

Paloalto-Networks

Exam Questions PCNSE

Palo Alto Networks Certified Security Engineer (PCNSE) PAN-OS 9.0



NEW QUESTION 1

With the default TCP and UDP settings on the firewall, what will be the identified application in the following session?

The screenshot shows a 'Detailed Log View' window with three main sections: General, Source, and Destination. The General section shows the rule 'vWire-1298554-Deny-All' and the session end reason 'policy-deny'. The Source section shows the zone 'vWire-1298554' and interface 'ethernet1/1'. The Destination section shows the zone 'vWire-1298554' and interface 'ethernet1/1'. The Details section shows the type 'drop' and bytes '60'. The Flags section shows various options like 'Captive Portal', 'Proxy Transaction', 'Decrypted', etc., all of which are unchecked.

General	Source	Destination
Rule: vWire-1298554-Deny-All Rule UUID: Session End Reason: policy-deny Category: any Device SN: IP Protocol: tcp Log Action: Generated Time: 2019/12/17 20:41:39 Start Time: 2019/12/17 20:41:37 Receive Time: 2019/12/17 20:41:39 Elapsed Time(sec): 0 Tunnel Type: N/A	Zone: vWire-1298554 Interface: ethernet1/1 X-Forwarded-For IP: 0.0.0.0 Details: Type: drop Bytes: 60 Bytes Received: 0 Bytes Sent: 60 Repeat Count: 1 Packets: 1 Packets Received: 0 Packets Sent: 1	Zone: vWire-1298554 Interface: Flags: Captive Portal <input type="checkbox"/> Proxy Transaction <input type="checkbox"/> Decrypted <input type="checkbox"/> Packet Capture <input type="checkbox"/> Client to Server <input type="checkbox"/> Server to Client <input type="checkbox"/> Symmetric Return <input type="checkbox"/> Mirrored <input type="checkbox"/> Tunnel Inspected <input type="checkbox"/> MPTCP Options <input type="checkbox"/> Recon excluded <input type="checkbox"/> Decrypt Forwarded <input type="checkbox"/>

- A. Incomplete
- B. unknown-tcp
- C. Insufficient-data
- D. not-applicable

Answer: D

Explanation:

Traffic didn't match any other policies and so landed at the implicit "deny all" policy. If it's deny all, the traffic was dropped before the application could be determined. <https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClibCAC>

NEW QUESTION 2

Which GlobalProtect gateway setting 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

Explanation:

<https://docs.paloaltonetworks.com/globalprotect/9-1/globalprotect-admin/globalprotect-gateways/split-tunnel-tra>

NEW QUESTION 3

After implementing a new NGFW, a firewall engineer sees a VoIP traffic issue going through the firewall. After troubleshooting, the engineer finds that the firewall performs NAT on the voice packets payload and opens dynamic pinholes for media ports. What can the engineer do to solve the VoIP traffic issue?

- A. Disable ALG under H.323 application
- B. Increase the TCP timeout under H.323 application
- C. Increase the TCP timeout under SIP application
- D. Disable ALG under SIP application

Answer: D

Explanation:

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/app-id/disable-the-sip-application-level-gateway-a>

NEW QUESTION 4

A network administrator is trying to prevent domain username and password submissions to phishing sites on some allowed URL categories. Which set of steps does the administrator need to take in the URL Filtering profile to prevent credential phishing on the firewall?

- A. Choose the URL categories in the User Credential Submission column and set action to block. Select the User credential Detection tab and select Use Domain Credential Filter Commit.
- B. Choose the URL categories in the User Credential Submission column and set action to block. Select the User credential Detection tab and select use IP User Mapping Commit.
- C. Choose the URL categories on Site Access column and set action to block. Click the User credential Detection tab and select IP User Mapping Commit.
- D. Choose the URL categories in the User Credential Submission column and set action to block. Select the URL filtering settings and enable Domain Credential Filter Commit.

Answer: A

Explanation:

[https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/threat-prevention/prevent-credential-phishing/set-up https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/url-filtering/prevent-credential-phishing/set-up-cre](https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/threat-prevention/prevent-credential-phishing/set-up-https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/url-filtering/prevent-credential-phishing/set-up-cre)

NEW QUESTION 5

Which statement about High Availability timer settings is true?

- A. Use the Critical timer for faster failover timer settings.
- B. Use the Aggressive timer for faster failover timer settings
- C. Use the Moderate timer for typical failover timer settings
- D. Use the Recommended timer for faster failover timer settings.

Answer: D

Explanation:

Recommended: Use for typical failover timer settings. Unless you're sure that you need different settings, the best practice is to use the Recommended settings.

Aggressive: Use for faster failover timer settings.

Advanced: Allows you to customize the values to suit your network requirement for each of the following timers:

NEW QUESTION 6

An engineer needs to configure a standardized template for all Panorama-managed firewalls. These settings will be configured on a template named "Global" and will be included in all template stacks.

Which three settings can be configured in this template? (Choose three.)

- A. Log Forwarding profile
- B. SSL decryption exclusion
- C. Email scheduler
- D. Login banner
- E. Dynamic updates

Answer: BDE

Explanation:

A template is a set of configuration options that can be applied to one or more firewalls or virtual systems managed by Panorama. A template can include settings from the Device and Network tabs on the firewall web interface, such as login banner, SSL decryption exclusion, and dynamic updates⁴. These settings can be configured in a template named "Global" and included in all template stacks. A template stack is a group of templates that Panorama pushes to managed firewalls in an ordered hierarchy⁴. References: Manage Templates and Template Stacks, PCNSE Study Guide (page 50)

NEW QUESTION 7

In a security-first network, what is the recommended threshold value for apps and threats to be dynamically updated?

- A. 1 to 4 hours
- B. 6 to 12 hours
- C. 24 hours
- D. 36 hours

Answer: B

Explanation:

Schedule content updates so that they download-and-install automatically. Then, set a Threshold that determines the amount of time the firewall waits before installing the latest content. In a security-first network, schedule a six to twelve hour threshold.

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/threat-prevention/best-practices-for-content-and-thr>

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-upgrade/software-and-content-updates/best-practices-for>

NEW QUESTION 8

An administrator Just enabled HA Heartbeat Backup on two devices However, the status on tie firewall's dashboard is showing as down High Availability.

High Availability		
Mode		Active-passive
Local	<div></div>	Active
Peer (10.0.0.9)	<div></div>	Passive
Running Config	<div></div>	Synchronized 
App Version	<div></div>	Match
Threat Version	<div></div>	Match
Antivirus Version	<div></div>	Match
PAN-OS Version	<div></div>	Match
Global Protect Version	<div></div>	Match
HA1	<div></div>	Up
HA1 Backup	<div></div>	Up
Heartbeat Backup	<div></div>	Down
HA2	<div></div>	Up
HA2 Backup	<div></div>	Up

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

Explanation:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIF4CAK>

NEW QUESTION 9

Which template values will be configured on the firewall if each template has an SSL to be deployed. The template stack should consist of four templates arranged according to the diagram.



Which template values will be configured on the firewall if each template has an SSL/TLS Service profile configured named Management?

- A. Values in Datacenter
- B. Values in efwOlab.chi
- C. Values in Global Settings
- D. Values in Chicago

Answer: D

Explanation:

The template stack should consist of four templates arranged according to the diagram. The template values that will be configured on the firewall if each template has an SSL/TLS Service profile configured named Management will be the values in Chicago. This is because the SSL/TLS Service profile is configured in the Chicago template, which is the highest priority template in the stack. The firewall will inherit the settings from the highest priority template that has the setting configured, and ignore the settings from the lower priority templates that have the same setting configured. Therefore, the values in Datacenter, efwOlab.chi, and Global Settings will not be applied to the firewall. References:

- > [Template Stack Configuration]
- > [Template Stack Priority]

NEW QUESTION 10

An engineer troubleshoots a Panorama-managed firewall that is unable to reach the DNS servers configured via a global template. As a troubleshooting step, the engineer needs to configure a local DNS server in place of the template value.

Which two actions can be taken to ensure that only the specific firewall is affected during this process? (Choose two)

- A. Configure the DNS server locally on the firewall.
- B. Change the DNS server on the global template.
- C. Override the DNS server on the template stack.
- D. Configure a service route for DNS on a different interface.

Answer: AC

Explanation:

To override a device and network setting applied by a template, you can either configure the setting locally on the firewall or override the setting on the template stack. Configuring the setting locally on the firewall will copy the setting to the local configuration of the device and will no longer be controlled by the template. Overriding the setting on the template stack will apply the setting to all the firewalls that are assigned to the template stack, unless the setting is also overridden locally on a firewall. Changing the setting on the global template will affect all the firewalls that inherit the setting from the template, which is not desirable in this scenario. Configuring a service route for DNS on a different interface will not change the DNS server address, but only the interface that the firewall uses to reach the DNS server. References:

- > [Override a Template Setting](#)
- > [Overriding Panorama Template settings](#)

NEW QUESTION 10

Which GloDalProtect gateway setting is required to enable split-tunneling by access route, destination domain and application?

- A. Tunnel mode
- B. Satellite mode
- C. IPSec mode
- D. No Direct Access to local networks

Answer: A

Explanation:

<https://docs.paloaltonetworks.com/globalprotect/9-1/globalprotect-admin/globalprotect-gateways/split-tunnel-tra>

NEW QUESTION 14

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: C

Explanation:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIGJCA0>

NEW QUESTION 19

What is the best definition of the Heartbeat Interval?

- A. The interval in milliseconds between hello packets
- B. The frequency at which the HA peers check link or path availability
- C. The frequency at which the HA peers exchange ping
- D. The interval during which the firewall will remain active following a link monitor failure

Answer: C

Explanation:

The firewalls exchange hello messages and heartbeats at configurable intervals to verify that the peer firewall is responsive and operational. Hello messages are sent from one peer to the other to verify the state of the firewall. The heartbeat is an ICMP ping to the HA peer. A response from the peer indicates that the firewalls are connected and responsive.

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIUcCAK>

"A "heartbeat-interval" CLI command was added to the election settings for HA, this interval has a 1000ms minimum for all Palo Alto Networks platforms and is an ICMP ping to the other device through the HA control link." <https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIMaCAK>

NEW QUESTION 23

Which two profiles should be configured when sharing tags from threat logs with a remote User-ID agent? (Choose two.)

- A. Log Ingestion
- B. HTTP
- C. Log Forwarding
- D. LDAP

Answer: BC

Explanation:

>Threat logs, create a log forwarding profile to define how you want the firewall or Panorama to handle logs.

>Configure an HTTP server profile to forward logs to a remote User-ID agent. > Select the log forwarding profile you created then select this server profile as the

HTTP server profile <https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/policy/use-auto-tagging-to-automate-security-actio>

NEW QUESTION 25

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: ABC

Explanation:

User-ID is a feature that allows the firewall to identify and classify users and groups on the network based on their usernames, IP addresses, and other attributes1. User-ID information can be collected from various sources, such as:

- > A: Windows User-ID agent: A software agent that runs on a Windows server and collects user information from Active Directory domain controllers, Exchange servers, or eDirectory servers2. The agent then sends the user information to the firewall or Panorama for user mapping2.
- > B: GlobalProtect: A software agent that runs on the endpoints and provides secure VPN access to the network3. GlobalProtect also collects user information from the endpoints and sends it to the firewall or Panorama for user mapping4.
- > C: XMLAPI: An application programming interface that allows external systems or scripts to send user information to the firewall or Panorama in XML format. The XMLAPI can be used to integrate with third-party systems, such as identity providers, captive portals, or custom applications.

NEW QUESTION 29

A company has configured a URL Filtering profile with override action on their firewall. Which two profiles are needed to complete the configuration? (Choose two)

- A. SSL/TLS Service
- B. HTTP Server
- C. Decryption
- D. Interface Management

Answer: AD

Explanation:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIRdCAK> <https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/url-filtering/configure-url-filtering>
<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/url-filtering/allow-password-access-to-certain-site>

NEW QUESTION 33

Refer to the exhibit.

```
#####
admin@Lab33-111-PA-3060(active)>show routing fib

id      destination      nexthop      flags      interface      mtu
-----
47      0.0.0.0/0        10.46.40.1   ug         ethernet1/3    1500
46      10.46.40.0/23    0.0.0.0      u          ethernet1/3    1500
45      10.46.41.111/32  0.0.0.0      uh         ethernet1/3    1500
70      10.46.41.113/32  10.46.40.1   ug         ethernet1/3    1500
51      192.168.111.0/24 0.0.0.0      u          ethernet1/6    1500
50      192.168.111.2/32 0.0.0.0      uh         ethernet1/6    1500

#####

admin@Lab33-111-PA-3060(active)>show virtual-wire all

total virtual-wire shown:
flags: m-multicast firewalling
      p= link state pass-through
      s- vlan sub-interface
      i- ip+vlan sub-interface
      t-tenant sub-interface

name      interface1      interface2      flags      allowed-tags
-----
VW-1      ethernet1/7     ethernet1/5     p
```

Which will be the egress interface if the traffic's ingress interface is ethernet1/7 sourcing from 192.168.111.3 and to the destination 10.46.41.113?

- A. ethernet1/6
- B. ethernet1/3
- C. ethernet1/7
- D. ethernet1/5

Answer: D

Explanation:

In the second image, VW ports mentioned are 1/5 and 1/7. Hence it can not be a part of any other routing. So if any traffic coming as ingress from 1/7, it has to go out via 1/5.

The egress interface for the traffic with ingress interface ethernet1/7, source 192.168.111.3, and destination 10.46.41.113 will be ethernet1/5. This is because the traffic will match the virtual wire with interfaces ethernet1/5 and ethernet1/7, which is configured to allow VLAN-tagged traffic with tags 10 and 201. The traffic will also match the security policy rule that allows traffic from zone Trust to zone Untrust, which are assigned to ethernet1/7 and ethernet1/5 respectively². Therefore, the traffic will be forwarded to the same interface from which it was received, which is ethernet1/5.

NEW QUESTION 34

An organization conducts research on the benefits of leveraging the Web Proxy feature of PAN-OS 11.0. What are two benefits of using an explicit proxy method versus a transparent proxy method? (Choose two.)

- A. No client configuration is required for explicit proxy, which simplifies the deployment complexity.
- B. Explicit proxy supports interception of traffic using non-standard HTTPS ports.
- C. It supports the X-Authenticated-User (XAU) header, which contains the authenticated username in the outgoing request.
- D. Explicit proxy allows for easier troubleshooting, since the client browser is aware of the existence of the proxy.

Answer: CD

Explanation:

<https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-cloud-managed-admin/secure-mobile-us> <https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-new-features/networking-features/web-proxy>

NEW QUESTION 36

Which three options does Panorama offer for deploying dynamic updates to its managed devices? (Choose three.)

- A. Check dependencies
- B. Schedules
- C. Verify
- D. Revert content
- E. Install

Answer: BDE

Explanation:

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

NEW QUESTION 39

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: AD

Explanation:

<https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/panorama-overview/centralized-firewall-conf>

NEW QUESTION 42

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: B

Explanation:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/user-id/map-ip-addresses-to-users/configure-user-i>

NEW QUESTION 47

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

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

Answer: A

Explanation:

To use PAN-OS multi-factor authentication (MFA) to secure access to critical assets, the enterprise should configure a Captive Portal authentication policy that uses an authentication sequence. An authentication sequence is a feature that allows the firewall to enforce multiple authentication methods (factors) for users who access sensitive services or applications. An authentication sequence can include up to four factors, such as login and password, Voice, SMS, Push, or One-time Password (OTP) authentication. The firewall can integrate with MFA vendors through RADIUS or vendor APIs to provide the additional factors¹². To configure an authentication sequence, the enterprise needs to create an authentication profile for each factor and then add them to the sequence in the desired order. The enterprise also needs to create a Captive Portal authentication policy that matches the traffic that requires MFA and applies the authentication sequence to it. The Captive Portal is a web page that the firewall displays to users who need to authenticate before accessing the network or the internet. The Captive Portal can be customized to include a welcome message, a login prompt, a disclaimer, a certificate download link, and a logout button³⁴. When a user tries to access a service or application that matches the Captive Portal authentication policy, the firewall redirects the user to the Captive Portal web form for the first factor. After the user successfully authenticates for the first factor, the firewall prompts the user for the second factor through RADIUS or vendor API integration. The firewall repeats this process until all factors in the sequence are completed or until one factor fails. If all factors are completed successfully, the firewall allows the user to access the service or application. If one factor fails, the firewall denies access and logs an event⁵⁶. Configuring a Captive Portal authentication policy that uses an authentication profile that references a RADIUS profile is not sufficient to use PAN-OS MFA. This option only provides one factor of authentication through RADIUS integration with an MFA vendor. To use multiple factors of authentication, an authentication sequence is required. Creating an authentication profile and assigning another authentication factor to be used by a Captive Portal authentication policy is not correct to use PAN-OS MFA. This option does not specify how to create or apply an authentication sequence, which is necessary for enforcing multiple factors of authentication. Using a Credential Phishing agent to detect, prevent, and mitigate credential phishing campaigns is not relevant to use PAN-OS MFA. This option is a feature of Palo Alto Networks Cortex XDR™ that helps protect endpoints from credential theft by malicious actors. It does not provide any MFA functionality for accessing critical assets. References: Authentication Sequence, Configure Multi-Factor Authentication, Configure an Authentication Portal, Create an Authentication Profile, Create an Authentication Sequence, Create a Captive Portal Authentication Policy, [Credential Phishing Agent]

NEW QUESTION 51

An administrator is receiving complaints about application performance degradation. After checking the ACC, the administrator observes that there is an excessive amount of VoIP traffic. Which three elements should the administrator configure to address this issue? (Choose three.)

- A. An Application Override policy for the SIP traffic
- B. QoS on the egress interface for the traffic flows
- C. QoS on the ingress interface for the traffic flows
- D. A QoS profile defining traffic classes
- E. A QoS policy for each application ID

Answer: BDE

Explanation:

To address the issue of application performance degradation due to excessive VoIP traffic, the administrator should configure QoS on the egress interface for the traffic flows and a QoS profile defining traffic classes. QoS stands for Quality of Service, which is a feature that allows the firewall to manage bandwidth usage and prioritize traffic based on various criteria, such as application, user, service, etc. QoS can help improve the performance and quality of latency-sensitive applications, such as VoIP, by guaranteeing them sufficient bandwidth and priority over other traffic¹. To enable QoS on the firewall, the administrator needs to create a QoS profile and a QoS policy. A QoS profile defines the eight classes of service that traffic can receive, including priority, guaranteed bandwidth, maximum bandwidth, and weight. A QoS policy identifies the traffic that matches a specific class of service based on source and destination zones, addresses, users, applications, services, etc². The administrator can also create a custom QoS profile or use the default one. The administrator should apply QoS on the egress interface for the traffic flows, which is the interface where the traffic leaves the firewall. This is because QoS can only shape outbound traffic and not inbound traffic. The egress interface can be either internal or external, depending on the direction of the VoIP traffic. For example, if the VoIP traffic is from internal users to external servers, then the egress interface is the untrust interface facing the ISP. If the VoIP traffic is from external users to internal servers, then the egress interface is the trust interface facing the LAN³. The administrator should assign a high priority and a sufficient guaranteed bandwidth to the VoIP traffic in the QoS profile. This will ensure that the VoIP packets are processed first by the firewall and are not dropped or delayed due to congestion. The administrator can also limit or block other applications that consume too much bandwidth or pose security risks in the same or different QoS classes⁴. An Application Override policy for SIP traffic is not necessary to address this issue. An Application Override policy is used to change or customize the App-ID of certain traffic based on port and protocol criteria. This can be useful for optimizing performance or security for some applications that are difficult to identify or have non-standard behaviors. However, SIP is a predefined App-ID that identifies Session Initiation Protocol (SIP) traffic, which is commonly used for VoIP signaling. The firewall can recognize SIP traffic without an Application Override policy⁵. QoS on the ingress interface for the traffic flows is not effective to address this issue. As mentioned earlier, QoS can only shape outbound traffic and not inbound traffic. Applying QoS on the ingress interface will not have any impact on how the firewall handles or prioritizes the incoming packets⁶. A QoS policy for each application is not required to address this issue. A QoS policy can match multiple applications in a single rule by using application filters or application groups. This can simplify and consolidate the QoS policy configuration and management. The administrator does not need to create a separate QoS policy for each application unless there is a specific need to assign different classes of service or parameters to each application⁷. References: QoS Overview, Configure QoS, QoS Use Cases, QoS Best Practices, Application Override FAQ, Create a QoS Policy Rule

NEW QUESTION 52

An administrator notices that an interface configuration has been overridden locally on a firewall. They require all configuration to be managed from Panorama and overrides are not allowed. What is one way the administrator can meet this requirement?

- A. Perform a commit force from the CLI of the firewall.
- B. Perform a template commit push from Panorama using the "Force Template Values" option.
- C. Perform a device-group commit push from Panorama using the "Include Device and Network Templates" option.
- D. Reload the running configuration and perform a Firewall local commit.

Answer: B

Explanation:

The best way for the administrator to meet the requirement of managing all configuration from Panorama and preventing local overrides is B: Perform a template commit push from Panorama using the "Force Template Values" option. This option allows the administrator to overwrite any local configuration on the firewall with the values defined in the template¹. This way, the administrator can ensure that the interface configuration and any other

NEW QUESTION 53

If an administrator wants to apply QoS to traffic based on source, what must be specified in a QoS policy rule?

- A. Post-NAT destination address
- B. Pre-NAT destination address
- C. Post-NAT source address
- D. Pre-NAT source address

Answer: C

Explanation:

If an administrator wants to apply QoS to traffic based on source, they must specify the post-NAT source address in a QoS policy rule. This is because QoS is enforced on traffic as it egresses the firewall, and the firewall applies NAT rules before QoS rules. Therefore, the firewall will match the QoS policy rule based on the translated source address, not the original source address. If the administrator uses the pre-NAT source address in the QoS policy rule, the firewall will not be able to identify the traffic correctly and apply the desired QoS treatment. References:

- > QoS Policy
- > Configure QoS

NEW QUESTION 58

An engineer is monitoring an active/active high availability (HA) firewall pair.
 Which HA firewall state describes the firewall that is experiencing a failure of a monitored path?

- A. Initial
- B. Tentative
- C. Passive
- D. Active-secondary

Answer: B

Explanation:

In an active/active high availability (HA) firewall pair, when a firewall experiences a failure of a monitored path, it enters the "Tentative" state¹. This state indicates that the firewall is synchronizing sessions and configurations from its peer due to a failure or a change in monitored objects such as a link or path. The firewall in this state is not fully functional but is working towards resuming normal operations by syncing with its peer. Therefore, the correct answer is B. Tentative.

Firewall Stuck in Initial (Leaving Suspended State) - Palo Alto Networks



NEW QUESTION 63

Which three items must be configured to implement application override? (Choose three)

- A. Custom app
- B. Security policy rule
- C. Application override policy rule
- D. Decryption policy rule
- E. Application filter

Answer: ABC

Explanation:

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/policies/policies-application-override>
<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PPDrCAO>

NEW QUESTION 65

What must be configured to apply tags automatically based on User-ID logs?

- A. Device ID
- B. Log Forwarding profile
- C. Group mapping
- D. Log settings

Answer: B

Explanation:

To apply tags automatically based on User-ID logs, the engineer must configure a Log Forwarding profile that specifies the criteria for matching the logs and the tags to apply. The Log Forwarding profile can be attached to a security policy rule or a decryption policy rule to enable auto-tagging for the traffic that matches the rule. The tags can then be used for dynamic address groups, policy enforcement, or reporting¹. References: Use Auto-Tagging to Automate Security Actions, PCNSE Study Guide (page 49)

NEW QUESTION 67

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: B

Explanation:

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/user-id/user-id-concepts/user-mapping/globalprote> GlobalProtect is a VPN solution that provides secure remote access to corporate networks. When a user connects to GlobalProtect, their identity is verified against an LDAP server. This ensures that all IP address-to-user mappings are explicitly known.

NEW QUESTION 71

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: ABE

Explanation:

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/firewall-administration/manage-firewall-administra>

NEW QUESTION 74

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 applications seen from traffic matching the same rule
- C. Applications configured in the rule with their dependencies
- D. The security rule with any other security rule selected

Answer: B

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 helps the administrator to identify any new applications that are not explicitly defined in the rule, but are implicitly allowed by the firewall based on the dependencies of the configured applications. The compare option also shows the usage statistics and risk levels of the applications, and provides suggestions for optimizing the rule by adding, removing, or replacing applications¹². References: New App Viewer (Policy Optimizer), PCNSE Study Guide (page 47)

Why use Security Policy Optimizer and what are the benefits?



NEW QUESTION 77

Which three authentication types can be used to authenticate users? (Choose three.)

- A. Local database authentication
- B. PingID
- C. Kerberos single sign-on
- D. GlobalProtect client
- E. Cloud authentication service

Answer: ACE

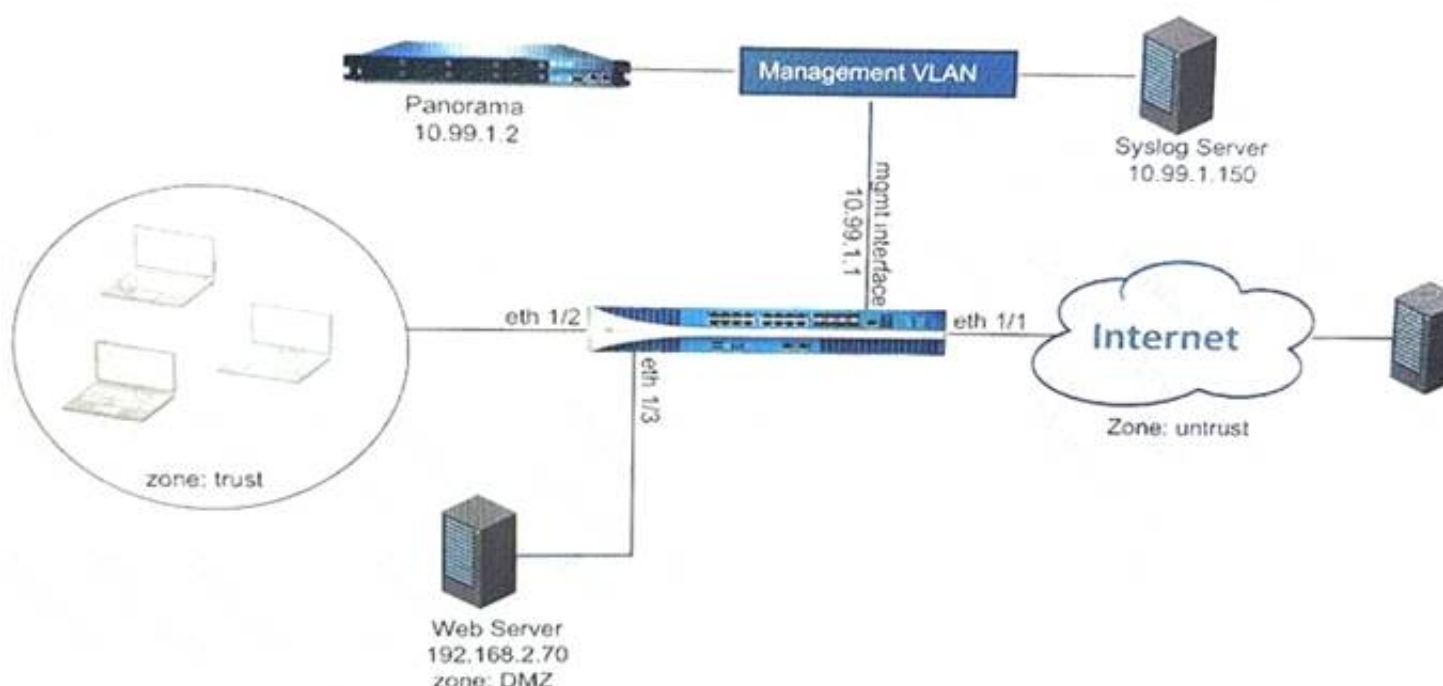
Explanation:

The three authentication types that can be used to authenticate users are:

- > A: Local database authentication. This is the authentication type that uses the local user database on the firewall or Panorama to store and verify user credentials¹.
- > C: Cloud authentication service. This is the authentication type that uses a cloud-based identity provider such as Okta, PingOne, or PingFederate, to authenticate users and provide SAML assertions to the firewall or Panorama².
- > E: Kerberos single sign-on. This is the authentication type that uses the Kerberos protocol to authenticate users who are logged in to a Windows domain and provide them with seamless access to resources on the firewall or Panorama³.

NEW QUESTION 82

Refer to Exhibit:



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)

Panorama Settings

Panorama Servers

10.99.1.21

Receive Timeout for Connection to Panorama (sec) 240

Send Timeout for Connection to Panorama (sec) 240

Retry Count for SSL Send to Panorama 25

Secure Client Communication

Certificate Type: None

☐ Check Server Identity

B)

Security Policy Rule

General | Source | User | Destination | Application | Service/URL Category | Actions

Action Setting

Action: Allow

Log Setting

☒ Log at Session Start

☒ Log at Session End

Log Forwarding None

Profile Setting

Profile Type: Profiles

Antivirus: None

Vulnerability Protection: None

Anti-Spyware: None

URL Filtering: Filter1

File Blocking: None

Data Filtering: None

WildFire Analysis: None

Other Settings

Schedule: None

QoS Marking: None

☐ Disable Server Response Inspection

C)

Syslog Server Profile

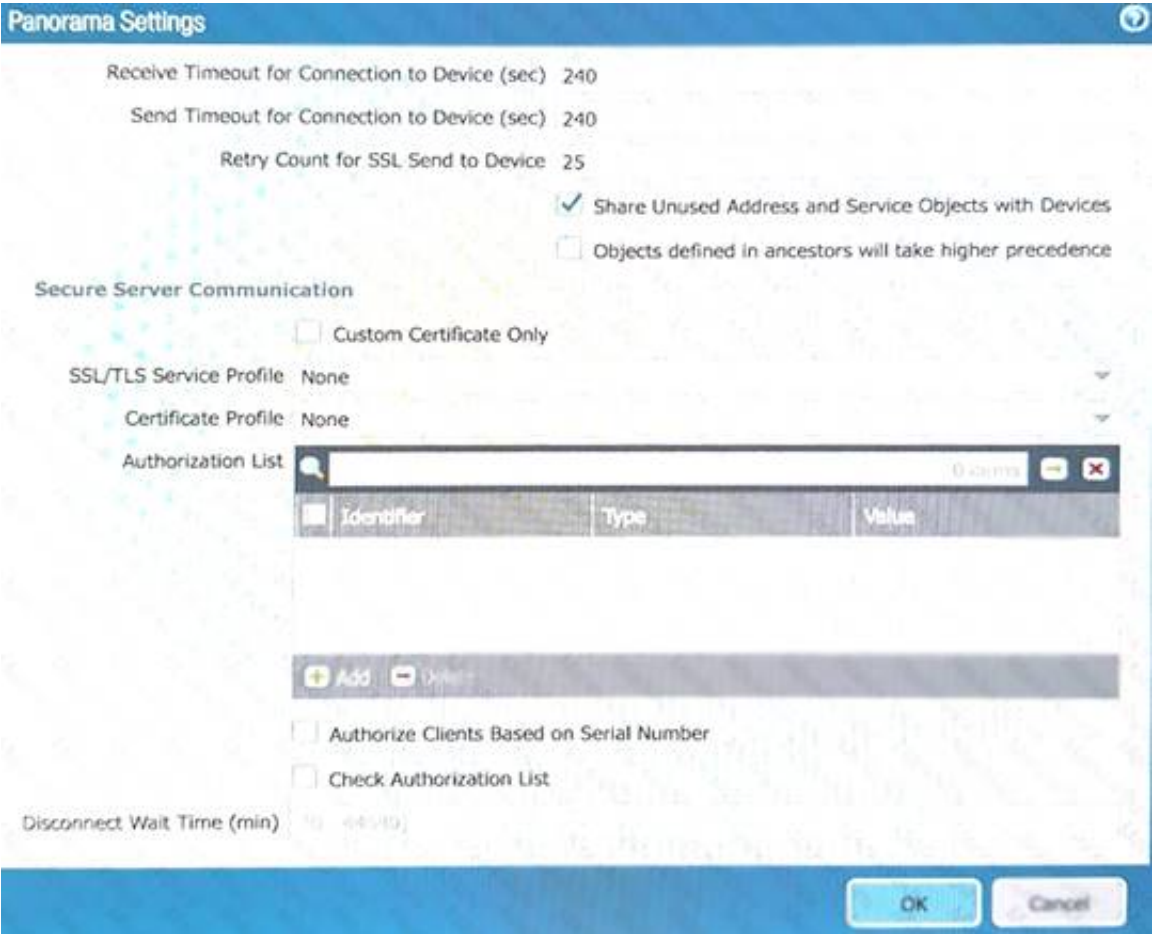
Name: SyslogProfile1

Servers Custom Log Format

Name	Syslog Server	Transport	Port	Format	Facility
SyslogServer1	192.168.229.17	UDP	514	BSD	LOG_USER

Enter the IP address or FQDN of the Syslog server.

D)



- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: C

NEW QUESTION 85

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. CVE column
- C. Exceptions tab
- D. The profile rule threat name

Answer: C

Explanation:

The Exceptions settings allows you to change the response to a specific signature. For example, you can block all packets that match a signature, except for the selected one, which generates an alert. The Exception tab supports filtering functions. If you not believed, then login the firewall go to Vulnerability > Exceptions and select "Show all signatures". From there you will see all threat information including specific actions. More detail: <https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Cm4yCAC>

NEW QUESTION 88

An engineer must configure a new SSL decryption deployment.

Which profile or certificate is required before any traffic that matches an SSL decryption rule is decrypted?

- A. A Decryption profile must be attached to the Decryption policy that the traffic matches.
- B. A Decryption profile must be attached to the Security policy that the traffic matches.
- C. There must be a certificate with only the Forward Trust option selected.
- D. There must be a certificate with both the Forward Trust option and Forward Untrust option selected.

Answer: A

Explanation:

To use PAN-OS multi-factor authentication (MFA) to secure access to critical assets, the enterprise should configure a Captive Portal authentication policy that uses an authentication sequence. An authentication sequence is a feature that allows the firewall to enforce multiple authentication methods (factors) for users who access sensitive services or applications. An authentication sequence can include up to four factors, such as login and password, Voice, SMS, Push, or One-time Password (OTP) authentication. The firewall can integrate with MFA vendors through RADIUS or vendor APIs to provide the additional factors¹².

To configure an authentication sequence, the enterprise needs to create an authentication profile for each factor and then add them to the sequence in the desired order. The enterprise also needs to create a Captive Portal authentication policy that matches the traffic that requires MFA and applies the authentication sequence to it. The Captive Portal is a web page that the firewall displays to users who need to authenticate before accessing the network or the internet. The Captive Portal can be customized to include a welcome message, a login prompt, a disclaimer, a certificate download link, and a logout button³⁴.

When a user tries to access a service or application that matches the Captive Portal authentication policy, the firewall redirects the user to the Captive Portal web form for the first factor. After the user successfully authenticates for the first factor, the firewall prompts the user for the second factor through RADIUS or vendor API integration. The firewall repeats this process until all factors in the sequence are completed or until one factor fails. If all factors are completed successfully, the firewall allows the user to access the service or application. If one factor fails, the firewall denies access and logs an event⁵⁶.

Configuring a Captive Portal authentication policy that uses an authentication profile that references a RADIUS profile is not sufficient to use PAN-OS MFA. This option only provides one factor of authentication through RADIUS integration with an MFA vendor. To use multiple factors of authentication, an authentication sequence is required.

Creating an authentication profile and assigning another authentication factor to be used by a Captive Portal authentication policy is not correct to use PAN-OS MFA. This option does not specify how to create or apply an authentication sequence, which is necessary for enforcing multiple factors of authentication.

Using a Credential Phishing agent to detect, prevent, and mitigate credential phishing campaigns is not relevant to use PAN-OS MFA. This option is a feature of Palo Alto Networks Cortex XDR™ that helps

protect endpoints from credential theft by malicious actors. It does not provide any MFA functionality for accessing critical assets⁷.

References: Authentication Sequence, Configure Multi-Factor Authentication, Configure an Authenticatio Portal, Create an Authentication Profile, Create an Authentication Sequence, Create a Captive Portal Authentication Policy, Credential Phishing Agent

NEW QUESTION 90

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

PCNSE Practice Exam Features:

- * PCNSE Questions and Answers Updated Frequently
- * PCNSE Practice Questions Verified by Expert Senior Certified Staff
- * PCNSE Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * PCNSE Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The PCNSE Practice Test Here](#)