

Exam Questions PCNSE

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

<https://www.2passeasy.com/dumps/PCNSE/>



NEW QUESTION 1

- (Exam Topic 2)

Which CLI command enables an administrator to view details about the firewall including uptime, PAN-OS® version, and serial number?

- A. debug system details
- B. show session info
- C. show system info
- D. show system details

Answer: C

Explanation:

Reference:

https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/technical-documentation/pan-os-60/PAN CLI-ref.pdf

NEW QUESTION 2

- (Exam Topic 2)

If the firewall has the link monitoring configuration, what will cause a failover?

- A. ethernet1/3 and ethernet1/6 going down
- B. ethernet1/3 going down
- C. ethernet1/3 or Ethernet1/6 going down
- D. ethernet1/6 going down

Answer: A

NEW QUESTION 3

- (Exam Topic 2)

A client has a sensitive application server in their data center and is particularly concerned about session flooding because of denial of-service attacks. How can the Palo Alto Networks NGFW be configured to specifically protect this server against session floods originating from a single IP address?

- A. Define a custom App-ID to ensure that only legitimate application traffic reaches the server
- B. Add QoS Profiles to throttle incoming requests
- C. Add a tuned DoS Protection Profile
- D. Add an Anti-Spyware Profile to block attacking IP address

Answer: C

NEW QUESTION 4

- (Exam Topic 2)

What are the differences between using a service versus using an application for Security Policy match?

- A. Use of a "service" enables the firewall to take action after enough packets allow for App-ID identification
- B. Use of a "service" enables the firewall to take immediate action with the first observed packet based on port numbers Use of an "application" allows the firewall to take action after enough packets allow for App-ID identification regardless of the ports being used.
- C. There are no differences between "service" or "application" Use of an "application" simplifies configuration by allowing use of a friendly application name instead of port numbers.
- D. Use of a "service" enables the firewall to take immediate action with the first observed packet based on port number
- E. Use of an "application" allows the firewall to take immediate action if the port being used is a member of the application standard port list

Answer: B

NEW QUESTION 5

- (Exam Topic 2)

Refer to the exhibit.

An administrator is using DNAT to map two servers to a single public IP address. Traffic will be steered to the specific server based on the application, where Host A (10.1.1.100) received HTTP traffic and host B(10.1.1.101) receives SSH traffic. Which two security policy rules will accomplish this configuration? (Choose two)

- A. Untrust (Any) to Untrust (10.1.1.1) Ssh-Allow
- B. Untrust (Any) to DMZ (1.1.1.100) Ssh-Allow
- C. Untrust (Any) to DMZ (1.1.1.100) Web-browsing -Allow
- D. Untrust (Any) to Untrust (10.1.1.1) Web-browsing -Allow

Answer: CD

NEW QUESTION 6

- (Exam Topic 2)

What is exchanged through the HA2 link?

- A. hello heartbeats
- B. User-ID information
- C. session synchronization
- D. HA state information

Answer: C

Explanation:

Reference:

<https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/high-availability/ha-links-and-backup-links>

NEW QUESTION 7

- (Exam Topic 2)

Which item enables a firewall administrator to see details about traffic that is currently active through the NGFW?

- A. ACC
- B. System Logs
- C. App Scope
- D. Session Browser

Answer: D

NEW QUESTION 8

- (Exam Topic 2)

An administrator sees several inbound sessions identified as unknown-tcp in the traffic logs. The administrator determines that these sessions are from external users accessing the company's proprietary accounting application. The administrator wants to reliably identify this as their accounting application and to scan this traffic for threats. Which option would achieve this result?

- A. Create an Application Override policy and a custom threat signature for the application
- B. Create an Application Override policy
- C. Create a custom App-ID and use the "ordered conditions" check box
- D. Create a custom App ID and enable scanning on the advanced tab

Answer: D

NEW QUESTION 9

- (Exam Topic 2)

Which two methods can be used to verify firewall connectivity to AutoFocus? (Choose two.)

- A. Verify AutoFocus status using CLI.
- B. Check the WebUI Dashboard AutoFocus widget.
- C. Check for WildFire forwarding logs.
- D. Check the license
- E. Verify AutoFocus is enabled below Device Management tab.

Answer: DE

Explanation:

Reference:

<https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/getting-started/enable-autofocus-threat-intel>

NEW QUESTION 10

- (Exam Topic 2)

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. Configuration Logs
- B. System Logs
- C. Task Manager
- D. Traffic Logs

Answer: BC

NEW QUESTION 10

- (Exam Topic 2)

SAML SLO is supported for which two firewall features? (Choose two.)

- A. GlobalProtect Portal
- B. CaptivePortal
- C. WebUI
- D. CLI

Answer: AB

NEW QUESTION 13

- (Exam Topic 2)

What is the purpose of the firewall decryption broker?

- A. Decrypt SSL traffic and then send it as cleartext to a security chain of inspection tools
- B. Force decryption of previously unknown cipher suites
- C. Inspection traffic within IPsec tunnel
- D. Reduce SSL traffic to a weaker cipher before sending it to a security chain of inspection tools

Answer: A

NEW QUESTION 15

- (Exam Topic 2)

A Palo Alto Networks NGFW just submitted a file to WildFire for analysis. Assume a 5-minute window for analysis. The firewall is configured to check for verdicts every 5 minutes.

How quickly will the firewall receive back a verdict?

- A. More than 15 minutes
- B. 5 minutes
- C. 10 to 15 minutes
- D. 5 to 10 minutes

Answer: D

NEW QUESTION 19

- (Exam Topic 2)

On the NGFW, how can you generate and block a private key from export and thus harden your security posture and prevent rogue administrators or other bad actors from misusing keys?

- A. * 1. Select Device > Certificate Management > Certificates > Device > Certificates* 2. Import the certificate.* 3 Select Import Private Key* 4 Click Generate to generate the new certificate
- B. * 1 Select Device > Certificates * 2 Select Certificate Profile* 3 Generate the certificate* 4 Select Block Private Key Export.
- C. * 1 Select Device > Certificates * 2 Select Certificate Profile.* 3 Generate the certificate* 4 Select Block Private Key Export
- D. * 1 Select Device > Certificate Management > Certificates > Device > Certificates * 2 Generate the certificate* 3 Select Block Private Key Export* 4 Click Generate to generate the new certificate.

Answer: D

NEW QUESTION 20

- (Exam Topic 2)

When is the content inspection performed in the packet flow process?

- A. after the application has been identified
- B. before session lookup
- C. before the packet forwarding process
- D. after the SSL Proxy re-encrypts the packet

Answer: A

Explanation:

Reference:

<https://live.paloaltonetworks.com/t5/Learning-Articles/Packet-Flow-Sequence-in-PAN-OS/ta-p/56081>

NEW QUESTION 22

- (Exam Topic 2)

Refer to the exhibit.

Which certificates can be used as a Forwarded Trust certificate?

- A. Certificate from Default Trust Certificate Authorities
- B. Domain Sub-CA
- C. Forward_Trust
- D. Domain-Root-Cert

Answer: B

NEW QUESTION 25

- (Exam Topic 2)

Which CLI command can be used to export the tcpdump capture?

- A. scp export tcpdump from mgmt.pcap to <username@host:path>
- B. scp extract mgmt-pcap from mgmt.pcap to <username@host:path>
- C. scp export mgmt-pcap from mgmt.pcap to <username@host:path>
- D. download mgmt.-pcap

Answer: C

Explanation:

Reference:

<https://live.paloaltonetworks.com/t5/Management-Articles/How-To-Packet-Capture-tcpdump-On-Management-p/55415>

NEW QUESTION 27

- (Exam Topic 2)

A speed/duplex negotiation mismatch is between the Palo Alto Networks management port and the switch port which it connects. How would an administrator configure the interface to 1Gbps?

- A. set deviceconfig interface speed-duplex 1Gbps-full-duplex
- B. set deviceconfig system speed-duplex 1Gbps-duplex
- C. set deviceconfig system speed-duplex 1Gbps-full-duplex
- D. set deviceconfig Interface speed-duplex 1Gbps-half-duplex

Answer: C

Explanation:

Reference:

<https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Change-the-Speed-and-Duplex-of-the-Man-Port/ta-p/59034>

user@PA# set deviceconfig system speed-duplex100Mbps-full-duplex

100Mbps-full-duplex100Mbps-half-duplex 100Mbps-half-duplex10Mbps-full-duplex 10Mbps-full-duplex10Mbps-half-duplex 10Mbps-half-duplex1Gbps-full-duplex

1Gbps-full-duplex1Gbps-half-duplex 1Gbps-half-duplexauto-negotiate auto-negotiate

NEW QUESTION 31

- (Exam Topic 2)

Which option enables a Palo Alto Networks NGFW administrator to schedule Application and Threat updates while applying only new content-IDs to traffic?

- A. Select download-and-install.
- B. Select download-and-install, with "Disable new apps in content update" selected.
- C. Select download-only.
- D. Select disable application updates and select "Install only Threat updates"

Answer: C

NEW QUESTION 35

- (Exam Topic 2)

Which data flow describes redistribution of user mappings?

- A. User-ID agent to firewall
- B. firewall to firewall
- C. Domain Controller to User-ID agent
- D. User-ID agent to Panorama

Answer: B

Explanation:

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

NEW QUESTION 40

- (Exam Topic 2)

If a template stack is assigned to a device and the stack includes three templates with overlapping settings, which settings are published to the device when the template stack is pushed?

- A. The settings assigned to the template that is on top of the stack.
- B. The administrator will be promoted to choose the settings for that chosen firewall.
- C. All the settings configured in all templates.
- D. Depending on the firewall location, Panorama decides with settings to send.

Answer: A

Explanation:

Reference:

https://www.paloaltonetworks.com/documentation/80/panorama/panorama_adminguide/manage-firewalls/mana-templates-and-template-stacks/configure-a-template-stack

NEW QUESTION 43

- (Exam Topic 2)

Which feature must you configure to prevent users from accidentally submitting their corporate credentials to a phishing website?

- A. URL Filtering profile
- B. Zone Protection profile
- C. Anti-Spyware profile
- D. Vulnerability Protection profile

Answer: A

Explanation:

Reference:

<https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/threat-prevention/prevent-credential-phishing>

NEW QUESTION 46

- (Exam Topic 2)

Where can an administrator see both the management plane and data plane CPU utilization in the WebUI?

- A. System log
- B. CPU Utilization widget
- C. Resources widget
- D. System Utilization log

Answer: C

Explanation:

System Resources (widget) Displays the Management CPU usage, Data Plane usage, and the Session Count (the number of sessions established through the firewall or

Panorama). <https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-web-interface-help/dashboard/dashboard-widgets>

NEW QUESTION 49

- (Exam Topic 2)

VPN traffic intended for an administrator's Palo Alto Networks NGFW is being maliciously intercepted and retransmitted by the interceptor. When creating a VPN tunnel, which protection profile can be enabled to prevent this malicious behavior?

- A. Zone Protection
- B. DoS Protection
- C. Web Application
- D. Replay

Answer: D

Explanation:

<https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/vpns/set-up-site-to-site-vpn/set-up-an-ipsec>

NEW QUESTION 53

- (Exam Topic 2)

A company needs to preconfigure firewalls to be sent to remote sites with the least amount of reconfiguration. Once deployed, each firewall must establish secure tunnels back to multiple regional data centers to include the future regional data centers.

Which VPN configuration would adapt to changes when deployed to the future site?

- A. Preconfigured GlobalProtect satellite
- B. Preconfigured GlobalProtect client
- C. Preconfigured IPsec tunnels
- D. Preconfigured PPTP Tunnels

Answer: A

Explanation:

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/large-scale-vpn-lsvpn/configure-the-globalprotect>

NEW QUESTION 56

- (Exam Topic 2)

Which GlobalProtect Client connect method requires the distribution and use of machine certificates?

- A. User-logon (Always on)
- B. At-boot
- C. On-demand
- D. Pre-logon

Answer: D

NEW QUESTION 60

- (Exam Topic 2)

Which two benefits come from assigning a Decryption Profile to a Decryption policy rule with a "No Decrypt" action? (Choose two.)

- A. Block sessions with expired certificates

- B. Block sessions with client authentication
- C. Block sessions with unsupported cipher suites
- D. Block sessions with untrusted issuers
- E. Block credential phishing

Answer: AD

Explanation:

<https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/decryption/configure-decryption-exception>

NEW QUESTION 62

- (Exam Topic 2)

Which Panorama administrator types require the configuration of at least one access domain? (Choose two)

- A. Dynamic
- B. Custom Panorama Admin
- C. Role Based
- D. Device Group
- E. Template Admin

Answer: DE

NEW QUESTION 66

- (Exam Topic 2)

What are the two behavior differences between Highlight Unused Rules and the Rule Usage Hit counter when a firewall is rebooted? (Choose two.)

- A. Rule Usage Hit counter will not be reset
- B. Highlight Unused Rules will highlight all rules.
- C. Highlight Unused Rules will highlight zero rules.
- D. Rule Usage Hit counter will reset.

Answer: AB

NEW QUESTION 70

- (Exam Topic 2)

A customer has an application that is being identified as unknown-top for one of their custom PostgreSQL database connections. Which two configuration options can be used to correctly categorize their custom database application? (Choose two.)

- A. Application Override policy.
- B. Security policy to identify the custom application.
- C. Custom application.
- D. Custom Service object.

Answer: AC

Explanation:

Unlike the App-ID engine, which inspects application packet contents for unique signature elements, the Application Override policy's matching conditions are limited to header-based data only. Traffic matched by an Application Override policy is identified by the App-ID entered in the Application entry box. Choices are limited to applications currently in the App-ID database. Because this traffic bypasses all Layer 7 inspection, the resulting security is that of a Layer-4 firewall. Thus, this traffic should be trusted without the need for Content-ID inspection. The resulting application assignment can be used in other firewall functions such as Security policy and QoS. Use Cases Three primary uses cases for Application Override Policy are:

To identify "Unknown" App-IDs with a different or custom application signature To re-identify an existing application signature

To bypass the Signature Match Engine (within the SP3 architecture) to improve processing times A discussion of typical uses of application override and specific implementation examples is here: <https://live.paloaltonetworks.com/t5/Learning-Articles/Tips-amp-Tricks-How-to-Create-an-Application>

NEW QUESTION 73

- (Exam Topic 2)

An administrator has configured a QoS policy rule and a QoS profile that limits the maximum allowable bandwidth for the YouTube application. However, YouTube is consuming more than the maximum bandwidth allotment configured.

Which configuration step needs to be configured to enable QoS?

- A. Enable QoS Data Filtering Profile
- B. Enable QoS monitor
- C. Enable Qos interface
- D. Enable Qos in the interface Management Profile.

Answer: C

Explanation:

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface-help/network/network-qos/qos-interface-set>

NEW QUESTION 78

- (Exam Topic 2)

When configuring the firewall for packet capture, what are the valid stage types?

- A. Receive, management, transmit, and drop
- B. Receive, firewall, send, and non-syn
- C. Receive management, transmit, and non-syn

D. Receive , firewall, transmit, and drop

Answer: D

NEW QUESTION 83

- (Exam Topic 2)

Which three firewall states are valid? (Choose three.)

- A. Active
- B. Functional
- C. Pending
- D. Passive
- E. Suspended

Answer: ADE

Explanation:

Reference:

<https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/high-availability/ha-firewall-states>

NEW QUESTION 86

- (Exam Topic 2)

Which two subscriptions are available when configuring panorama to push dynamic updates to connected devices? (Choose two.)

- A. Content-ID
- B. User-ID
- C. Applications and Threats
- D. Antivirus

Answer: CD

Explanation:

Reference:

<https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/device/device-dynamic-update>

NEW QUESTION 89

- (Exam Topic 2)

Which two methods can be configured to validate the revocation status of a certificate? (Choose two.)

- A. CRL
- B. CRT
- C. OCSP
- D. Cert-Validation-Profile
- E. SSL/TLS Service Profile

Answer: AC

NEW QUESTION 92

- (Exam Topic 2)

An administrator has been asked to configure active/passive HA for a pair of Palo Alto Networks NGFWs. The administrator assigns priority 100 to the active firewall.

Which priority is correct for the passive firewall?

- A. 99
- B. 1
- C. 255

Answer: D

Explanation:

Reference:

[https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/framemaker/71/pan-os/pan-os/section_5. \(page 9\)](https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/framemaker/71/pan-os/pan-os/section_5. (page 9))

https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/10-0/pan-os-admin/pan-os-admin.pd page 315

NEW QUESTION 94

- (Exam Topic 1)

Which CLI command displays the physical media that are connected to ethernetl/8?

- A. > show system state filter-pretty sys.si.p8.stats
- B. > show interface ethernetl/8
- C. > show system state filter-pretty sys.sl.p8.phy
- D. > show system state filter-pretty sys.si.p8.med

Answer: D

NEW QUESTION 98

- (Exam Topic 1)

A variable name must start with which symbol?

- A. \$
- B. &
- C. !
- D. #

Answer: A

Explanation:

<https://docs.paloaltonetworks.com/panorama/8-1/panorama-admin/manage-firewalls/manage-templates-and-tem>

NEW QUESTION 102

- (Exam Topic 1)

Below are the steps in the workflow for creating a Best Practice Assessment in a firewall and Panorama configuration Place the steps in order.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 106

- (Exam Topic 1)

Match each GlobalProtect component to the purpose of that component

- A. Mastered
- B. Not Mastered

Answer: A

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 111

- (Exam Topic 1)

In a firewall, which three decryption methods are valid? (Choose three)

- A. SSL Inbound Inspection
- B. SSL Outbound Proxyless Inspection
- C. SSL Inbound Proxy
- D. Decryption Mirror
- E. SSH Proxy

Answer: ADE

NEW QUESTION 112

- (Exam Topic 1)

An organization is building a Bootstrap Package to deploy Palo Alto Networks VM-Series firewalls into their AWS tenant Which two statements are correct regarding the bootstrap package contents? (Choose two)

- A. The /config /content and /software folders are mandatory while the /license and /plugin folders are optional
- B. The bootstrap package is stored on an AFS share or a discrete container file bucket
- C. The directory structure must include a /config /content, /software and /license folders
- D. The init-cfg txt and bootstrap.xml files are both optional configuration items for the /config folder
- E. The bootstrap xml file allows for automated deployment of VM-Series firewalls with full network and policy configurations.

Answer: DE

NEW QUESTION 116

- (Exam Topic 1)

Place the steps in the WildFire process workflow in their correct order.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Timeline Description automatically generated

<https://docs.paloaltonetworks.com/wildfire/9-1/wildfire-admin/wildfire-overview/about-wildfire.html>

NEW QUESTION 118

- (Exam Topic 1)

Before you upgrade a Palo Alto Networks NGFW what must you do?

- A. Make sure that the PAN-OS support contract is valid for at least another year
- B. Export a device state of the firewall
- C. Make sure that the firewall is running a version of antivirus software and a version of WildFire that support the licensed subscriptions.
- D. Make sure that the firewall is running a supported version of the app + threat update

Answer: B

NEW QUESTION 123

- (Exam Topic 1)

A firewall is configured with SSL Forward Proxy decryption and has the following four enterprise certificate authorities (Cas)

- A. Enterprise-Trusted-CA; which is verified as Forward Trust Certificate (The CA is also installed in the trusted store of the end-user browser and system)i
- B. Enterpnse-Untrusted-CA, which is verified as Forward Untrust Certificateii
- C. Enterprise-Intermediate-CAi
- D. Enterprise-Root-CA which is verified only as Trusted Root CAAn end-user visits [https //www example-website com/](https://www.example-website.com/) with a server certificate Common Name (CN) [www example-website com](https://www.example-website.com/) The firewall does the SSL Forward Proxy decryption for the website and the server certificate is not trusted by the firewallThe end-user's browser will show that the certificate for [www example-website com](https://www.example-website.com/) was issued by which of the following?
- E. Enterprise-Untrusted-CA which is a self-signed CA
- F. Enterprise-Trusted-CA which is a self-signed CA
- G. Enterprise-Intermediate-CA which wa
- H. in turn, issued by Enterprise-Root-CA
- I. Enterprise-Root-CA which is a self-signed CA

Answer: B

NEW QUESTION 126

- (Exam Topic 1)

A traffic log might list an application as "not-applicable" for which two reasons'? (Choose two)

- A. 0The firewall did not install the session
- B. The TCP connection terminated without identifying any application data
- C. The firewall dropped a TCP SYN packet
- D. There was not enough application data after the TCP connection was established

Answer: AD

NEW QUESTION 130

- (Exam Topic 1)

An engineer must configure the Decryption Broker feature

Which Decryption Broker security chain supports bi-directional traffic flow?

- A. Layer 2 security chain
- B. Layer 3 security chain
- C. Transparent Bridge security chain
- D. Transparent Proxy security chain

Answer: B

Explanation:

Together, the primary and secondary interfaces form a pair of decryption forwarding interfaces. Only interfaces that you have enabled to be Decrypt Forward interfaces are displayed here. Your security chain type (Layer 3 or Transparent Bridge) and the traffic flow direction (unidirectional or bidirectional) determine which of the two interfaces forwards allowed, clear text traffic to the security chain, and which interface receives the traffic back from the security chain after it has undergone additional enforcement.

NEW QUESTION 134

- (Exam Topic 1)

The SSL Forward Proxy decryption policy is configured. The following four certificate authority (CA) certificates are installed on the firewall.

An end-user visits the untrusted website [https //www firewall-do-not-trust-website com](https://www.firewall-do-not-trust-website.com)

Which certificate authority (CA) certificate will be used to sign the untrusted webserver certificate?

- A. Forward-Untrust-Certificate
- B. Forward-Trust-Certificate
- C. Firewall-CA
- D. Firewall-Trusted-Root-CA

Answer: B

NEW QUESTION 136

- (Exam Topic 1)

In a security-first network what is the recommended threshold value for content updates to be dynamically updated?

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

Answer: B

Explanation:

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

NEW QUESTION 139

- (Exam Topic 1)

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: ADE

NEW QUESTION 144

- (Exam Topic 1)

An administrator needs to troubleshoot a User-ID deployment The administrator believes that there is an issue related to LDAP authentication The administrator

wants to create a packet capture on the management plane

Which CLI command should the administrator use to obtain the packet capture for validating the configuration^

- A. > ftp export mgmt-pcap from mgmt.pcap to <FTP host>
- B. > scp export mgmt-pcap from mgmt.pcap to {usernameQhost:path>
- C. > scp export pcap-mgmt from pcap.mgiat to (username@host:path)
- D. > scp export pcap from pcap to (usernameQhost:path)

Answer: C

NEW QUESTION 147

- (Exam Topic 1)

An administrator wants to upgrade a firewall HA pair to PAN-OS 10.1 The firewalls are currently running PAN-OS 8.1.17.

Which upgrade path maintains synchronization of the HA session (and prevents network outage)?

- A. Upgrade directly to the target major version
- B. Upgrade one major version at a time
- C. Upgrade the HA pair to a base image
- D. Upgrade two major versions at a time

Answer: D

NEW QUESTION 148

- (Exam Topic 1)

A company needs to preconfigure firewalls to be sent to remote sites with the least amount of preconfiguration Once deployed each firewall must establish secure tunnels back to multiple regional data centers to include the future regional data centers

Which VPN preconfigured configuration would adapt to changes when deployed to the future site?

- A. IPsec tunnels using IKEv2
- B. PPTP tunnels
- C. GlobalProtect satellite
- D. GlobalProtect client

Answer: C

NEW QUESTION 153

- (Exam Topic 1)

Please match the terms to their corresponding definitions.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 157

- (Exam Topic 1)

Given the following configuration, which route is used for destination 10.10.0.4?

- A. Route 4
- B. Route 3
- C. Route 1
- D. Route 3

Answer: A

NEW QUESTION 159

- (Exam Topic 2)

Which four NGFW multi-factor authentication factors are supported by PAN-OS? (Choose four.)

- A. Short message service
- B. Push
- C. User logon
- D. Voice
- E. SSH key
- F. One-Time Password

Answer: ABDF

Explanation:

<https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/authentication/authentication-types/multi-factor-aut>

NEW QUESTION 160

- (Exam Topic 2)

Which two features can be used to tag a username so that it is included in a dynamic user group? (Choose two)

- A. log forwarding auto-tagging
- B. GlobalProtect agent
- C. User-ID Windows-based agent
- D. XML API

Answer: BC

NEW QUESTION 162

- (Exam Topic 2)

An administrator needs to optimize traffic to prefer business-critical applications over non-critical applications. QoS natively integrates with which feature to provide service quality?

- A. Port Inspection
- B. Certificate revocation
- C. Content-ID
- D. App-ID

Answer: D

Explanation:

Reference:

<https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/quality-of-service/qos-for-applications-and>

NEW QUESTION 164

- (Exam Topic 2)

Based on the image, what caused the commit warning?

- A. The CA certificate for FWDtrust has not been imported into the firewall.
- B. The FWDtrust certificate has not been flagged as Trusted Root CA.
- C. SSL Forward Proxy requires a public certificate to be imported into the firewall.
- D. The FWDtrust certificate does not have a certificate chain.

Answer: D

NEW QUESTION 169

- (Exam Topic 2)

Which method does an administrator use to integrate all non-native MFA platforms in PAN-OS® software?

- A. Okta
- B. DUO
- C. RADIUS
- D. PingID

Answer: C

Explanation:

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/authentication/authentication-types/multi-factor-aut>

NEW QUESTION 173

- (Exam Topic 3)

When using the predefined default profile, the policy will inspect for viruses on the decoders. Match each decoder with its default action.

Answer options may be used more than once or not at all.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

IMAP , POP3 , SMTP - > Alert

HTTP,FTP,SMB -> Reset-both

NEW QUESTION 178

- (Exam Topic 3)

Which three function are found on the dataplane of a PA-5050? (Choose three)

- A. Protocol Decoder
- B. Dynamic routing
- C. Management
- D. Network Processing
- E. Signature Match

Answer: BDE

NEW QUESTION 182

- (Exam Topic 3)

Click the Exhibit button

An administrator has noticed a large increase in bittorrent activity. The administrator wants to determine where the traffic is going on the company. What would be the administrator's next step?

- A. Right-Click on the bittorrent link and select Value from the context menu
- B. Create a global filter for bittorrent traffic and then view Traffic logs.
- C. Create local filter for bittorrent traffic and then view Traffic logs.
- D. Click on the bittorrent application link to view network activity

Answer: D

NEW QUESTION 187

- (Exam Topic 3)

During the packet flow process, which two processes are performed in application identification? (Choose two.)

- A. pattern based application identification
- B. application changed from content inspection
- C. session application identified
- D. application override policy match

Answer: AD

NEW QUESTION 191

- (Exam Topic 3)

What are three valid actions in a File Blocking Profile? (Choose three)

- A. Forward
- B. Block
- C. Alert
- D. Upload
- E. Reset-both
- F. Continue

Answer: ABC

Explanation:

<https://live.paloaltonetworks.com/t5/Configuration-Articles/File-Blocking-Rulebase-and-Action-Precedence/ta-p>

NEW QUESTION 196

- (Exam Topic 3)

A VPN connection is set up between Site-A and Site-B, but no traffic is passing in the system log of Site-A, there is an event logged as like-nego-p1-fail-psk. What action will bring the VPN up and allow traffic to start passing between the sites?

- A. Change the Site-B IKE Gateway profile version to match Site-A,
- B. Change the Site-A IKE Gateway profile exchange mode to aggressive mode.
- C. Enable NAT Traversal on the Site-A IKE Gateway profile.
- D. Change the pre-shared key of Site-B to match the pre-shared key of Site-A

Answer: D

NEW QUESTION 201

- (Exam Topic 3)

A file sharing application is being permitted and no one knows what this application is used for. How should this application be blocked?

- A. Block all unauthorized applications using a security policy
- B. Block all known internal custom applications
- C. Create a WildFire Analysis Profile that blocks Layer 4 and Layer 7 attacks
- D. Create a File blocking profile that blocks Layer 4 and Layer 7 attacks

Answer: D

NEW QUESTION 202

- (Exam Topic 3)

A client is deploying a pair of PA-5000 series firewalls using High Availability (HA) in Active/Passive mode. Which statement is true about this deployment?

- A. The two devices must share a routable floating IP address
- B. The two devices may be different models within the PA-5000 series
- C. The HA1 IP address from each peer must be on a different subnet
- D. The management port may be used for a backup control connection

Answer: D

NEW QUESTION 205

- (Exam Topic 3)

A network security engineer needs to configure a virtual router using IPv6 addresses. Which two routing options support these addresses? (Choose two)

- A. BGP not sure
- B. OSPFv3
- C. RIP
- D. Static Route

Answer: BD

Explanation:

<https://live.paloaltonetworks.com/t5/Management-Articles/Does-PAN-OS-Support-Dynamic-Routing-Protocols>

NEW QUESTION 206

- (Exam Topic 3)

Which Public Key infrastructure component is used to authenticate users for GlobalProtect when the Connect Method is set to pre-logon?

- A. Certificate revocation list
- B. Trusted root certificate
- C. Machine certificate
- D. Online Certificate Status Protocol

Answer: C

NEW QUESTION 208

- (Exam Topic 3)

Which two interface types can be used when configuring GlobalProtect Portal?(Choose two)

- A. Virtual Wire
- B. Loopback
- C. Layer 3
- D. Tunnel

Answer: BC

NEW QUESTION 213

- (Exam Topic 3)

A company is upgrading its existing Palo Alto Networks firewall from version 7.0.1 to 7.0.4.

Which three methods can the firewall administrator use to install PAN-OS 8.0.4 across the enterprise?(Choose three)

- A. Download PAN-OS 8.0.4 files from the support site and install them on each firewall after manually uploading.
- B. Download PAN-OS 8.0.4 to a USB drive and the firewall will automatically update after the USB drive is inserted in the firewall.
- C. Push the PAN-OS 8.0.4 updates from the support site to install on each firewall.
- D. Push the PAN-OS 8.0.4 update from one firewall to all of the other remaining after updating one firewall.
- E. Download and install PAN-OS 8.0.4 directly on each firewall.
- F. Download and push PAN-OS 8.0.4 from Panorama to each firewall.

Answer: ACF

NEW QUESTION 214

- (Exam Topic 3)

Which three rule types are available when defining policies in Panorama? (Choose three.)

- A. Pre Rules
- B. Post Rules
- C. Default Rules
- D. Stealth Rules
- E. Clean Up Rules

Answer: ABC

Explanation:

<https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/panorama-web-interface/defini>

NEW QUESTION 216

- (Exam Topic 3)

An Administrator is configuring an IPSec VPN to a Cisco ASA at the administrator's home and experiencing issues completing the connection. The following is the output from the command:

less mp-log ikemgr.log:

What could be the cause of this problem?

- A. The public IP addresses do not match for both the Palo Alto Networks Firewall and the ASA.
- B. The Proxy IDs on the Palo Alto Networks Firewall do not match the settings on the ASA.
- C. The shared secrets do not match between the Palo Alto firewall and the ASA
- D. The dead peer detection settings do not match between the Palo Alto Networks Firewall and the ASA

Answer: B

NEW QUESTION 217

- (Exam Topic 3)

How does Panorama handle incoming logs when it reaches the maximum storage capacity?

- A. Panorama discards incoming logs when storage capacity is full.
- B. Panorama stops accepting logs until licenses for additional storage space are applied
- C. Panorama stops accepting logs until a reboot to clean storage space.
- D. Panorama automatically deletes older logs to create space for new ones.

Answer: D

Explanation:

(https://www.paloaltonetworks.com/documentation/60/panorama/panorama_adminguide/set-up-panorama/deter

NEW QUESTION 221

- (Exam Topic 3)

Which URL Filtering Security Profile action toggles the URL Filtering category to the URL Filtering log?

- A. Log
- B. Alert
- C. Allow
- D. Default

Answer: B

NEW QUESTION 222

- (Exam Topic 3)

A Network Administrator wants to deploy a Large Scale VPN solution. The Network Administrator has chosen a GlobalProtect Satellite solution. This configuration needs to be deployed to multiple remote offices and the Network Administrator decides to use Panorama to deploy the configurations. How should this be accomplished?

- A. Create a Template with the appropriate IKE Gateway settings
- B. Create a Template with the appropriate IPSec tunnel settings
- C. Create a Device Group with the appropriate IKE Gateway settings
- D. Create a Device Group with the appropriate IPSec tunnel settings

Answer: B

NEW QUESTION 223

- (Exam Topic 3)

Which three log-forwarding destinations require a server profile to be configured? (Choose three)

- A. SNMP Trap
- B. Email
- C. RADIUS
- D. Kerberos
- E. Panorama
- F. Syslog

Answer: ABF

NEW QUESTION 226

- (Exam Topic 3)

In an enterprise deployment, a network security engineer wants to assign to a group of administrators without creating local administrator accounts on the firewall. Which authentication method must be used?

- A. LDAP
- B. Kerberos
- C. Certification based authentication
- D. RADIUS with Vendor-Specific Attributes

Answer: D

NEW QUESTION 229

- (Exam Topic 3)

Several offices are connected with VPNs using static IPV4 routes. An administrator has been tasked with implementing OSPF to replace static routing. Which step is required to accomplish this goal?

- A. Assign an IP address on each tunnel interface at each site
- B. Enable OSPFv3 on each tunnel interface and use Area ID 0.0.0.0
- C. Assign OSPF Area ID 0.0.0.0 to all Ethernet and tunnel interfaces
- D. Create new VPN zones at each site to terminate each VPN connection

Answer: C

NEW QUESTION 234

- (Exam Topic 3)

A company has a policy that denies all applications it classifies as bad and permits only application it classifies as good. The firewall administrator created the following security policy on the company's firewall.

Which interface configuration will accept specific VLAN IDs?

Which two benefits are gained from having both rule 2 and rule 3 presents? (choose two)

- A. A report can be created that identifies unclassified traffic on the network.
- B. Different security profiles can be applied to traffic matching rules 2 and 3.
- C. Rule 2 and 3 apply to traffic on different ports.
- D. Separate Log Forwarding profiles can be applied to rules 2 and 3.

Answer: BD

NEW QUESTION 239

- (Exam Topic 3)

A network design calls for a "router on a stick" implementation with a PA-5060 performing inter-VLAN routing All VLAN-tagged traffic will be forwarded to the PA-5060 through a single dot1q trunk interface
Which interface type and configuration setting will support this design?

- A. Trunk interface type with specified tag
- B. Layer 3 interface type with specified tag
- C. Layer 2 interface type with a VLAN assigned
- D. Layer 3 subinterface type with specified tag

Answer: D

NEW QUESTION 240

- (Exam Topic 3)
Refer to Exhibit:

A firewall has three PDF rules and a default route with a next hop of 172.29.19.1 that is configured in the default VR. A user named XX-bes a PC with a 192.168.101.10 IP address.
He makes an HTTPS connection to 172.16.10.29.
What is the next hop IP address for the HTTPS traffic from Wills PC.

- A. 172.20.30.1
- B. 172.20.20.1
- C. 172.20.10.1
- D. 172.20.40.1

Answer: B

NEW QUESTION 244

- (Exam Topic 3)
Panorama provides which two SD_WAN functions? (Choose two.)

- A. data plane
- B. physical network links
- C. network monitoring
- D. control plane

Answer: CD

NEW QUESTION 246

- (Exam Topic 3)
What can missing SSL packets when performing a packet capture on dataplane interfaces?

- A. The packets are hardware offloaded to the offloaded processor on the dataplane
- B. The missing packets are offloaded to the management plane CPU
- C. The packets are not captured because they are encrypted
- D. There is a hardware problem with offloading FPGA on the management plane

Answer: A

NEW QUESTION 251

- (Exam Topic 3)
Which CLI command displays the current management plan memory utilization?

- A. > show system info
- B. > show system resources
- C. > debug management-server show
- D. > show running resource-monitor

Answer: B

Explanation:

<https://live.paloaltonetworks.com/t5/Management-Articles/Show-System-Resource-Command-Displays-CPU-U>

NEW QUESTION 256

- (Exam Topic 3)

A company has a web server behind a Palo Alto Networks next-generation firewall that it wants to make accessible to the public at 1.1.1.1. The company has decided to configure a destination NAT Policy rule.

Given the following zone information:

- DMZ zone: DMZ-L3
- Public zone: Untrust-L3
- Guest zone: Guest-L3
- Web server zone: Trust-L3
- Public IP address (Untrust-L3): 1.1.1.1
- Private IP address (Trust-L3): 192.168.1.50

What should be configured as the destination zone on the Original Packet tab of NAT Policy rule?

- A. Untrust-L3
- B. DMZ-L3
- C. Guest-L3
- D. Trust-L3

Answer: A

NEW QUESTION 259

- (Exam Topic 3)

Which two options are required on an M-100 appliance to configure it as a Log Collector? (Choose two)

- A. From the Panorama tab of the Panorama GUI select Log Collector mode and then commit changes
- B. Enter the command request system system-mode logger then enter Y to confirm the change to Log Collector mode.
- C. From the Device tab of the Panorama GUI select Log Collector mode and then commit changes.
- D. Enter the command logger-mode enable then enter Y to confirm the change to Log Collector mode.
- E. Log in the Panorama CLI of the dedicated Log Collector

Answer: BE

Explanation:

(https://www.paloaltonetworks.com/documentation/60/panorama/panorama_adminguide/set-up-panorama/set-u)

NEW QUESTION 262

- (Exam Topic 3)

Which URL Filtering Security Profile action logs the URL Filtering category to the URL Filtering log?

- A. Log
- B. Alert
- C. Allow
- D. Default

Answer: B

Explanation:

<https://www.paloaltonetworks.com/documentation/70/pan-os/pan-os/url-filtering/url-filtering-profile-actions>

NEW QUESTION 266

- (Exam Topic 3)

A company hosts a publicly accessible web server behind a Palo Alto Networks next-generation firewall with the following configuration information:

- * Users outside the company are in the "Untrust-L3" zone.
- * The web server physically resides in the "Trust-L3" zone.
- * Web server public IP address: 23.54.6.10
- * Web server private IP address: 192.168.1.10

Which two items must the NAT policy contain to allow users in the Untrust-L3 zone to access the web server? (Choose two.)

- A. Destination IP of 23.54.6.10
- B. UntrustL3 for both Source and Destination Zone
- C. Destination IP of 192.168.1.10
- D. UntrustL3 for Source Zone and Trust-L3 for Destination Zone

Answer: AB

NEW QUESTION 269

- (Exam Topic 3)

When a malware-infected host attempts to resolve a known command-and-control server, the traffic matches a security policy with DNS sinhole enabled,

generating a traffic log.

What will be the destination IP Address in that log entry?

- A. The IP Address of sinkhole.paloaltonetworks.com
- B. The IP Address of the command-and-control server
- C. The IP Address specified in the sinkhole configuration
- D. The IP Address of one of the external DNS servers identified in the anti-spyware database

Answer: C

Explanation:

<https://live.paloaltonetworks.com/t5/Management-Articles/How-to-Verify-DNS-Sinkhole-Function-is-Working/>

NEW QUESTION 274

- (Exam Topic 3)

Which option is an IPv6 routing protocol?

- A. RIPv3
- B. OSPFv3
- C. OSPv3
- D. BGP NG

Answer: B

NEW QUESTION 276

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual PCNSE Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the PCNSE Product From:

<https://www.2passeasy.com/dumps/PCNSE/>

Money Back Guarantee

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