



# **Paloalto-Networks**

## **Exam Questions PCNSE**

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

## About ExamBible

*[Your Partner of IT Exam](#)*

## Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

## Our Advances

### \* 99.9% Uptime

All examinations will be up to date.

### \* 24/7 Quality Support

We will provide service round the clock.

### \* 100% Pass Rate

Our guarantee that you will pass the exam.

### \* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

#### 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](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)

Which option is part of the content inspection process?

- A. Packet forwarding process
- B. SSL Proxy re-encrypt
- C. IPsec tunnel encryption
- D. Packet egress process

**Answer: B**

#### Explanation:

<http://live.paloaltonetworks.com/t5/image/serverpage/image-id/12862i950F549C7D4E6309>

#### NEW QUESTION 3

- (Exam Topic 2)

An administrator has left a firewall to use the default port for all management services. Which three functions are performed by the dataplane? (Choose three.)

- A. WildFire updates
- B. NAT
- C. NTP
- D. antivirus
- E. File blocking

**Answer: BDE**

#### NEW QUESTION 4

- (Exam Topic 2)

In which two types of deployment is active/active HA configuration supported? (Choose two.)

- A. TAP mode
- B. Layer 2 mode
- C. Virtual Wire mode
- D. Layer 3 mode

**Answer: CD**

#### NEW QUESTION 5

- (Exam Topic 2)

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

- A. Pattern based application identification
- B. Application override policy match
- C. Application changed from content inspection
- D. Session application identified.

**Answer: AB**

#### Explanation:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIVHCA0> <http://live.paloaltonetworks.com/t5/image/serverpage/image-id/12862i950F549C7D4E6309>

#### NEW QUESTION 6

- (Exam Topic 2)

Which version of GlobalProtect supports split tunneling based on destination domain, client process, and HTTP/HTTPS video streaming application?

- A. GlobalProtect version 4.0 with PAN-OS 8.1
- B. GlobalProtect version 4.1 with PAN-OS 8.1
- C. GlobalProtect version 4.1 with PAN-OS 8.0

D. GlobalProtect version 4.0 with PAN-OS 8.0

**Answer:** B

#### NEW QUESTION 7

- (Exam Topic 2)

Which method will dynamically register tags on the Palo Alto Networks NGFW?

- A. Restful API or the VMWare API on the firewall or on the User-ID agent or the read-only domain controller (RODC)
- B. Restful API or the VMware API on the firewall or on the User-ID agent
- C. XML-API or the VMware API on the firewall or on the User-ID agent or the CLI
- D. XML API or the VM Monitoring agent on the NGFW or on the User-ID agent

**Answer:** D

#### Explanation:

Reference:

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/policy/monitor-changes-in-the-virtual-environmen>

#### NEW QUESTION 8

- (Exam Topic 2)

An administrator has users accessing network resources through Citrix XenApp 7 x. Which User-ID mapping solution will map multiple users who are using Citrix to connect to the network and access resources?

- A. Client Probing
- B. Terminal Services agent
- C. GlobalProtect
- D. Syslog Monitoring

**Answer:** C

#### NEW QUESTION 9

- (Exam Topic 2)

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

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

**Answer:** C

#### NEW QUESTION 10

- (Exam Topic 2)

Which log file can be used to identify SSL decryption failures?

- A. Configuration
- B. Threats
- C. ACC
- D. Traffic

**Answer:** D

#### Explanation:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClboCAC>

#### NEW QUESTION 10

- (Exam Topic 2)

A customer wants to combine multiple Ethernet interfaces into a single virtual interface using link aggregation. Which two formats are correct for naming aggregate interfaces? (Choose two.)

- A. ae.8
- B. aggregate.1
- C. ae.1
- D. aggregate.8

**Answer:** AC

#### NEW QUESTION 12

- (Exam Topic 2)

An administrator needs to upgrade a Palo Alto Networks NGFW to the most current version of PAN-OS® software. The firewall has internet connectivity through an Ethernet interface, but no internet connectivity from the management interface. The Security policy has the default security rules and a rule that allows all web-browsing traffic from any to any zone. What must the administrator configure so that the PAN-OS® software can be upgraded?

- A. Security policy rule
- B. CRL

- C. Service route
- D. Scheduler

**Answer:** A

#### NEW QUESTION 14

- (Exam Topic 2)

A global corporate office has a large-scale network with only one User-ID agent, which creates a bottleneck near the User-ID agent server. Which solution in PAN-OS® software would help in this case?

- A. application override
- B. Virtual Wire mode
- C. content inspection
- D. redistribution of user mappings

**Answer:** D

#### Explanation:

Reference:

<https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/user-id/deploy-user-id-in-a-large-scale-net>

#### NEW QUESTION 18

- (Exam Topic 2)

How can a candidate or running configuration be copied to a host external from Panorama?

- A. Commit a running configuration.
- B. Save a configuration snapshot.
- C. Save a candidate configuration.
- D. Export a named configuration snapshot.

**Answer:** D

#### Explanation:

Reference:

[https://www.paloaltonetworks.com/documentation/71/panorama/panorama\\_adminguide/administer-panorama/ba-panorama-and-firewall-configurations](https://www.paloaltonetworks.com/documentation/71/panorama/panorama_adminguide/administer-panorama/ba-panorama-and-firewall-configurations)

#### NEW QUESTION 20

- (Exam Topic 2)

To connect the Palo Alto Networks firewall to AutoFocus, which setting must be enabled?

- A. Device>Setup>Services>AutoFocus
- B. Device> Setup>Management >AutoFocus
- C. AutoFocus is enabled by default on the Palo Alto Networks NGFW
- D. Device>Setup>WildFire>AutoFocus
- E. Device>Setup> Management> Logging and Reporting Settings

**Answer:** B

#### Explanation:

Reference:

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

#### NEW QUESTION 25

- (Exam Topic 2)

Refer to the exhibit.

Which will be the egress interface if the traffic's ingress interface is ethernet 1/7 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

#### NEW QUESTION 29

- (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. Replay
- C. Web Application
- D. DoS Protection

**Answer:** B

**Explanation:**

<https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/vpns/set-up-site-to-site-vpn/set-up-an-ipsec-tunnel#>

**NEW QUESTION 31**

- (Exam Topic 2)

Which is not a valid reason for receiving a decrypt-cert-validation error?

- A. Unsupported HSM
- B. Unknown certificate status
- C. Client authentication
- D. Untrusted issuer

**Answer:** A

**NEW QUESTION 32**

- (Exam Topic 2)

Starling with PAN-OS version 9.1, GlobalProtect logging information is now recorded in which firewall log?

- A. Configuration
- B. GlobalProtect
- C. Authentication
- D. System

**Answer:** C

**NEW QUESTION 34**

- (Exam Topic 2)

Which feature can provide NGFWs with User-ID mapping information?

- A. Web Captcha
- B. Native 802.1q authentication
- C. GlobalProtect
- D. Native 802.1x authentication

**Answer:** C

**NEW QUESTION 36**

- (Exam Topic 2)

Which two features does PAN-OS® software use to identify applications? (Choose two)

- A. port number
- B. session number
- C. transaction characteristics
- D. application layer payload

**Answer:** AD

**Explanation:**

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/app-id/application-level-gateways#>

**NEW QUESTION 40**

- (Exam Topic 2)

An administrator has enabled OSPF on a virtual router on the NGFW. OSPF is not adding new routes to the virtual router. Which two options enable the administrator to troubleshoot this issue? (Choose two.)

- A. View Runtime Stats in the virtual router.
- B. View System logs.
- C. Add a redistribution profile to forward as BGP updates.
- D. Perform a traffic pcap at the routing stage.

**Answer:** AB

**Explanation:**

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIdcCAC>

**NEW QUESTION 41**

- (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. Exhibit A
- B. Exhibit B
- C. Exhibit C
- D. Exhibit D

**Answer:** AD

#### NEW QUESTION 42

- (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 44

- (Exam Topic 2)

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.txt 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 9.1.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:** C

#### NEW QUESTION 49

- (Exam Topic 2)

Which option would an administrator choose to define the certificate and protocol that Panorama and its managed devices use for SSL/TLS services?

- A. Configure a Decryption Profile and select SSL/TLS services.
- B. Set up SSL/TLS under Policies > Service/URL Category > Service.
- C. Set up Security policy rule to allow SSL communication.
- D. Configure an SSL/TLS Profile.

**Answer:** D

#### Explanation:

Reference:

<https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/device/device-certificate-management/ssl-tls-service-profile>

#### NEW QUESTION 50

- (Exam Topic 2)

The firewall is not downloading IP addresses from MineMeld. Based on the image, what most likely is wrong?



- A. A Certificate Profile that contains the client certificate needs to be selected.
- B. The source address supports only files hosted with an ftp://<address/file>.
- C. External Dynamic Lists do not support SSL connections.
- D. A Certificate Profile that contains the CA certificate needs to be selected.

**Answer:** D

#### NEW QUESTION 51

- (Exam Topic 2)

Which three authentication factors does PAN-OS® software support for MFA (Choose three.)

- A. Push
- B. Pull
- C. Okta Adaptive
- D. Voice
- E. SMS

**Answer:** ADE

#### Explanation:

Reference:

<https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/authentication/configure-multi-factor-authentication>

#### NEW QUESTION 53

- (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 58

- (Exam Topic 2)

A company wants to install a PA-3060 firewall between two core switches on a VLAN trunk link. They need to assign each VLAN to its own zone and to assign untagged (native) traffic to its own zone which options differentiates multiple VLAN into separate zones?

- A. Create V-Wire objects with two V-Wire interfaces and define a range of "0-4096 in the "Tag Allowed" field of the V-Wire object.
- B. Create V-Wire objects with two V-Wire subinterfaces and assign only a single VLAN ID to the Tag Allowed" field of the V-Wire object
- C. Repeat for every additional VLAN and use a VLAN ID of 0 for untagged traffic
- D. Assign each interface/sub interface to a unique zone.
- E. Create Layer 3 subinterfaces that are each assigned to
- F. single VLAN ID and a common virtual router. The physical Layer 3 interface would handle untagged traffic
- G. Assign each interface/subinterface to
- H. unique zone
- I. Do not assign any interface an IP address.
- J. Create VLAN objects for each VLAN and assign VLAN interfaces matching each VLAN ID
- K. Repeat for every additional VLAN and use a VLAN ID of 0 for untagged traffic
- L. Assign each interface/sub interface to a unique zone.

**Answer:** B

#### Explanation:

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/networking/configure-interfaces/virtual-wire-interfaces> Virtual wire interfaces by default allow all untagged traffic. You can, however, use a virtual wire to connect two interfaces and configure either interface to block or allow traffic based on the virtual LAN (VLAN) tags. VLAN tag 0 indicates untagged traffic. You can also create multiple subinterfaces, add them into different zones, and then classify traffic according to a VLAN tag or a combination of a VLAN tag with IP classifiers (address, range, or subnet) to apply granular policy control for specific VLAN tags or for VLAN tags from a specific source IP address, range, or subnet.

#### NEW QUESTION 61

- (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 66

- (Exam Topic 2)

Which two are valid ACC GlobalProtect Activity tab widgets? (Choose two)



- A. Successful GlobalProtect Connection Activity
- B. Successful GlobalProtect Deployed Activity
- C. GlobalProtect Quarantine Activity
- D. GlobalProtect Deployment Activity

**Answer:** AC

#### NEW QUESTION 69

- (Exam Topic 2)

Which three options are supported in HA Lite? (Choose three.)

- A. Virtual link
- B. Active/passive deployment
- C. Synchronization of IPsec security associations
- D. Configuration synchronization
- E. Session synchronization

**Answer:** BCD

#### Explanation:

“The PA-200 firewall supports HA Lite only. HA Lite is an active/passive deployment that provides configuration synchronization and some runtime data synchronization such as IPSec security associations. It does not support any session synchronization (HA2), and therefore does not offer stateful failover.”

Reference:

<https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/device/device-high-availability>

#### NEW QUESTION 74

- (Exam Topic 2)

An administrator needs to implement an NGFW between their DMZ and Core network. EIGRP Routing between the two environments is required. Which interface type would support this business requirement?

- A. Virtual Wire interfaces to permit EIGRP routing to remain between the Core and DMZ
- B. Layer 3 or Aggregate Ethernet interfaces, but configuring EIGRP on subinterfaces only
- C. Tunnel interfaces to terminate EIGRP routing on an IPsec tunnel (with the GlobalProtect License to support LSVPN and EIGRP protocols)
- D. Layer 3 interfaces, but configuring EIGRP on the attached virtual router

**Answer:** A

#### NEW QUESTION 78

- (Exam Topic 2)

The firewall determines if a packet is the first packet of a new session or if a packet is part of an existing session using which kind of match?

- A. 6-tuple match:Source IP Address, Destination IP Address, Source port, Destination Port, Protocol, and Source Security Zone
- B. 5-tuple match:Source IP Address, Destination IP Address, Source port, Destination Port, Protocol
- C. 7-tuple match:Source IP Address, Destination IP Address, Source port, Destination Port, Source User, URL Category, and Source Security Zone
- D. 9-tuple match:Source IP Address, Destination IP Address, Source port, Destination Port, Source User, Source Security Zone, Destination Security Zone, Application, and URL Category

**Answer:** A

#### Explanation:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIVECA0>

#### NEW QUESTION 82

- (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 84

- (Exam Topic 2)

Which three user authentication services can be modified to provide the Palo Alto Networks NGFW with both usernames and role names? (Choose three.)

- A. TACACS+
- B. Kerberos
- C. PAP
- D. LDAP
- E. SAML
- F. RADIUS

**Answer:** BDE

**Explanation:**

<https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/firewall-administration/manage-firewall-administra>

#### NEW QUESTION 88

- (Exam Topic 2)

A session in the Traffic log is reporting the application as “incomplete.” What does “incomplete” mean?

- A. The three-way TCP handshake was observed, but the application could not be identified.
- B. The three-way TCP handshake did not complete.
- C. The traffic is coming across UDP, and the application could not be identified.
- D. Data was received but was instantly discarded because of a Deny policy was applied before App-ID could be applied.

**Answer:** B

**Explanation:**

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClibCAC>

#### NEW QUESTION 91

- (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 94

- (Exam Topic 2)

Updates to dynamic user group membership are automatic therefore using dynamic user groups instead of static group objects allows you to:

- A. respond to changes in user behavior or potential threats using manual policy changes
- B. respond to changes in user behavior or potential threats without automatic policy changes
- C. respond to changes in user behavior and confirmed threats with manual policy changes
- D. respond to changes in user behavior or potential threats without manual policy changes

**Answer:** D

**Explanation:**

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/user-id-features/dynamic-user-groups#:~:tex>

#### NEW QUESTION 98

- (Exam Topic 2)

ESTION NO: 94

If an administrator wants to decrypt SMTP traffic and possesses the server's certificate, which SSL decryption mode will allow the Palo Alto Networks NGFW to inspect traffic to the server?

- A. TLS Bidirectional Inspection
- B. SSL Inbound Inspection
- C. SSH Forward Proxy
- D. SMTP Inbound Decryption

**Answer:** B

**Explanation:**

Reference:

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

#### NEW QUESTION 99

- (Exam Topic 2)

Which virtual router feature determines if a specific destination IP address is reachable?

- A. Heartbeat Monitoring
- B. Failover
- C. Path Monitoring
- D. Ping-Path

**Answer:** C

**Explanation:**

Reference: <https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/policy/pbf>

#### NEW QUESTION 101

- (Exam Topic 2)

An administrator has a requirement to export decrypted traffic from the Palo Alto Networks NGFW to a third-party, deep-level packet inspection appliance. Which interface type and license feature are necessary to meet the requirement?

- A. Decryption Mirror interface with the Threat Analysis license
- B. Virtual Wire interface with the Decryption Port Export license
- C. Tap interface with the Decryption Port Mirror license
- D. Decryption Mirror interface with the associated Decryption Port Mirror license

**Answer: D**

#### Explanation:

Reference:

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

“Before you can enable Decryption Mirroring, you must obtain and install a Decryption Port Mirror license. The license is free of charge and can be activated through the support portal as described in the following procedure. After you install the Decryption Port Mirror license and reboot the firewall, you can enable decryption port mirroring. “

#### NEW QUESTION 106

- (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 107

- (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 112

- (Exam Topic 2)

Which Zone Pair and Rule Type will allow a successful connection for a user on the internet zone to a web server hosted in the DMZ zone? The web server is reachable using a destination Nat policy in the Palo Alto Networks firewall.

- A. Zone Pair:Source Zone: Internet Destination Zone: DMZ Rule Type:“intrazone”
- B. Zone Pair:Source Zone: Internet Destination Zone: DMZ Rule Type:“intrazone” or “universal”
- C. Zone Pair:Source Zone: Internet Destination Zone: Internet Rule Type:“intrazone” or “universal”
- D. Zone Pair:Source Zone: Internet Destination Zone: Internet Rule Type:“intrazone”

**Answer: B**

#### Explanation:

<https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/zone-protection-and-dos-protection/zone-defense/z>

<https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/networking/nat/nat-configuration-examples/destinat>

#### NEW QUESTION 116

- (Exam Topic 2)

Which processing order will be enabled when a Panorama administrator selects the setting “Objects defined in ancestors will take higher precedence?”

- A. Descendant objects will take precedence over other descendant objects.
- B. Descendant objects will take precedence over ancestor objects.
- C. Ancestor objects will have precedence over descendant objects.
- D. Ancestor objects will have precedence over other ancestor objects.

**Answer: C**

#### Explanation:

Reference:

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

#### NEW QUESTION 120

- (Exam Topic 2)

An administrator needs to upgrade an NGFW to the most current version of PAN-OS® software. The following is occurring:

- Firewall has Internet connectivity through e1/1.
- Default security rules and security rules allowing all SSL and web-browsing traffic to and from any zone.
- Service route is configured, sourcing update traffic from e1/1.
- A communication error appears in the System logs when updates are performed.
- Download does not complete.

What must be configured to enable the firewall to download the current version of PAN-OS software?

- A. DNS settings for the firewall to use for resolution
- B. scheduler for timed downloads of PAN-OS software
- C. static route pointing application PaloAlto-updates to the update servers
- D. Security policy rule allowing PaloAlto-updates as the application

**Answer:** D

#### NEW QUESTION 122

- (Exam Topic 2)

Which feature prevents the submission of corporate login information into website forms?

- A. Data filtering
- B. User-ID
- C. File blocking
- D. Credential phishing prevention

**Answer:** D

#### Explanation:

Reference:

<https://www.paloaltonetworks.com/cyberpedia/how-the-next-generation-security-platform-contributes-to-gdpr-c>

“Credential phishing prevention works by scanning username and password submissions to websites and comparing those submissions against valid corporate credentials. You can choose what websites you want to either allow, alert on, or block corporate credential submissions to based on the URL category of the website. Alternatively, you can present a page that warns users against submitting credentials to sites classified in certain URL categories. This gives you the opportunity to educate users against reusing corporate credentials, even on legitimate, non-phishing sites. In the event that corporate credentials are compromised, this feature allows you to identify the user who submitted credentials so that you can remediate.”

#### NEW QUESTION 125

- (Exam Topic 2)

Which CLI command is used to simulate traffic going through the firewall and determine which Security policy rule, NAT translation, static route, or PBF rule will be triggered by the traffic?

- A. check
- B. find
- C. test
- D. sim

**Answer:** C

#### Explanation:

Reference: <http://www.shanekillen.com/2014/02/palo-alto-useful-cli-commands.html>

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIQSCA0>

#### NEW QUESTION 130

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

#### NEW QUESTION 134

- (Exam Topic 2)

Which three file types can be forwarded to WildFire for analysis as a part of the basic WildFire service? (Choose three.)

- A. .dll
- B. .exe

- C. .src
- D. .apk
- E. .pdf
- F. .jar

**Answer:** DEF

**Explanation:**

<https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-admin/getting-started/enable-basic-wildfire-forwarding>

**NEW QUESTION 135**

- (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-phishi>

**NEW QUESTION 138**

- (Exam Topic 2)

Based on the following image,

what is the correct path of root, intermediate, and end-user certificate?

- A. Palo Alto Networks > Symantec > VeriSign
- B. Symantec > VeriSign > Palo Alto Networks
- C. VeriSign > Palo Alto Networks > Symantec
- D. VeriSign > Symantec > Palo Alto Networks

**Answer:** B

**NEW QUESTION 141**

- (Exam Topic 2)

An administrator has created an SSL Decryption policy rule that decrypts SSL sessions on any port. Which log entry can the administrator use to verify that sessions are being decrypted?

- A. In the details of the Traffic log entries
- B. Decryption log
- C. Data Filtering log
- D. In the details of the Threat log entries

**Answer:** A

**Explanation:**

Reference:

<https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Implement-and-Test-SSL-Decryption/ta-p/5>

**NEW QUESTION 144**

- (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-widg>

**NEW QUESTION 149**

- (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 154**

- (Exam Topic 2)

Which administrative authentication method supports authorization by an external service?

- A. Certificates
- B. LDAP
- C. RADIUS
- D. SSH keys

**Answer:** C

**NEW QUESTION 157**

- (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 158**

- (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 162**

- (Exam Topic 2)

Which three settings are defined within the Templates object of Panorama? (Choose three.)

- A. Setup
- B. Virtual Routers
- C. Interfaces
- D. Security
- E. Application Override

**Answer:** ABC

**NEW QUESTION 167**

- (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 168**

- (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-and-Tricks-How-to-Create-an-Application>

**NEW QUESTION 170**

- (Exam Topic 2)

An administrator needs to determine why users on the trust zone cannot reach certain websites. The only information available is shown on the following image. Which configuration change should the administrator make?

A)

B)

C)

D)

E)

A. Option A

B. Option B

C. Option C

D. Option D

E. Option E

**Answer: B**

**NEW QUESTION 172**

- (Exam Topic 2)

Decrypted packets from the website <https://www.microsoft.com> will appear as which application and service within the Traffic log?

A. web-browsing and 443

B. SSL and 80

C. SSL and 443

D. web-browsing and 80

**Answer: A**

**Explanation:**

We know that SSL decryption is supposed to give us visibility of traffic that would otherwise be encrypted. Therefore, we'd expect decrypted traffic to be identified as the underlying applications, such as web-browsing, facebook-base or other, but not as SSL.

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CmdLCAS>

**NEW QUESTION 173**

- (Exam Topic 2)

Which User-ID method maps IP address to usernames for users connecting through a web proxy that has already authenticated the user?

A. Client Probing

B. Port mapping

C. Server monitoring

D. Syslog listening

**Answer: D**

**Explanation:**

To obtain user mappings from existing network services that authenticate users—such as wireless controllers, 802.1x devices, Apple Open Directory servers, proxy servers, or other Network Access Control (NAC) mechanisms—Configure User-ID to Monitor Syslog Senders for User Mapping. While you can configure either the Windows agent or the PAN-OS integrated User-ID agent on the firewall to listen for authentication syslog messages from the network services, because only the PAN-OS integrated agent supports syslog listening over TLS, it is the preferred configuration.

**NEW QUESTION 176**

- (Exam Topic 2)

Which feature can provide NGFWs with User-ID mapping information?



- A. GlobalProtect
- B. Web Captcha
- C. Native 802.1q authentication
- D. Native 802.1x authentication

**Answer:** A

#### NEW QUESTION 178

- (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 181

- (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 183

- (Exam Topic 2)

In High Availability, which information is transferred via the HA data link?

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

**Answer:** A

#### Explanation:

Reference:

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

#### NEW QUESTION 185

- (Exam Topic 2)

Exhibit:

What will be the egress interface if the traffic's ingress interface is ethernet1/6 sourcing from 192.168.111.3 and to the destination 10.46.41.113 during the time shown in the image?

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

**Answer:** D

#### NEW QUESTION 186

- (Exam Topic 2)

An administrator using an enterprise PKI needs to establish a unique chain of trust to ensure mutual authentication between Panorama and the managed firewalls and Log Collectors.

How would the administrator establish the chain of trust?

- A. Use custom certificates
- B. Enable LDAP or RADIUS integration
- C. Set up multi-factor authentication
- D. Configure strong password authentication

**Answer:** A

#### Explanation:

Reference:

[https://www.paloaltonetworks.com/documentation/80/panorama/panorama\\_adminguide/panorama-overview/pla-panorama-deployment](https://www.paloaltonetworks.com/documentation/80/panorama/panorama_adminguide/panorama-overview/pla-panorama-deployment)

#### NEW QUESTION 190

- (Exam Topic 2)

Which logs enable a firewall administrator to determine whether a session was decrypted?

- A. Correlated Event
- B. Traffic
- C. Decryption
- D. Security Policy

**Answer:** B

#### NEW QUESTION 195

- (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 198

- (Exam Topic 1)

An administrator wants to enable zone protection. Before doing so, what must the administrator consider?

- A. Activate a zone protection subscription.
- B. To increase bandwidth no more than one firewall interface should be connected to a zone
- C. Security policy rules do not prevent lateral movement of traffic between zones
- D. The zone protection profile will apply to all interfaces within that zone

**Answer:** A

#### NEW QUESTION 201

- (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 203

- (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 207

- (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 209

- (Exam Topic 1)

Which statement accurately describes service routes and virtual systems?

- A. Virtual systems can only use one interface for all global service and service routes of the firewall
- B. The interface must be used for traffic to the required external services
- 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 cannot have dedicated service routes configured: and virtual systems always use the global service and service route settings for the firewall

**Answer:** A

#### NEW QUESTION 210

- (Exam Topic 1)

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

- A. Ye
- B. because the action is set to "allow "
- C. No because WildFire categorized a file with the verdict "malicious"
- D. Yes because the action is set to "alert"
- E. No because WildFire classified the seventy as "high."

**Answer:** B

#### NEW QUESTION 215

- (Exam Topic 1)

PBF can address which two scenarios? (Select Two)

- A. forwarding all traffic by using source port 78249 to a specific egress interface
- B. providing application connectivity the primary circuit fails
- C. enabling the firewall to bypass Layer 7 inspection
- D. routing FTP to a backup ISP link to save bandwidth on the primary ISP link

**Answer:** AC

#### NEW QUESTION 218

- (Exam Topic 1)

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

**Answer:** A

#### NEW QUESTION 222

- (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 225

- (Exam Topic 1)

Match each type of DoS attack to an example of that type of attack

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Plan to defend your network against different types of DoS attacks:

Application-Based Attacks

—Target weaknesses in a particular application and try to exhaust its resources so legitimate users can't use it. An example of this is the Slowloris attack.

Protocol-Based Attacks

—Also known as state-exhaustion attacks, these attacks target protocol weaknesses. A common example is a SYN flood attack.

Volumetric Attacks

—High-volume attacks that attempt to overwhelm the available network resources, especially bandwidth, and bring down the target to prevent legitimate users from accessing those resources. An example of this is a UDP flood attack.

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/zone-protection-and-dos-protection/zone-defense.ht>

**NEW QUESTION 230**

- (Exam Topic 1)

When you configure a Layer 3 interface what is one mandatory step?

- A. Configure Security profiles, which need to be attached to each Layer 3 interface
- B. Configure Interface Management profiles which need to be attached to each Layer 3 interface
- C. Configure virtual routers to route the traffic for each Layer 3 interface
- D. Configure service routes to route the traffic for each Layer 3 interface

**Answer:** A

**NEW QUESTION 232**

- (Exam Topic 1)

When overriding a template configuration locally on a firewall, what should you consider?

- A. Only Panorama can revert the override
- B. Panorama will lose visibility into the overridden configuration
- C. Panorama will update the template with the overridden value
- D. The firewall template will show that it is out of sync within Panorama

**Answer:** B

**NEW QUESTION 236**

- (Exam Topic 1)

An internal system is not functioning The firewall administrator has determined that the incorrect egress interface is being used After looking at the configuration, the administrator believes that the firewall is not using a static route

What are two reasons why the firewall might not use a static route"? (Choose two.)

- A. no install on the route
- B. duplicate static route
- C. path monitoring on the static route
- D. disabling of the static route

**Answer:** C

**NEW QUESTION 240**

- (Exam Topic 1)

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. LDAP Server Profile configuration
- C. GlobalProtect
- D. Windows-based User-ID agent

**Answer:** A

**NEW QUESTION 244**

- (Exam Topic 1)

A firewall should be advertising the static route 10.2.0.0/24 into OSPF The configuration on the neighbor is correct but the route is not in the neighbor's routing table Which two configurations should you check on the firewall? (Choose two )

- A. Within the redistribution profile ensure that Redist is selected
- B. In the redistribution profile check that the source type is set to "ospf"
- C. In the OSFP configuration ensure that the correct redistribution profile is selected in the OSPF Export Rules section
- D. Ensure that the OSPF neighbor state is "2-Way"

**Answer:** AC

**NEW QUESTION 249**

- (Exam Topic 1)

What does SSL decryption require to establish a firewall as a trusted third party and to establish trust between a client and server to secure an SSL/TLS connection?

- A. link state
- B. stateful firewall connection
- C. certificates
- D. profiles

**Answer:** C

**Explanation:**

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/decryption/decryption-overview.html#:~:text=SSL>

**NEW QUESTION 250**

- (Exam Topic 1)

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

**NEW QUESTION 255**

- (Exam Topic 1)

Which two statements correctly identify the number of Decryption Broker security chains that are supported on a pair of decryption-forwarding interfaces'? (Choose two)

- A. A single transparent bridge security chain is supported per pair of interfaces
- B. L3 security chains support up to 32 security chains
- C. L3 security chains support up to 64 security chains
- D. A single transparent bridge security chain is supported per firewall

**Answer:** AD

**NEW QUESTION 258**

- (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 262**

- (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 263**

- (Exam Topic 1)

An engineer is planning an SSL decryption implementation

Which of the following statements is a best practice for SSL decryption?

- A. Obtain an enterprise CA-signed certificate for the Forward Trust certificate
- B. Obtain a certificate from a publicly trusted root CA for the Forward Trust certificate
- C. Use an enterprise CA-signed certificate for the Forward Untrust certificate
- D. Use the same Forward Trust certificate on all firewalls in the network

**Answer:** D

#### NEW QUESTION 264

- (Exam Topic 1)

As a best practice, which URL category should you target first for SSL decryption\*?

- A. Online Storage and Backup
- B. High Risk
- C. Health and Medicine
- D. Financial Services

**Answer:** A

#### NEW QUESTION 266

- (Exam Topic 1)

An administrator plans to deploy 15 firewalls to act as GlobalProtect gateways around the world Panorama will manage the firewalls

The firewalls will provide access to mobile users and act as edge locations to on-premises infrastructure The administrator wants to scale the configuration out quickly and wants all of the firewalls to use the same template configuration

Which two solutions can the administrator use to scale this configuration? (Choose two.)

- A. variables
- B. template stacks
- C. collector groups
- D. virtual systems

**Answer:** C

#### NEW QUESTION 271

- (Exam Topic 1)

Which rule type controls end user SSL traffic to external websites?

- A. SSL Outbound Proxyless Inspection
- B. SSL Forward Proxy
- C. SSL Inbound Inspection
- D. SSH Proxy

**Answer:** C

#### NEW QUESTION 276

- (Exam Topic 1)

An administrator is considering upgrading the Palo Alto Networks NGFW and central management Panorama version

What is considered best practice for this scenario?

- A. Perform the Panorama and firewall upgrades simultaneously
- B. Upgrade the firewall first wait at least 24 hours and then upgrade the Panorama version
- C. Upgrade Panorama to a version at or above the target firewall version
- D. Export the device state perform the update, and then import the device state

**Answer:** A

#### NEW QUESTION 280

- (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 283

- (Exam Topic 1)

Which value in the Application column indicates UDP traffic that did not match an App-ID signature?

- A. not-applicable
- B. incomplete
- C. unknown-ip
- D. unknown-udp

**Answer:** D

#### Explanation:

To safely enable applications you must classify all traffic, across all ports, all the time. With App-ID, the only applications that are typically classified as unknown traffic—tcp, udp or non-syn-tcp—in the ACC and the Traffic logs are commercially available applications that have not yet been added to App-ID, internal or custom applications on your network, or potential threats.

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/app-id/use-application-objects-in-policy/create-a-cu>



#### NEW QUESTION 284

- (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 287

- (Exam Topic 1)

Which three statements accurately describe Decryption Mirror? (Choose three.)

- A. Decryption Mirror requires a tap interface on the firewall
- B. Decryption, storage, inspection, and use of SSL traffic are regulated in certain countries
- C. Only management consent is required to use the Decryption Mirror feature
- D. You should consult with your corporate counsel before activating and using Decryption Mirror in a production environment
- E. Use of Decryption Mirror might enable malicious users with administrative access to the firewall to harvest sensitive information that is submitted via an encrypted channel

**Answer:** ABC

#### NEW QUESTION 290

- (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 295

- (Exam Topic 2)

What file type upload is supported as part of the basic WildFire service?

- A. PE
- B. BAT
- C. VBS
- D. ELF

**Answer:** A

#### NEW QUESTION 300

- (Exam Topic 2)

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 information shown in the image, which NAT rule will forward web-browsing traffic correctly? A)

B)

C)

D)

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

**Answer:** C

#### NEW QUESTION 301

- (Exam Topic 2)

For which two reasons would a firewall discard a packet as part of the packet flow sequence? (Choose two )

- A. equal-cost multipath
- B. ingress processing errors
- C. rule match with action "allow"
- D. rule match with action "deny"

**Answer:** BD

#### NEW QUESTION 304

- (Exam Topic 2)

View the GlobalProtect configuration screen capture.

What is the purpose of this configuration?

- A. It configures the tunnel address of all internal clients to an IP address range starting at 192.168.10.1.
- B. It forces an internal client to connect to an internal gateway at IP address 192.168.10.1.
- C. It enables a client to perform a reverse DNS lookup on 192.168.10.1 to detect that it is an internal client.
- D. It forces the firewall to perform a dynamic DNS update, which adds the internal gateway's hostname and IP address to the DNS server.

**Answer:** C

#### Explanation:

Reference:

<https://www.paloaltonetworks.com/documentation/80/globalprotect/globalprotect-admin-guide/globalprotect-po-the-globalprotect-client-authentication-configurations/define-the-globalprotect-agent-configurations>

“Select this option to allow the GlobalProtect agent to determine if it is inside the enterprise network. This option applies only to endpoints that are configured to communicate with internal gateways. When the user attempts to log in, the agent does a reverse DNS lookup of an internal host using the specified Hostname to the specified IP Address. The host serves as a reference point that is reachable if the endpoint is inside the enterprise network. If the agent finds the host, the endpoint is inside the network and the agent connects to an internal gateway; if the agent fails to find the internal host, the endpoint is outside the network and the agent establishes a tunnel to one of the external gateways”

#### NEW QUESTION 308

- (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 310

- (Exam Topic 2)

An administrator encountered problems with inbound decryption. Which option should the administrator investigate as part of triage?

- A. Security policy rule allowing SSL to the target server
- B. Firewall connectivity to a CRL
- C. Root certificate imported into the firewall with “Trust” enabled
- D. Importation of a certificate from an HSM

**Answer:** A

#### Explanation:

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/decryption/configure-ssl-inbound-inspection.html>

#### NEW QUESTION 311

- (Exam Topic 2)

To protect your firewall and network from single source denial of service (DoS) attacks that can overwhelm its packet buffer and cause legitimate traffic to drop, you can configure.

- A. BGP (Border Gateway Protocol)
- B. PBP (Packet Buffer Protection)

- C. PGP (Packet Gateway Protocol)
- D. PBP (Protocol Based Protection)

**Answer:** D

#### NEW QUESTION 315

- (Exam Topic 2)

How does an administrator schedule an Applications and Threats dynamic update while delaying installation of the update for a certain amount of time?

- A. Configure the option for “Threshold”.
- B. Disable automatic updates during weekdays.
- C. Automatically “download only” and then install Applications and Threats later, after the administrator approves the update.
- D. Automatically “download and install” but with the “disable new applications” option used.

**Answer:** A

#### Explanation:

For Antivirus and Applications and Threats updates, you have the option to set a minimum Threshold of time that a content update must be available before the firewall installs it. Very rarely, there can be an error in a content update and this threshold ensures that the firewall only downloads content releases that have been available and functioning in customer environments for the specified amount of time. <https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/device/device-dynamic-updates>

#### NEW QUESTION 320

- (Exam Topic 2)

An administrator has been asked to configure a Palo Alto Networks NGFW to provide protection against external hosts attempting to exploit a flaw in an operating system on an internal system.

Which Security Profile type will prevent this attack?

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

**Answer:** A

#### Explanation:

Reference:

<https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/objects/objects-security-profile-vulnerability-protection>

#### NEW QUESTION 324

- (Exam Topic 2)

How can an administrator configure the NGFW to automatically quarantine a device using GlobalProtect?

- A. by adding the device's Host ID to a quarantine list and configure GlobalProtect to prevent users from connecting to the GlobalProtect gateway from a quarantined device
- B. by using security policies, log forwarding profiles, and log settings.
- C. by exporting the list of quarantined devices to a pdf or csv file by selecting PDF/CSV at the bottom of the Device Quarantine page and leveraging the appropriate XSOAR playbook
- D. There is no native auto-quarantine feature so a custom script would need to be leveraged.

**Answer:** A

#### NEW QUESTION 328

- (Exam Topic 2)

An administrator wants to upgrade an NGFW from PAN-OS® 9.0 to PAN-OS® 10.0. The firewall is not a part of an HA pair. What needs to be updated first?

- A. XML Agent
- B. Applications and Threats
- C. WildFire
- D. PAN-OS® Upgrade Agent

**Answer:** B

#### Explanation:

<https://www.paloaltonetworks.com/documentation/80/pan-os/newfeaturesguide/upgrade-to-pan-os-80/upgrade-t>

#### NEW QUESTION 333

- (Exam Topic 2)

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

- A. Reuse of the existing Security policy rules and objects
- B. Requires configuring both function and location for every device
- C. All device groups inherit settings from the Shared group
- D. Overwrites local firewall configuration

**Answer:** AC

**Explanation:**

Creation of a device group hierarchy enables you to organize firewalls based on common policy requirements without redundant configuration. When you create objects for use in shared or device group policy once and use them many times, you reduce administrative overhead and ensure consistency across firewall policies.

**NEW QUESTION 336**

- (Exam Topic 2)

Which Security policy rule will allow an admin to block facebook chat but allow Facebook in general?

- A. Deny application facebook-chat before allowing application facebook
- B. Deny application facebook on top
- C. Allow application facebook on top
- D. Allow application facebook before denying application facebook-chat

**Answer:** A

**Explanation:**

Reference:

<https://live.paloaltonetworks.com/t5/Configuration-Articles/Failed-to-Block-Facebook-Chat-Consistently/ta-p/1>

**NEW QUESTION 340**

- (Exam Topic 3)

Which three fields can be included in a pcap filter? (Choose three)

- A. Egress interface
- B. Source IP
- C. Rule number
- D. Destination IP
- E. Ingress interface

**Answer:** BCD

**Explanation:**

(<https://live.paloaltonetworks.com/t5/Featured-Articles/Getting-Started-Packet-Capture/ta-p/72069>)

**NEW QUESTION 342**

- (Exam Topic 3)

A network security engineer is asked to provide a report on bandwidth usage. Which tab in the ACC provides the information needed to create the report?

- A. Blocked Activity
- B. Bandwidth Activity
- C. Threat Activity
- D. Network Activity

**Answer:** D

**NEW QUESTION 345**

- (Exam Topic 3)

Which two methods can be used to mitigate resource exhaustion of an application server? (Choose two)

- A. Vulnerability Object
- B. DoS Protection Profile
- C. Data Filtering Profile
- D. Zone Protection Profile

**Answer:** BD

**NEW QUESTION 349**

- (Exam Topic 3)

A network security engineer has been asked to analyze Wildfire activity. However, the Wildfire Submissions item is not visible from the Monitor tab. What could cause this condition?

- A. The firewall does not have an active WildFire subscription.
- B. The engineer's account does not have permission to view WildFire Submissions.
- C. A policy is blocking WildFire Submission traffic.
- D. Though WildFire is working, there are currently no WildFire Submissions log entries.

**Answer:** B

**NEW QUESTION 354**

- (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 356**

- (Exam Topic 3)

Site-A and Site-B need to use IKEv2 to establish a VPN connection. Site A connects directly to the internet using a public IP address. Site-B uses a private IP address behind an ISP router to connect to the internet.

How should NAT Traversal be implemented for the VPN connection to be established between Site-A and Site-B?

- A. Enable on Site-A only
- B. Enable on Site-B only
- C. Enable on Site-B only with passive mode
- D. Enable on Site-A and Site-B

**Answer:** D

**NEW QUESTION 358**

- (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 359**

- (Exam Topic 3)

Support for which authentication method was added in PAN-OS 8.0?

- A. RADIUS
- B. LDAP
- C. Diameter
- D. TACACS+

**Answer:** D

**Explanation:**

<https://www.paloaltonetworks.com/resources/datasheets/whats-new-in-pan-os-7-1>

**NEW QUESTION 360**

- (Exam Topic 3)

Which three options does the WF-500 appliance support for local analysis? (Choose three)

- A. E-mail links
- B. APK files
- C. jar files
- D. PNG files
- E. Portable Executable (PE) files

**Answer:** ACE

**NEW QUESTION 362**

- (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 365**

- (Exam Topic 3)

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

- A. Certificate revocation list

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

**Answer:** C

#### NEW QUESTION 370

- (Exam Topic 3)

Which Palo Alto Networks VM-Series firewall is supported for VMware NSX?

- A. VM-100
- B. VM-200
- C. VM-1000-HV
- D. VM-300

**Answer:** C

#### NEW QUESTION 375

- (Exam Topic 3)

Which client software can be used to connect remote Linux client into a Palo Alto Networks Infrastructure without sacrificing the ability to scan traffic and protect against threats?

- A. X-Auth IPsec VPN
- B. GlobalProtect Apple IOS
- C. GlobalProtect SSL
- D. GlobalProtect Linux

**Answer:** A

#### Explanation:

( <http://blog.webernetz.net/2014/03/31/palo-alto-globalprotect-for-linux-with-vpnc/> )

#### NEW QUESTION 377

- (Exam Topic 3)

A firewall administrator has completed most of the steps required to provision a standalone Palo Alto Networks Next-Generation Firewall. As a final step, the administrator wants to test one of the security policies.

Which CLI command syntax will display the rule that matches the test?

- A. test security -policy- match source <ip\_address> destination <IP\_address> destination port <port number> protocol <protocol number>
- B. show security rule source <ip\_address> destination <IP\_address> destination port <port number> protocol <protocol number>
- C. test security rule source <ip\_address> destination <IP\_address> destination port <port number> protocol<protocol number>
- D. show security-policy-match source <ip\_address> destination <IP\_address> destination port <port number> protocol <protocol number>test security-policy-match source

**Answer:** A

#### Explanation:

test security-policy-match source <source IP> destination <destination IP> protocol <protocol number> <https://live.paloaltonetworks.com/t5/Management-Articles/How-to-Test-Which-Security-Policy-Applies-to-a-Tr>

#### NEW QUESTION 381

- (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 386

- (Exam Topic 3)

A firewall administrator has been asked to configure a Palo Alto Networks NGFW to prevent against compromised hosts trying to phone-home or beacon out to external command-and-control (C2) servers.

Which security Profile type will prevent these behaviors?

- A. WildFire
- B. Anti-Spyware
- C. Vulnerability Protection
- D. Antivirus

**Answer:** D

#### NEW QUESTION 389

- (Exam Topic 3)



Which CLI command displays the current management plane memory utilization?

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

**Answer:** D

**Explanation:**

<https://live.paloaltonetworks.com/t5/Learning-Articles/How-to-Interpret-show-system-resources/ta-p/59364> "The command show system resources gives a snapshot of Management Plane (MP) resource utilization including memory and CPU. This is similar to the 'top' command in Linux." <https://live.paloaltonetworks.com/t5/Learning-Articles/How-to-Interpret-show-system-resources/ta-p/59>

**NEW QUESTION 393**

- (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 398**

- (Exam Topic 3)

The GlobalProtect Portal interface and IP address have been configured. Which other value needs to be defined to complete the network settings configuration of GlobalProtect Portal?

- A. Server Certificate
- B. Client Certificate
- C. Authentication Profile
- D. Certificate Profile

**Answer:** A

**Explanation:**

(<https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Configure-GlobalProtect/ta-p/58351>)

**NEW QUESTION 401**

- (Exam Topic 3)

Only two Trust to Untrust allow rules have been created in the Security policy Rule1 allows google-base Rule2 allows youtube-base

The youtube-base App-ID depends on google-base to function. The google-base App-ID implicitly uses SSL and web-browsing. When user try to access <https://www.youtube.com> in a web browser, they get an error indicating that the server cannot be found.

Which action will allow youtube.com display in the browser correctly?

- A. Add SSL App-ID to Rule1
- B. Create an additional Trust to Untrust Rule, add the web-browsing, and SSL App-ID's to it
- C. Add the DNS App-ID to Rule2
- D. Add the Web-browsing App-ID to Rule2

**Answer:** C

**NEW QUESTION 402**

- (Exam Topic 3)

A network security engineer is asked to perform a Return Merchandise Authorization (RMA) on a firewall Which part of files needs to be imported back into the replacement firewall that is using Panorama?

- A. Device state and license files
- B. Configuration and serial number files
- C. Configuration and statistics files
- D. Configuration and Large Scale VPN (LSVPN) setups file

**Answer:** A

**NEW QUESTION 405**

- (Exam Topic 3)

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

- A. Panorama discards incoming logs when storage capacity 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](https://www.paloaltonetworks.com/documentation/60/panorama/panorama_adminguide/set-up-panorama/deter)

**NEW QUESTION 408**

- (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 411**

- (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 416**

- (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 418**

- (Exam Topic 3)

A host attached to ethernet1/3 cannot access the internet. The default gateway is attached to ethernet1/4. After troubleshooting. It is determined that traffic cannot pass from the ethernet1/3 to ethernet1/4. What can be the cause of the problem?

- A. DHCP has been set to Auto.
- B. Interface ethernet1/3 is in Layer 2 mode and interface ethernet1/4 is in Layer 3 mode.
- C. Interface ethernet1/3 and ethernet1/4 are in Virtual Wire Mode.
- D. DNS has not been properly configured on the firewall

**Answer:** B

**NEW QUESTION 420**

- (Exam Topic 3)

YouTube videos are consuming too much bandwidth on the network, causing delays in mission-critical traffic. The administrator wants to throttle YouTube traffic.

The following interfaces and zones are in use on the firewall:

\* ethernet1/1, Zone: Untrust (Internet-facing)

\* ethernet1/2, Zone: Trust (client-facing)

A QoS profile has been created, and QoS has been enabled on both interfaces. A QoS rule exists to put the YouTube application into QoS class 6. Interface Ethernet1/1 has a QoS profile called Outbound, and interface Ethernet1/2 has a QoS profile called Inbound.

Which setting for class 6 will throttle YouTube traffic?

- A. Outbound profile with Guaranteed Ingress
- B. Outbound profile with Maximum Ingress
- C. Inbound profile with Guaranteed Egress
- D. Inbound profile with Maximum Egress

**Answer:** D

**NEW QUESTION 421**

- (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 425

- (Exam Topic 3)

Which field is optional when creating a new Security Policy rule?

- A. Name
- B. Description
- C. Source Zone
- D. Destination Zone
- E. Action

**Answer:** B

#### NEW QUESTION 430

- (Exam Topic 3)

Click the Exhibit button below,

A firewall has three PBF rules and a default route with a next hop of 172.20.10.1 that is configured in the default VR. A user named Will has a PC with a 192.168.10.10 IP address. He makes an HTTPS connection to 172.16.10.20.

Which is the next hop IP address for the HTTPS traffic from Will's PC?

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

**Answer:** C

#### NEW QUESTION 435

- (Exam Topic 3)

Which interface configuration will accept specific VLAN IDs?

- A. Tab Mode
- B. Subinterface
- C. Access Interface
- D. Trunk Interface

**Answer:** B

#### NEW QUESTION 440

- (Exam Topic 3)

Given the following table.

Which configuration change on the firewall would cause it to use 10.66.24.88 as the next hop for the 192.168.93.0/30 network?

- A. Configuring the administrative Distance for RIP to be lower than that of OSPF Int.
- B. Configuring the metric for RIP to be higher than that of OSPF Int.
- C. Configuring the administrative Distance for RIP to be higher than that of OSPF Ext.
- D. Configuring the metric for RIP to be lower than that OSPF Ext.

**Answer:** A

#### NEW QUESTION 441

- (Exam Topic 3)

A logging infrastructure may need to handle more than 10,000 logs per second. Which two options support a dedicated log collector function? (Choose two)

- A. Panorama virtual appliance on ESX(i) only
- B. M-500
- C. M-100 with Panorama installed
- D. M-100

**Answer:** BC

#### Explanation:

(<https://live.paloaltonetworks.com/t5/Management-Articles/Panorama-Sizing-and-Design-Guide/ta-p/72181>)

#### NEW QUESTION 442

- (Exam Topic 3)

What are three valid method of user mapping? (Choose three)

- A. Syslog
- B. XML API
- C. 802.1X
- D. WildFire
- E. Server Monitoring

**Answer:** ABE

#### NEW QUESTION 444

- (Exam Topic 3)

A distributed log collection deployment has dedicated log Collectors. A developer needs a device to send logs to Panorama instead of sending logs to the Collector Group.

What should be done first?

- A. Remove the cable from the management interface, reload the log Collector and then re-connect that cable
- B. Contact Palo Alto Networks Support team to enter kernel mode commands to allow adjustments
- C. remove the device from the Collector Group
- D. Revert to a previous configuration

**Answer:** C

#### NEW QUESTION 448

- (Exam Topic 3)

Which two mechanisms help prevent a spilt brain scenario an Active/Passive High Availability (HA) pair? (Choose two)

- A. Configure the management interface as HA3 Backup
- B. Configure Ethernet 1/1 as HA1 Backup
- C. Configure Ethernet 1/1 as HA2 Backup
- D. Configure the management interface as HA2 Backup
- E. Configure the management interface as HA1 Backup
- F. Configure ethernet1/1 as HA3 Backup

**Answer:** BE

#### NEW QUESTION 450

- (Exam Topic 3)

What are three possible verdicts that WildFire can provide for an analyzed sample? (Choose three)

- A. Clean
- B. Benign
- C. Adware
- D. Suspicious
- E. Grayware
- F. Malware

**Answer:** BEF

#### Explanation:

<https://www.paloaltonetworks.com/documentation/70/pan-os/newfeaturesguide/wildfire-features/wildfire-grayw>

#### NEW QUESTION 453

- (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 455

- (Exam Topic 3)

Which two virtualized environments support Active/Active High Availability (HA) in PAN-OS 8.0? (Choose two.)

- A. KVM
- B. VMware ESX
- C. VMware NSX
- D. AWS

**Answer:** AB

#### NEW QUESTION 457

- (Exam Topic 3)

Which option is an IPv6 routing protocol?

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

**Answer: B**

#### NEW QUESTION 459

- (Exam Topic 3)

A company has a pair of Palo Alto Networks firewalls configured as an Active/Passive High Availability (HA) pair.

What allows the firewall administrator to determine the last date a failover event occurred?

- A. From the CLI issue use the show System log
- B. Apply the filter subtype eq ha to the System log
- C. Apply the filter subtype eq ha to the configuration log
- D. Check the status of the High Availability widget on the Dashboard of the GUI

**Answer: B**

#### NEW QUESTION 462

- (Exam Topic 3)

A network administrator uses Panorama to push security policies to managed firewalls at branch offices. Which policy type should be configured on Panorama if the administrators at the branch office sites to override these products?

- A. Pre Rules
- B. Post Rules
- C. Explicit Rules
- D. Implicit Rules

**Answer: A**

#### NEW QUESTION 466

.....

## Relate Links

**100% Pass Your PCNSE Exam with ExamBible Prep Materials**

<https://www.exambible.com/PCNSE-exam/>

## Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>