E. self-signed CA certificate
Answer: B,E (LEAVE A REPLY)
Explanation
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/decryption/configure-ssl-forward-proxy.html

NEW QUESTION: 14
An administrator is required to create an application-based Security policy rule to allow Evernote. The Evernote application implicitly uses SSL and web browsing. What is the minimum the administrator needs to configure in the Security rule to allow only Evernote?
A. Add the HTTP, SSL, and Evernote applications to the same Security policy
B. Add only the Evernote application to the Security policy rule.
C. Add the Evernote application to the Security policy rule, then add a second Security policy rule containing both HTTP and SSL.
D. Create an Application Override using TCP ports 443 and 80.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 15
With the default TCP and UDP settings on the firewall, what will be the identified application in the following session?
A. Incomplete
B. Insufficient-data
C. not-applicable
D. unknown-udp

Answer: D (LEAVE A REPLY)

NEW QUESTION: 16
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 remote networks with a service connection and trust-to-untrust Security policy rules to allow the desired traffic outbound to the internet
C. Configure remote networks with trust-to-trust Security policy rules to allow the desired traffic outbound to the internet
D. Configure mobile users with a service connection and trust-to-trust Security policy rules to allow the desired traffic outbound to the internet
Answer: (SHOW ANSWER)

NEW QUESTION: 17
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: C (LEAVE A REPLY)

NEW QUESTION: 18
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)
A. Option D
B. Option B
C. Option A
D. Option C
Answer: D (LEAVE A REPLY)

NEW QUESTION: 19
An engineer is in the planning stages of deploying User-ID in a diverse directory services environment.
Which server OS platforms can be used for server monitoring with User-ID?
A. Microsoft Terminal Server, Red Hat Linux, and Microsoft Active Directory
B. Microsoft Active Directory, Red Hat Linux, and Microsoft Exchange
C. Microsoft Exchange, Microsoft Active Directory, and Novell eDirectory
D. Novell eDirectory, Microsoft Terminal Server, and Microsoft Active Directory
Answer: (SHOW ANSWER)
Explanation
https://docs.paloaltonetworks.com/compatibility-matrix/user-id-agent/which-servers-can-the-user-id-agent-monit

NEW QUESTION: 20
A firewall administrator requires an A/P HA pair to fail over more quickly due to critical business application uptime requirements.
What is the correct setting?
A. Change the HA timer profile to "aggressive" or customize the settings in advanced profile.
B. Change the HA timer profile to "fast".
C. Change the HA timer profile to "user-defined" and manually set the timers.
D. Change the HA timer profile to "quick" and customize in advanced profile.
Answer: (SHOW ANSWER)

Explanation
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/high-availability/set-up-activepassive-ha/configure In an A/P HA pair, HA (High Availability) timers are used to determine how quickly the firewall should fail over in case of a failure. Typically, the firewall administrator can choose between several predefined timer profiles such as "normal", "aggressive", and "fast". Changing the HA timer profile to "user-defined" and manually setting the timers would allow the administrator to fine-tune the failover timing and make sure it meets the uptime requirements for the critical business applications. This approach allows the administrator to set the timers to the lowest possible value without compromising the stability and security of the firewall.

NEW QUESTION: 21
Refer to the diagram. Users at an internal system want to ssh to the SSH server The server is configured to respond only to the ssh requests coming from IP 172.16.16.1.
In order to reach the SSH server only from the Trust zone, which Security rule and NAT rule must be configured on the firewall?
A)
B)
C)
D)
A. Option D
B. Option C
C. Option B
D. Option A
Answer: B (LEAVE A REPLY)

NEW QUESTION: 22
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. # set deviceconfig setting session tcp-reject-non-syn no
B. 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
C. > set session tcp-reject-non-syn no
D. 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
Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 23

An engineer is troubleshooting traffic routing through the virtual router. The firewall uses multiple routing protocols, and the engineer is trying to determine routing priority Match the default Administrative Distances for each routing protocol.

Answer:

Explanation

* Static

-Range is 10-240; default is 10.

* OSPF Internal

-Range is 10-240; default is 30.

* OSPF External

-Range is 10-240; default is 110.

* IBGP

-Range is 10-240; default is 200.

* EBGP

-Range is 10-240; default is 20.

* RIP

-Range is 10-240; default is 120.

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/networking/virtual-routers

NEW QUESTION: 24

Which statement accurately describes service routes and virtual systems?

A. The interface must be used for traffic to the required external services.

B. Virtual systems cannot have dedicated service routes configured; and virtual systems always use the global service and service route settings for the firewall.

C. Virtual systems that do not have specific service routes configured inherit the global service and service route settings for the firewall.

D. Virtual systems can only use one interface for all global service and service routes of the firewall.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 25

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 Directory1. 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: 26
Which three actions can Panorama perform when deploying PAN-OS images to its managed devices? (Choose three.)
A. install and reboot
B. upload and install and reboot
C. verify and install
D. upload-only
E. upload and install
Answer: A,C,E (LEAVE A REPLY)

NEW QUESTION: 27
A network administrator is troubleshooting an issue with Phase 2 of an IPSec VPN tunnel. The administrator determines that the lifetime needs to be changed to match the peer.
Where should this change be made?
A. IPSec Crypto profile
B. IPSec Tunnel settings
C. IKE Crypto profile
D. IKE Gateway profile
Answer: (SHOW ANSWER)

NEW QUESTION: 28
Which statement best describes the Automated Commit Recovery feature?
A. It restores the running configuration on a firewall and Panorama if the last configuration commit fails.

B. 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.
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: B (LEAVE A REPLY)

NEW QUESTION: 29
You have upgraded your Panorama and Log Collectors lo 10.2 x. Before upgrading your firewalls using Panorama, what do you need do?
A. Commit and Push the configurations to the firewalls.
B. Re-associate the firewalls in Panorama/Managed Devices/Summary.
C. Refresh your licenses with Palo Alto Network Support - Panorama/Licenses/Retrieve License Keys from License Server.
D. Refresh the Mastor Key in Panorama/Master Key and Diagnostic
Answer: A (LEAVE A REPLY)

NEW QUESTION: 30
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; however, there were not enough packets to identify the application.
B. A handshake did not take place, and the application could not be identified.
C. A handshake took place, but no data packets were sent prior to the timeout.
D. A handshake did take place, but the application could not be identified.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 31
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 browser . 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: 32
During a laptop-replacement project, remote users must be able to establish a GlobalProtect VPN connection to the corporate network before logging in to their new Windows 10 endpoints.
The new laptops have the 5.2.10 GlobalProtect Agent installed, so the administrator chooses to use the Connect Before Logon feature to solve this issue.
What must be configured to enable the Connect Before Logon feature?
A. Registry keys on the Windows system.
B. X-Auth Support in the GlobalProtect Gateway Tunnel Settings.
C. The Certificate profile in the GlobalProtect Portal Authentication Settings.
D. The GlobalProtect Portal Agent App Settings Connect Method to Pre-logon then On-demand.
Answer: (SHOW ANSWER)

NEW QUESTION: 33
Which CLI command displays the physical media that are connected to ethernet1/8?
A. > show system state filter-pretty sys.si.p8.stats
B. > show system state filter-pretty sys.sl.p8.phy

C. > show interface ethernet1/8
D. > show system state filter-pretty sys.sl.p8.med
Answer: (SHOW ANSWER)
Explanation
Example output:
> show system state filter-pretty sys.s1.p1.phy
sys.s1.p1.phy: {
link-partner: { },
media: CAT5,
type: Ethernet,
}
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Cld3CAC

NEW QUESTION: 34
Which statement is correct given the following message from the PanGPA log on the GlobalProtect app?
Failed to connect to server at port:47 67
A. The GlobalProtect app failed to connect to the GlobalProtect Portal on port 4767
B. The PanGPS process failed to connect to the PanGPA process on port 4767
C. The PanGPA process failed to connect to the PanGPS process on port 4767
D. The GlobalProtect app failed to connect to the GlobalProtect Gateway on port 4767
Answer: D (LEAVE A REPLY)

NEW QUESTION: 35
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 2 SAs are synchronized over HA2 links.
C. Phase 1 and Phase 2 SAs are synchronized over HA2 links.
D. Phase 1 SAs are synchronized over HA1 links.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 36
A Security policy rule is configured with a Vulnerability Protection Profile and an action of "Deny." Which action will this configuration cause on the matched traffic?
A. The Profile Settings section will be grayed out when the Action is set to "Deny"
B. It will cause the firewall to skip this Security policy rule. A warning will be displayed during a commit
C. The configuration will allow the matched session unless a vulnerability signature is detected.
D. The "Deny" action will supersede the per-severity defined actions defined in the associated Vulnerability Protection Profile It will cause the firewall to deny the matched sessions.

Any configured Security Profiles have no effect if the Security policy rule action is set to "Deny"
Answer: D (LEAVE A REPLY)
Explanation
https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/policy/security-profiles.html
First note in above link states:
"Security profiles are not used in the match criteria of a traffic flow.
The security profile is applied to scan traffic after the application or category is allowed by the security policy."
The first thing the firewall checks per it's flow is the security policy match and action.
The Security Profile never gets checked if a match happens on a policy set to deny that match.

NEW QUESTION: 37
How would an administrator configure a Bidirectional Forwarding Detection profile for BGP after enabling the Advance Routing Engine run on PAN-OS 10.2?
A. create a BFD profile under Network > Network Profiles > BFD Profile and then select the BFD profile under Network > Virtual Router > BGP > BFD
B. create a BFD profile under Network > Routing > Routing Profiles > BFD and then select the BFD profile under Network > Routing > Logical Routers > BGP > General > Global BFD Profile
C. create a BFD profile under Network > Network Profiles > BFD Profile and then select the BFD profile under Network > Routing > Logical Routers > BGP > BFD
D. create a BFD profile under Network > Routing > Routing Profiles > BFD and then select the BFD profile under Network > Virtual Router > BGP > General > Global BFD Profile
Answer: D (LEAVE A REPLY)

NEW QUESTION: 38
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: 39
Where is Palo Alto Networks Device Telemetry data stored on a firewall with a device certificate installed?
A. Cortex Data Lake
B. Panorama

C. On Palo Alto Networks Update Servers
D. M600 Log Collectors
Answer: A (LEAVE A REPLY)
Explanation
The Device Telemetry data is stored on Cortex Data Lake , which is a cloud-based service that collects and stores logs from your firewalls and other sources. Cortex Data Lake also enables you to analyze and visualize your data using various applications.
To use Device Telemetry, you need to install a device certificate on your firewall3. This certificate authenticates your firewall to Cortex Data Lake and encrypts the data in transit.

NEW QUESTION: 40
A network engineer troubleshoots a VPN Phase 2 mismatch and decides that PFS (Perfect Forward Secrecy) needs to be enabled.
What action should the engineer take?
A. Select the appropriate DH Group under the IPSec Crypto profile.
B. Enable PFS under the IKE gateway advanced options
C. Add an authentication algorithm in the IPSec Crypto profile.
D. Enable PFS under the IPSec Tunnel advanced options.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 41
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. Use the tcpdump command.
D. Enable all four stages of traffic capture (TX, RX, DROP, Firewall).
Answer: (SHOW ANSWER)

NEW QUESTION: 42
When an in-band data port is set up to provide access to required services, what is required for an interface that is assigned to service routes?
A. The interface must be used for traffic to the required services
B. You must enable DoS and zone protection
C. You must set the interface to Layer 2 Layer 3. or virtual wire
D. You must use a static IP address
Answer: D (LEAVE A REPLY)
Explanation
According to the Palo Alto Networks documentation, "To configure a service route, you must specify a source interface and a source address. The source interface can be any data port

(Ethernet interface) or a loopback interface. The source address must be a static IP address that is configured on the source interface." References: https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-networking-admin/service-routes/service-routes-overview

NEW QUESTION: 43
Which Panorama feature protects logs against data loss if a Panorama server fails?
A. Panorama Collector Group automatically ensures that no logs are lost if a server fails inside the Collector Group
B. Panorama Collector Group with Log Redundancy ensures that no logs are lost if a server fails inside the Collector Group.
C. Panorama HA automatically ensures that no logs are lost if a server fails inside the HA Cluster.
D. Panorama HA with Log Redundancy ensures that no logs are lost if a server fails inside the HA Cluster.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 44
How should an administrator enable the Advance Routing Engine on a Palo Alto Networks firewall?
A. Enable Advanced Routing Engine in Device > Setup > Session > Session Settings, then commit and reboot.
B. Enable Advanced Routing in Network > Virtual Routers > Redistribution Profiles and then commit.
C. Enable Advanced Routing in Network > Virtual Routers > Router Settings > General, then commit and reboot.
D. Enable Advanced Routing in General Settings of Device > Setup > Management, then commit and reboot
Answer: (SHOW ANSWER)
Explanation
Enable Advanced Routing in Network > Virtual Routers > Router Settings > General, then commit and reboot
1. This means that the administrator can enable advanced routing features such as RIB filtering, BFD, multicast, and redistribution profiles for each virtual router on the firewall. The firewall requires a reboot after enabling advanced routing to apply the changes.

NEW QUESTION: 45
An engineer has discovered that certain real-time traffic is being treated as best effort due to it exceeding defined bandwidth Which QoS setting should the engineer adjust?
A. QoS profile: Egress Max
B. QoS interface: Egress Guaranteed
C. QoS profile: Egress Guaranteed

D. QoS interface: Egress Max
Answer: C (LEAVE A REPLY)
Explanation
When the egress guaranteed bandwidth is exceeded, the firewall passes traffic on a best-effort basis.
https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/quality-of-service/qos-concepts/qos-bandwidth-ma

NEW QUESTION: 46
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 management file command.
B. Enable all four stages of traffic capture (TX, RX, DROP, Firewall).
C. Use the tcpdump command.
D. Use the debug dataplane packet-diag set capture stage firewall file command.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 47
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. Locally-defined dynamic update settings take precedence over the settings that Panorama pushed
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. Panorama does not have valid licenses to push the dynamic updates
Answer: A (LEAVE A REPLY)

NEW QUESTION: 48

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: C (LEAVE A REPLY)
Explanation
A Custom Panorama Admin is a type of role-based access that allows a super user to create separate Panorama administrator accounts for each of the three contractors. This will allow each contractor to work with different device-groups in their hierarchy and deploy policies and objects in accordance with the organization's compliance requirements. The Custom Panorama Admin role also allows the super user to assign separate permissions to each contractor's account, granting them access to only the resources they are authorized to use.
This type of role-based access is the most appropriate for this project as it will ensure that each contractor is only able to access the resources they need in order to do their job.

NEW QUESTION: 49
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: 50
Which three use cases are valid reasons for requiring an Active/Active high availability deployment? (Choose three)
A. The environment requires real, full-time redundancy from both firewalls at all times
B. The environment requires Layer 2 interfaces in the deployment
C. The environment requires that both firewalls maintain their own routing tables for faster dynamic routing protocol convergence
D. The environment requires that all configuration must be fully synchronized between both members of the HA pair
E. The environment requires that traffic be load-balanced across both firewalls to handle peak traffic spikes
Answer: B,C,D (LEAVE A REPLY)

NEW QUESTION: 51
The firewall identifies a popular application as an unKnown-tcp.
Which two options are available to identify the application? (Choose two.)
A. Create a Security policy to identify the custom application.
B. Create a custom application.
C. Submit an App-ID request to Palo Alto Networks.
D. Create a custom object for the application server.
Answer: (SHOW ANSWER)

NEW QUESTION: 52
Which profile generates a packet threat type found in threat logs?
A. Antivirus
B. Anti-Spyware
C. WildFire
D. Zone Protection
Answer: D (LEAVE A REPLY)

NEW QUESTION: 53
Using multiple templates in a stack to manage many firewalls provides which two advantages? (Choose two.)
A. inherit address-objects from templates
B. define a common standard template configuration for firewalls
C. standardize server profiles and authentication configuration across all stacks
D. standardize log-forwarding profiles for security polices across all stacks
Answer: B,C (LEAVE A REPLY)

Explanation
Using multiple templates in a stack to manage many firewalls provides the advantages of defining a common standard template configuration for firewalls and standardizing server profiles and authentication configuration across all stacks. A template stack is a container for multiple templates that you can assign to firewalls and firewall groups. The templates in a stack are prioritized so that the settings in a higher-priority template override the same settings in a lower-priority template. This allows you to create a hierarchy of templates that define common settings for all firewalls and specific settings for different groups of firewalls. References: https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/manage-firewalls/manage-templates-and-temp

NEW QUESTION: 54
Given the screenshot, how did the firewall handle the traffic?
A. Traffic was allowed by policy but denied by profile as..
B. Traffic was allowed by policy but denied by profile as a..
C. Traffic was allowed by profile but denied by policy as a threat
D. Traffic was allowed by policy but denied by profile as ..
Answer: B (LEAVE A REPLY)

NEW QUESTION: 55
When using SSH keys for CLI authentication for firewall administration, which method is used for authorization?
A. Local
B. LDAP
C. Kerberos
D. Radius
Answer: A (LEAVE A REPLY)
Explanation
When using SSH keys for CLI authentication for firewall administration, the method used for authorization is local. This is described in the Palo Alto Networks PCNSE Study Guide in Chapter 4: Authentication and Authorization, under the section "CLI Authentication with SSH Keys": "SSH keys use public key cryptography to authenticate users, but they do not provide a mechanism for authorization. Therefore, when using SSH keys for CLI authentication, authorization is always performed locally on the firewall."

NEW QUESTION: 56
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. SSL/TLS Service Profile
B. SSH Service Profile
C. server certificate

D. certificate profile
Answer: (SHOW ANSWER)

NEW QUESTION: 57
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. captive portal
C. standalone User-ID agent
D. agentless User-ID with redistribution
Answer: C (LEAVE A REPLY)

NEW QUESTION: 58
Which GlobalProtect gateway selling is required to enable split-tunneling by access route, destination domain, and application?
A. No Direct Access to local networks
B. Tunnel mode
C. iPSec mode
D. Satellite mode
Answer: B (LEAVE A REPLY)
Explanation
To enable split-tunneling by access route, destination domain, and application, you need to configure a split tunnel based on the domain and application on your GlobalProtect gateway2. This allows you to specify which domains and applications are included or excluded from the VPN tunnel.

NEW QUESTION: 59
An administrator has configured a pair of firewalls using high availability in Active/Passive mode. Link and Path Monitoring Is enabled with the Failure Condition set to "any." There is one link group configured containing member interfaces ethernet1/1 and ethernet1/2 with a Group Failure Condition set to "all." Which HA state will the Active firewall go into if ethernet1/1 link goes down due to a failure?
A. Active
B. Active-Secondary
C. Passive
D. Non-functional
Answer: (SHOW ANSWER)

NEW QUESTION: 60
Which GlobalProtect component must be configured to enable Clientless VPN?
A. GlobalProtect satellite
B. GlobalProtect app
C. GlobalProtect portal
D. GlobalProtect gateway
Answer: C (LEAVE A REPLY)
Explanation
Creating the GlobalProtect portal is as simple as letting it know if you have accessed it already. A new gateway for accessing the GlobalProtect portal will appear. Client authentication can be used with an existing one.
https://www.nstec.com/how-to-configure-clientless-vpn-in-palo-alto/#5

NEW QUESTION: 61
Refer to the exhibit.
Using the above screenshot of the ACC, what is the best method to set a global filter, narrow down Blocked User Activity, and locate the user(s) that could be compromised by a botnet?
A. Click the left arrow beside the Zero Access.Gen threat.
B. Click the hyperlink for the Zero Access.Gen threat.
C. Click the hyperlink for the hotport threat Category.
D. Click the source user with the highest threat count.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 62
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. SSL/TLS Service profile
B. Decryption profile
C. SSH Service profile
D. Certificate profile
Answer: (SHOW ANSWER)

NEW QUESTION: 63
What would allow a network security administrator to authenticate and identify a user with a new BYOD-type device that is not joined to the corporate domain'?
A. a Security policy with 'known-user" selected in the Source User field
B. an Authentication policy with 'unknown' selected in the Source User field
C. a Security policy with 'unknown' selected in the Source User field
D. an Authentication policy with 'known-user' selected in the Source User field
Answer: B (LEAVE A REPLY)
Explanation
An Authentication policy with 'unknown' selected in the Source User field would allow a network security administrator to authenticate and identify a user with a new BYOD-type device that is not joined to the corporate domain. This policy would prompt the user to enter their credentials when they access a web-based application or service that requires authentication. The firewall would then use User-ID to map the user to the device and apply the appropriate security policies based on the user identity. References:
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/authentication/configure-an-authentication-policy

NEW QUESTION: 64
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. Promotion Hold Time
B. Monitor Fall Hold Up Time
C. Additional Master Hold Up Time
D. Heartbeat Interval
Answer: D (LEAVE A REPLY)

NEW QUESTION: 65
A firewall administrator has been tasked with ensuring that all Panorama-managed firewalls forward traffic logs to Panoram a. 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)

NEW QUESTION: 66
An administrator accidentally closed the commit window/screen before the commit was finished. Which two options could the administrator use to verify the progress or success of that commit task? (Choose two.)

A. System Logs
B. Task Manager
C. Traffic Logs
D. Configuration Logs
Answer: (SHOW ANSWER)
Explanation
A: System Logs: The system logs contain information about various events that occur on the firewall, including the commit process. The administrator can review the system logs to verify whether the commit completed successfully or whether there were any errors or warnings during the commit process.
B: Task Manager: The task manager displays a list of all active tasks on the firewall, including the commit task. The administrator can use the task manager to check the status of the commit task, including whether it is in progress, completed successfully, or failed.

NEW QUESTION: 67
The decision to upgrade to PAN-OS 10.2 has been approved. The engineer begins the process by upgrading the Panorama servers, but gets an error when trying to install.
When performing an upgrade on Panorama to PAN-OS 10.2, what is the potential cause of a failed install?
A. Outdated plugins
B. Expired certificates
C. Management only mode
D. GlobalProtect agent version
Answer: C (LEAVE A REPLY)

NEW QUESTION: 68
Match each GlobalProtect component to the purpose of that component
Answer:
Explanation
The GlobalProtect portal provides the management functions for your GlobalProtect infrastructure The GlobalProtect gateways provide security enforcement for traffic from GlobalProtect apps The GlobalProtect app software runs on endpoints and enables access to your network resources

NEW QUESTION: 69
An enterprise information Security team has deployed policies based on AD groups to restrict user access to critical infrastructure systems However a recent phisning campaign against the organization has prompted Information Security to look for more controls that can secure access to critical assets For users that need to access these systems Information Security wants to use PAN-OS multi-factor authentication (MFA) integration to enforce MFA.
What should the enterprise do to use PAN-OS MFA1?

A. Configure a Captive Porta1 authentication policy that uses an authentication profile that references a RADIUS profile
B. Create an authentication profile and assign another authentication factor to be used by a Captive Portal authentication policy
C. Configure a Captive Portal authentication policy that uses an authentication sequence
D. Use a Credential Phishing agent to detect prevent and mitigate credential phishing campaigns
Answer: (SHOW ANSWER)
Explanation
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/authentication/configure-multi-factor-authenticatio

NEW QUESTION: 70
An administrator needs to assign a specific DNS server to one firewall within a device group. Where would the administrator go to edit a template variable at the device level?
A. Variable CSV export under Panorama > templates
B. PDF Export under Panorama > templates
C. Manage variables under Panorama > templates
D. Managed Devices > Device Association
Answer: C (LEAVE A REPLY)
Explanation
To edit a template variable at the device level, you need to go to Manage variables under Panorama > templates. This allows you to override the default value of a variable for a specific device or device group. For example, you can assign a specific DNS server to one firewall within a device group by editing the
${dns-primary} variable for that device. References:
https://docs.paloaltonetworks.com/panorama/10-1/panorama-admin/manage-firewalls/manage-templates/use-tem

NEW QUESTION: 71
An administrator would like to determine which action the firewall will take for a specific CVE. Given the screenshot below, where should the administrator navigate to view this information?
A. The profile rule action
B. Exceptions lab
C. The profile rule threat name
D. CVE column
Answer: A (LEAVE A REPLY)

NEW QUESTION: 72
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 web server certificate signed by the organization's PKI
B. A self-signed Certificate Authority certificate generated by the firewall
C. A Machine Certificate for the firewall signed by the organization's PKI
D. A subordinate Certificate Authority certificate signed by the organization's PKI
Answer: B (LEAVE A REPLY)

NEW QUESTION: 73
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: 74
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. A master device with Group Mapping configured must be set in the device group where the Security rules are configured
B. The Security rules must be targeted to a firewall in the device group and have Group Mapping configured
C. A User-ID Certificate profile must be configured on Panorama
D. User-ID Redistribution must be configured on Panorama to ensure that all firewalls have the same mappings
Answer: A (LEAVE A REPLY)

NEW QUESTION: 75
An administrator is attempting to create policies tor deployment of a device group and template stack. When creating the policies, the zone drop down list does not include the required zone. What must the administrator do to correct this issue?
A. Specify the target device as the master device in the device group
B. Enable "Share Unused Address and Service Objects with Devices" in Panorama settings
C. Add the template as a reference template in the device group
D. Add a firewall to both the device group and the template
Answer: (SHOW ANSWER)

Explanation
Short Explanation: According to the Palo Alto Networks documentation, "To use a template stack for a device group, you must add the template stack as a reference template in the device group. This enables you to use zones and interfaces defined in the template stack when creating policies for the device group." References:
https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/manage-firewalls/manage-templates-and-temp

NEW QUESTION: 76
An administrator can not see any Traffic logs from the Palo Alto Networks NGFW in Panorama reports. The configuration problem seems to be on the firewall. Which settings, if configured incorrectly, most likely would stop only Traffic logs from being sent from the NGFW to Panorama?
A)
B)
C)
D)
A. Option C
B. Option A
C. Option D
D. Option B
Answer: A (LEAVE A REPLY)

NEW QUESTION: 77
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: 78
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 Panoram a. 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. Use the Firewall Migration plugin to retrieve the configuration directly from the managed devices
C. import Device Configuration to Panorama followed by Export or Push Device Config Bundle
D. Export Named Configuration Snapshot on each firewall followed by Import Named Configuration Snapshot in Panorama
Answer: C (LEAVE A REPLY)

NEW QUESTION: 79
Place the steps in the WildFire process workflow in their correct order.
Answer:
Explanation
Timeline Description automatically generated
https://docs.paloaltonetworks.com/wildfire/9-1/wildfire-admin/wildfire-overview/about-wildfire.html

NEW QUESTION: 80
A customer wants to set up a VLAN interface for a Layer 2 Ethernet port.
Which two mandatory options are used to configure a VLAN interface? (Choose two.)
A. ARP entries
B. Netflow Profile
C. Virtual router
D. Security zone
Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 81

An administrator has configured PAN-OS SD-WAN and has received a request to find out the reason for a session failover for a session that has already ended Where would you find this in Panorama or firewall logs?

A. Traffic Logs

B. System Logs

C. Session Browser

D. You cannot find failover details on closed sessions

Answer: A (LEAVE A REPLY)

Explanation

https://docs.paloaltonetworks.com/sd-wan/1-0/sd-wan-admin/configure-sd-wan/sd-wan-traffic-distribution-profil

NEW QUESTION: 82

An engineer is deploying multiple firewalls with common configuration in Panorama.

What are two benefits of using nested device groups? (Choose two.)

A. Inherit settings from the Shared group

B. Inherit IPSec crypto profiles

C. Inherit all Security policy rules and objects

D. Inherit parent Security policy rules and objects

Answer: B,D (LEAVE A REPLY)

Explanation

B: Inherit IPSec crypto profiles

This is correct because IPSec crypto profiles are one of the objects that can be inherited from a parent device group1. You can also create IPSec crypto profiles for use in shared or device group policy1.

D: Inherit parent Security policy rules and objects

This is correct because Security policy rules and objects are also inheritable from a parent device group1. You can also create Security policy rules and objects for use in shared or device group policy1.

NEW QUESTION: 83

An engineer wants to configure aggregate interfaces to increase bandwidth and redundancy between the firewall and switch. Which statement is correct about the configuration of the interfaces assigned to an aggregate interface group?

A. They can have a different bandwidth.

B. They can have a different interface type from an aggregate interface group.

C. They can have a different interface type such as Layer 3 or Layer 2.

D. They can have different hardware media such as the ability to mix fiber optic and copper.

Answer: (SHOW ANSWER)

NEW QUESTION: 84

Which statement is true regarding a Best Practice Assessment?
A. It runs only on firewalls
B. It shows how your current configuration compares to Palo Alto Networks recommendations
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: B (LEAVE A REPLY)

NEW QUESTION: 85
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: 86
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: 87
What happens, by default, when the GlobalProtect app fails to establish an IPSec tunnel to the GlobalProtect gateway?
A. It keeps trying to establish an IPSec tunnel to the GlobalProtect gateway.
B. It tries to establish a tunnel to the GlobalProtect portal using SSL/TLS.
C. It stops the tunnel-establishment processing to the GlobalProtect gateway immediately.
D. It tries to establish a tunnel to the GlobalProtect gateway using SSL/TLS.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 88
An administrator wants to enable WildFire inline machine learning. Which three file types does WildFire inline ML analyze? (Choose three.)
A. ELF
B. Powershell scripts
C. MS Office
D. VBscripts
E. APK
Answer: B,D,E (LEAVE A REPLY)

NEW QUESTION: 89
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: 90

What is a correct statement regarding administrative authentication using external services with a local authorization method?
A. The administrative accounts you define locally on the firewall serve as references to the accounts defined on an external authentication server.
B. The administrative accounts you define on an external authentication server serve as references to the accounts defined locally on the firewall.
C. 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.
D. Starting with PAN-OS 10.2. an administrator needs to configure Cloud Identity Engine to use external authentication services for administrative authentication.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 91
Which steps should an engineer take to forward system logs to email?
A. Enable log forwarding under the email profile in the Objects tab.
B. Enable log forwarding under the email profile in the Device 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. 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.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 92
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 Zone Protection profile, enable reconnaissance protection, set action to Block, and apply it to the outside zone.
D. Create a Security rule to deny all ICMP traffic from the outside zone.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 93
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: A,C (LEAVE A REPLY)
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: 94
Which two statements correctly describe Session 380280? (Choose two.)
A. The application has been identified as web-browsing.
B. The session did not go through SSL decryption processing.
C. The session has ended with the end-reason unknown.
D. The session went through SSL decryption processing.
Answer: (SHOW ANSWER)

NEW QUESTION: 95
A security engineer received multiple reports of an IPSec VPN tunnel going down the night before. The engineer couldn't find any events related to VPN under system togs.
What is the likely cause?
A. Dead Peer Detection is not enabled.
B. Tunnel Inspection settings are misconfigured.
C. The Tunnel Monitor is not configured.
D. The log quota for GTP and Tunnel needs to be adjusted
Answer: C (LEAVE A REPLY)
Explanation
This means that the firewall does not have a mechanism to monitor the status of the IPSec VPN tunnel and generate logs when it goes down or up. The Tunnel Monitor is an optional feature that

can be enabled on each IPSec tunnel interface and it uses ICMP probes to check the connectivity of the tunnel peer. If the firewall does not receive a response from the peer after a specified number of retries, it marks the tunnel as down and logs an event1.

NEW QUESTION: 96
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: A (LEAVE A REPLY)
Explanation
To configure LDAP authentication on Panorama, you need to23:
* 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: 97
When you navigate to Network: > GlobalProtect > Portals > Method section, which three options are available? (Choose three)
A. user-logon (always on)
B. pre-logon then on-demand
C. on-demand (manual user initiated connection)
D. post-logon (always on)
E. certificate-logon
Answer: A,B,C (LEAVE A REPLY)
Explanation
The Method section of the GlobalProtect portal configuration allows you to specify how users connect to the portal. The options are:
* user-logon (always on): The agent connects to the portal as soon as the user logs in to the endpoint.
* pre-logon then on-demand: The agent connects to the portal before the user logs in to the endpoint and then switches to on-demand mode after the user logs in.

* on-demand (manual user initiated connection): The agent connects to the portal only when the user initiates the connection manually. References: https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/globalprotect/configure-the-globalprotect-po

NEW QUESTION: 98
After importing a pre-configured firewall configuration to Panorama, what step is required to ensure a commit/push is successful without duplicating local configurations?
A. Ensure Force Template Values is checked when pushing configuration.
B. Push the Template first, then push Device Group to the newly managed firewal.
C. Perform the Export or push Device Config Bundle to the newly managed firewall.
D. Push the Device Group first, then push Template to the newly managed firewall
Answer: (SHOW ANSWER)
Explanation
When importing a pre-configured firewall configuration to Panorama, you need to perform the following steps
12:
* Add the serial number of the firewall under Panorama > Managed Devices
* In Panorama, import the firewall's configuration bundle under Panorama > Setup > Operations > Import device configuration to Panorama
* Make changes to the imported firewall configuration within Panorama
* Commit the changes you made to Panorama
* Perform an Export or push Device Config Bundle operation under Panorama > Setup > Operations The Export or push Device Config Bundle operation allows you to push a complete configuration bundle from Panorama to a managed firewall without duplicating local configurations . This operation ensures that any local settings on the firewall are preserved and merged with the settings from Panorama.

NEW QUESTION: 99
Which configuration is backed up using the Scheduled Config Export feature in Panorama?
A. Panorama running configuration
B. Panorama candidate configuration
C. Panorama running configuration and running configuration of all managed devices
D. Panorama candidate configuration and candidate configuration of all managed devices
Answer: (SHOW ANSWER)

NEW QUESTION: 100
What can you use with Global Protect to assign user-specific client certificates to each GlobalProtect user?
A. SCEP
B. OCSP Responder

C. SSL/TLS Service profile
D. Certificate profile
Answer: A (LEAVE A REPLY)

NEW QUESTION: 101
An engineer has been given approval to upgrade their environment 10 PAN-OS 10 2 The environment consists of both physical and virtual firewalls a virtual Panorama HA pair, and virtual log collectors What is the recommended order when upgrading to PAN-OS 10.2?
A. Upgrade the log collectors, upgrade the firewalls, upgrade Panorama
B. Upgrade the firewalls upgrade log collectors, upgrade Panorama
C. Upgrade the firewalls upgrade Panorama, upgrade the log collectors
D. Upgrade Panorama, upgrade the log collectors, upgrade the firewalls
Answer: B (LEAVE A REPLY)

NEW QUESTION: 102
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: 103
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 High Availability > Link and Path Monitoring settings.
C. Check the HA Link Monitoring interface cables.

D. Check High Availability > Active/Passive Settings > Passive Link State
E. Check the High Availability > HA Communications > Packet Forwarding settings.
Answer: A,B,C (LEAVE A REPLY)