



# **Paloalto-Networks**

## **Exam Questions PCNSE**

Palo Alto Networks Certified Security Engineer (PCNSE) PAN-OS 8.0

## 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

In the following image from Panorama, why are some values shown in red?

| Device Name | Logging Rate (Log/sec) | Device              | Session          |
|-------------|------------------------|---------------------|------------------|
|             |                        | Throughput (KB/sec) | Count (Sessions) |
| uk3         | 781                    | 209                 | 40221            |
| sg2         | 0                      | 953                 | 170              |
| us3         | 291                    | 0                   | 67455            |

- A. sg2 session count is the lowest compared to the other managed devices.
- B. us3 has a logging rate that deviates from the administrator-configured thresholds.
- C. uk3 has a logging rate that deviates from the seven-day calculated baseline.
- D. sg2 has misconfigured session thresholds.

**Answer: C**

### NEW QUESTION 2

What should an administrator consider when planning to revert Panorama to a pre-PAN-OS 8.1 version?

- A. Panorama cannot be reverted to an earlier PAN-OS release if variables are used in templates or template stacks.
- B. An administrator must use the Expedition tool to adapt the configuration to the pre-PAN-OS 8.1 state.
- C. When Panorama is reverted to an earlier PAN-OS release, variables used in templates or template stacks will be removed automatically.
- D. Administrators need to manually update variable characters to those used in pre-PAN-OS 8.1.

**Answer: A**

### NEW QUESTION 3

Which administrative authentication method supports authorization by an external service?

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

**Answer: C**

### NEW QUESTION 4

An administrator has been asked to configure active/active HA for a pair of Palo Alto Networks NGFWs. The firewall use Layer 3 interfaces to send traffic to a single gateway IP for the pair.

Which configuration will enable this HA scenario?

- A. The two firewalls will share a single floating IP and will use gratuitous ARP to share the floating IP.
- B. Each firewall will have a separate floating IP, and priority will determine which firewall has the primary IP.
- C. The firewalls do not use floating IPs in active/active HA.
- D. The firewalls will share the same interface IP address, and device 1 will use the floating IP if device 0 fails.

**Answer: A**

### NEW QUESTION 5

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

The screenshot shows the Palo Alto Networks Monitor tab with a list of system logs. The logs table is as follows:

| Receive Time   | Type          | Severity      | Event                        | Object | Description   |
|----------------|---------------|---------------|------------------------------|--------|---|
| 06/16 08:41:43 | general       | Informational | general                      |        | User admin accessed Monitor tab   |
| 06/16 08:40:40 | general       | Informational | general                      |        | User admin logged in via Web from 192.168.55.1 using https                      |
| 06/16 08:40:40 | auth          | Informational | auth-success                 |        | authenticated for user 'admin'. From: 192.168.55.1.                             |
| 06/16 08:40:06 | general       | Informational | general                      |        | LOGIN ON tty1 BY admin  |
| 06/16 08:39:43 | general       | Informational | general                      |        | User admin logged in via CLI from Console                                       |
| 06/16 08:39:42 | auth          | Informational | auth-success                 |        | authenticated for user 'admin'. From: (null).                                   |
| 06/16 08:39:16 | url-filtering | Informational | upgrade-uri-database-success |        | PAN-DB was upgraded to version 20170615.40151.                                  |
| 06/16 08:34:15 | url-filtering | Informational | upgrade-uri-database-success |        | PAN-DB was upgraded to version 20170615.40150.                                  |
| 06/16 08:31:44 | general       | Informational | general                      |        | Failed to connect to Panorama Server: 192.168.55.5 Port: 3978 Retry: 0          |
| 06/16 08:31:40 | ntpd          | Informational | restart                      |        | NTP restart synchronization performed   |
| 06/16 08:31:33 | general       | Informational | general                      |        | Commit job succeeded. Completion time=2017/06/16 09:31:33. JobId=29. User=admin |

B

The screenshot shows the Palo Alto Networks Monitor tab with a list of traffic logs. The logs table is as follows:

| Receive Time   | Type | From Zone | To Zone | Source       | Source User | Destination    |
|----------------|------|-----------|---------|--------------|-------------|----------------|
| 06/14 08:14:14 | end  | inside    | outside | 192.168.45.1 |             | 192.168.45.255 |
| 06/14 08:13:44 | drop | outside   | outside | 192.168.55.1 |             | 192.168.55.255 |
| 06/14 08:04:14 | end  | inside    | outside | 192.168.45.1 |             | 192.168.45.255 |
| 06/14 08:03:45 | drop | outside   | outside | 192.168.55.1 |             | 192.168.55.255 |
| 06/14 07:59:38 | end  | inside    | outside | 192.168.45.1 |             | 192.168.45.255 |
| 06/14 07:59:06 | drop | outside   | outside | 192.168.55.1 |             | 192.168.55.255 |
| 06/14 07:40:27 | end  | inside    | outside | 192.168.45.1 |             | 192.168.45.255 |
| 06/14 07:39:57 | drop | outside   | outside | 192.168.55.1 |             | 192.168.55.255 |
| 06/14 07:39:56 | drop | outside   | outside | 192.168.55.1 |             | 192.168.55.255 |
| 06/14 07:39:55 | drop | outside   | outside | 192.168.55.1 |             | 192.168.55.255 |

C

|                |      |               |             |             |   |
|----------------|------|---------------|-------------|-------------|---|
| 05/23 20:49:30 | port | Informational | link-change | ethernet1/1 | Port ethernet1/1: Down 10Gb/s-full duplex |
| 05/23 20:49:29 | port | High          | link-change | MGT         | Port MGT: Down 1Gb/s Full duplex          |
| 05/23 20:47:24 | port | Informational | link-change | ethernet1/1 | Port ethernet1/1: Up 10Gb/s-full duplex   |
| 05/23 20:47:22 | port | Informational | link-change | MGT         | Port MGT: Up Unknown                      |
| 05/23 20:47:18 | port | Informational | link-change | ethernet1/1 | Port ethernet1/1: Down 10Gb/s-full duplex |
| 05/23 20:47:17 | port | High          | link-change | MGT         | Port MGT: Down 1Gb/s Full duplex          |

D

The screenshot shows the Windows Task Manager window titled "Task Manager - All Tasks" with 32 items. The tasks are as follows:

| Type        | Status    | Start Time        | Messages   | Action |
|-------------|-----------|-------------------|--|--------|
| Config Logs | Completed | 06/16/17 08:40:53 |  |        |
| System Logs | Completed | 06/16/17 08:40:53 |  |        |
| Data Logs   | Completed | 06/16/17 08:40:53 |  |        |
| Commit      | Completed | 06/16/17 08:31:19 | Commit Processing By: admin<br>Start Time (Dequeued Time): 06/16/17 08:31:19 |        |
| Commit      | Completed | 06/16/17 08:30:15 | Commit Processing By: admin<br>Start Time (Dequeued Time): 06/16/17 08:30:15 |        |

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

**Answer:** AD

#### NEW QUESTION 6

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>

#### NEW QUESTION 7

An administrator has been asked to configure a Palo Alto Networks NGFW to provide protection against worms and trojans. Which Security Profile type will protect against worms and trojans?

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 8

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

#### NEW QUESTION 9

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

#### NEW QUESTION 10

An administrator pushes a new configuration from Panorama to a pair of firewalls that are configured as an active/passive HA pair. Which NGFW receives the configuration from Panorama?

- A. The Passive firewall, which then synchronizes to the active firewall
- B. The active firewall, which then synchronizes to the passive firewall
- C. Both the active and passive firewalls, which then synchronize with each other
- D. Both the active and passive firewalls independently, with no synchronization afterward

**Answer:** C

#### NEW QUESTION 10

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

#### NEW QUESTION 14

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-intelligence>

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

#### NEW QUESTION 19

A user's traffic traversing a Palo Alto Networks NGFW sometimes can reach <http://www.company.com>. At other times the session times out. The NGFW has been configured with a PBF rule that the user's traffic matches when it goes to <http://www.company.com>.

How can the firewall be configured automatically disable the PBF rule if the next hop goes down?

- A. Create and add a Monitor Profile with an action of Wait Recover in the PBF rule in question.
- B. Create and add a Monitor Profile with an action of Fail Over in the PBF rule in question.
- C. Enable and configure a Link Monitoring Profile for the external interface of the firewall.
- D. Configure path monitoring for the next hop gateway on the default route in the virtual router.

**Answer:** C

#### NEW QUESTION 24

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:** C

#### NEW QUESTION 28

How would an administrator monitor/capture traffic on the management interface of the Palo Alto Networks NGFW?

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

**Answer:** D

#### Explanation:

Reference: <https://live.paloaltonetworks.com/t5/Learning-Articles/How-to-Run-a-Packet-Capture/ta-p/62390>

#### NEW QUESTION 31

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-users>

#### NEW QUESTION 32

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:** BD

**NEW QUESTION 35**

An administrator logs in to the Palo Alto Networks NGFW and reports that the WebUI is missing the Policies tab. Which profile is the cause of the missing Policies tab?

- A. Admin Role
- B. WebUI
- C. Authentication
- D. Authorization

**Answer:** A

**NEW QUESTION 36**

An administrator is using Panorama and multiple Palo Alto Networks NGFWs. After upgrading all devices to the latest PAN-OS® software, the administrator enables log forwarding from the firewalls to Panorama. Pre-existing logs from the firewalls are not appearing in Panorama.

Which action would enable the firewalls to send their pre-existing logs to Panorama?

- A. Use the import option to pull logs into Panorama.
- B. A CLI command will forward the pre-existing logs to Panorama.
- C. Use the ACC to consolidate pre-existing logs.
- D. The log database will need to be exported from the firewalls and manually imported into Panorama.

**Answer:** B

**NEW QUESTION 38**

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:** A

**NEW QUESTION 42**

Which Palo Alto Networks VM-Series firewall is valid?

- A. VM-25
- B. VM-800
- C. VM-50
- D. VM-400

**Answer:** C

**Explanation:**

Reference: <https://www.paloaltonetworks.com/products/secure-the-network/virtualized-next-generation-firewall/vm-series>

**NEW QUESTION 47**

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:**

Reference: [https://www.paloaltonetworks.com/documentation/80/wildfire/wf\\_admin/wildfire-overview/wildfire-file-type-support](https://www.paloaltonetworks.com/documentation/80/wildfire/wf_admin/wildfire-overview/wildfire-file-type-support)

**NEW QUESTION 51**

Which event will happen if an administrator uses an Application Override Policy?

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Reference: <https://live.paloaltonetworks.com/t5/Learning-Articles/Tips-and-Tricks-How-to-Create-an-Application-Override/ta-p/65513>

#### NEW QUESTION 53

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: B**

#### NEW QUESTION 54

In a virtual router, which object contains all potential routes?

- A. MIB
- B. RIB
- C. SIP
- D. FIB

**Answer: B**

#### Explanation:

Reference: [https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=10&ved=0ahUKEwiOkbfYzPzXAhVnEJoKHcwVCg4QFghiMAk&url=https%3A%2F%2Flive.paloaltonetworks.com%2Ftwzvq79624%2Fattachments%2Ftwzvq79624%2Fdocumentation\\_tkb%2F487%2F1%2FRoute%2520Redistribution%2520and%2520Filtering%2520TechNote%2520-%2520Rev%2520B.pdf&usg=AOvVaw0H9qgaJK0ol2xjlJBNo1Km](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=10&ved=0ahUKEwiOkbfYzPzXAhVnEJoKHcwVCg4QFghiMAk&url=https%3A%2F%2Flive.paloaltonetworks.com%2Ftwzvq79624%2Fattachments%2Ftwzvq79624%2Fdocumentation_tkb%2F487%2F1%2FRoute%2520Redistribution%2520and%2520Filtering%2520TechNote%2520-%2520Rev%2520B.pdf&usg=AOvVaw0H9qgaJK0ol2xjlJBNo1Km)

#### NEW QUESTION 56

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 61

Which protection feature is available only in a Zone Protection Profile?

- A. SYN Flood Protection using SYN Flood Cookies
- B. ICMP Flood Protection
- C. Port Scan Protection
- D. UDP Flood Protections

**Answer: A**

#### NEW QUESTION 66

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:

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

#### NEW QUESTION 70

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-OS-6.0-CLI-ref.pdf](https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/technical-documentation/pan-os-60/PAN-OS-6.0-CLI-ref.pdf)

#### NEW QUESTION 74

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:** BD

**NEW QUESTION 79**

Which tool provides an administrator the ability to see trends in traffic over periods of time, such as threats detected in the last 30 days?

- A. Session Browser
- B. Application Command Center
- C. TCP Dump
- D. Packet Capture

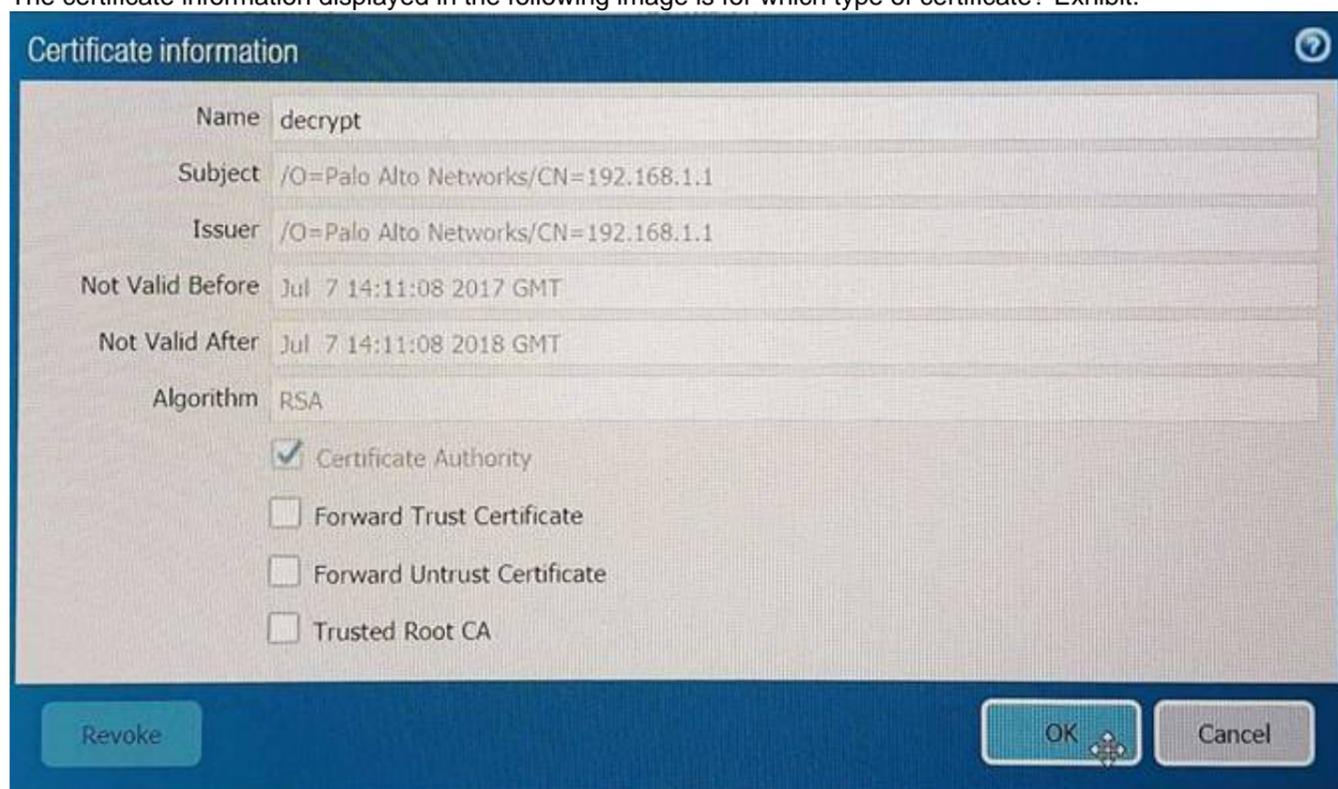
**Answer:** B

**Explanation:**

Reference: <https://live.paloaltonetworks.com/t5/Management-Articles/Tips-and-Tricks-How-to-Use-the-Application-Command-Center-ACC/ta-p/67342>

**NEW QUESTION 82**

The certificate information displayed in the following image is for which type of certificate? Exhibit:



- A. Forward Trust certificate
- B. Self-Signed Root CA certificate
- C. Web Server certificate
- D. Public CA signed certificate

**Answer:** D

**NEW QUESTION 84**

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 traffic as their accounting application and to scan this traffic for threats.

Which option would achieve this result?

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

**Answer:** A

**NEW QUESTION 86**

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

#### NEW QUESTION 91

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>

#### NEW QUESTION 95

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/59719>

#### NEW QUESTION 98

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-profiles-vulnerability-protection>

#### NEW QUESTION 101

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/plan-your-panorama-deployment](https://www.paloaltonetworks.com/documentation/80/panorama/panorama_adminguide/panorama-overview/plan-your-panorama-deployment)

#### NEW QUESTION 102

A web server is hosted in the DMZ and the server is configured to listen for incoming connections on TCP port 443. A Security policies rules allowing access from the Trust zone to the DMZ zone needs to be configured to allow web-browsing access. The web server hosts its contents over HTTP(S). Traffic from Trust to DMZ is being decrypted with a Forward Proxy rule.

Which combination of service and application, and order of Security policy rules, needs to be configured to allow cleartext web- browsing traffic to this server on tcp/443.

- A. Rule #1: application: web-browsing; service: application-default; action: allow Rule #2: application: ssl; service: application-default; action: allow
- B. Rule #1: application: web-browsing; service: service-https; action: allow Rule #2: application: ssl; service: application-default; action: allow
- C. Rule # 1: application: ssl; service: application-default; action: allow Rule #2: application: web-browsing; service: application-default; action: allow
- D. Rule #1: application: web-browsing; service: service-http; action: allow Rule #2: application: ssl; service: application-default; action: allow

**Answer:** A

#### NEW QUESTION 107

Which two options prevent the firewall from capturing traffic passing through it? (Choose two.)

- A. The firewall is in multi-vsyt mode.
- B. The traffic is offloaded.

- C. The traffic does not match the packet capture filter.
- D. The firewall's DP CPU is higher than 50%.

**Answer:** BC

**Explanation:**

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/monitoring/take-packet-captures/disable-hardware-offload>

**NEW QUESTION 111**

Which User-ID method should be configured to map IP addresses to usernames for users connected through a terminal server?

- A. port mapping
- B. server monitoring
- C. client probing
- D. XFF headers

**Answer:** A

**Explanation:**

Reference: <https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/user-id/configure-user-mapping-for-terminal-server-users>

**NEW QUESTION 114**

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. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

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

**NEW QUESTION 118**

A client has a sensitive application server in their data center and is particularly concerned about resource exhaustion because of distributed denial-of-service attacks.

How can the Palo Alto Networks NGFW be configured to specifically protect this server against resource exhaustion originating from multiple IP addresses (DDoS attack)?

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

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

**NEW QUESTION 123**

Which CLI command enables an administrator to check the CPU utilization of the dataplane?

- A. show running resource-monitor
- B. debug data-plane dp-cpu
- C. show system resources
- D. debug running resources

**Answer:** A

**NEW QUESTION 125**

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-updates>

**NEW QUESTION 129**

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 130

Which prerequisite must be satisfied before creating an SSH proxy Decryption policy?

- A. Both SSH keys and SSL certificates must be generated.
- B. No prerequisites are required.
- C. SSH keys must be manually generated.
- D. SSL certificates must be generated.

**Answer:** B

**Explanation:**

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

#### NEW QUESTION 133

An administrator deploys PA-500 NGFWs as an active/passive high availability pair. The devices are not participating in dynamic routing and preemption is disabled.

What must be verified to upgrade the firewalls to the most recent version of PAN-OS software?

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Dependencies : Before upgrade, make sure the firewall is running a version of app + threat (content version) that meets the minimum requirement of the new PAN-OS Upgrade. Reference: <https://live.paloaltonetworks.com/t5/Featured-Articles/Best-Practices-for-PAN-OS-Upgrade/ta-p/111045>

#### NEW QUESTION 134

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

**Answer:** A

#### NEW QUESTION 137

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 VLAN objects for each VLAN and assign VLAN interfaces matching each VLAN I
- B. Repeat forevery additional VLANand use a VLAN ID of 0 for untagged traffi
- C. Assign each interface/subinterface to a unique zone.
- D. Create V-Wire objects with two V-Wire sub interface and assign only a single VLAN ID to the "Tag Allowed field one of the V-Wire object Repeat for every additional VLAN and use a VIAN ID of 0 for untagged traffi
- E. Assign each interface/subinterfaceto a unique zone.
- F. Create V-Wire objects with two V-Wire interfaces and define a range "0- 4096" in the "Tag Allowed filed of the V-Wire object.
- G. Create Layer 3 sub interfaces that are each assigned to a single VLAN ID and a common virtual route
- H. The physical Layer 3interface would handle untagged traffi
- I. Assign each interface /subinterface to a unique zon
- J. Do not assign any interface anIP address

**Answer:** C

#### NEW QUESTION 140

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:** A

**NEW QUESTION 145**

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 149**

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**

**NEW QUESTION 153**

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: CD**

**NEW QUESTION 154**

An administrator wants a new Palo Alto Networks NGFW to obtain automatic application updates daily, so it is configured to use a scheduler for the application database. Unfortunately, they required the management network to be isolated so that it cannot reach the internet. Which configuration will enable the firewall to download and install application updates automatically?

- A. Configure a Policy Based Forwarding policy rule for the update server IP address so that traffic sourced from the management interface destined for the update servers goes out of the interface acting as your internet connection.
- B. Configure a security policy rule to allow all traffic to and from the update servers.
- C. Download and install application updates cannot be done automatically if the MGT port cannot reach the internet.
- D. Configure a service route for Palo Alto networks services that uses a dataplane interface that can route traffic to the internet, and create a security policy rule to allow the traffic from that interface to the update servers if necessary.

**Answer: B**

**NEW QUESTION 156**

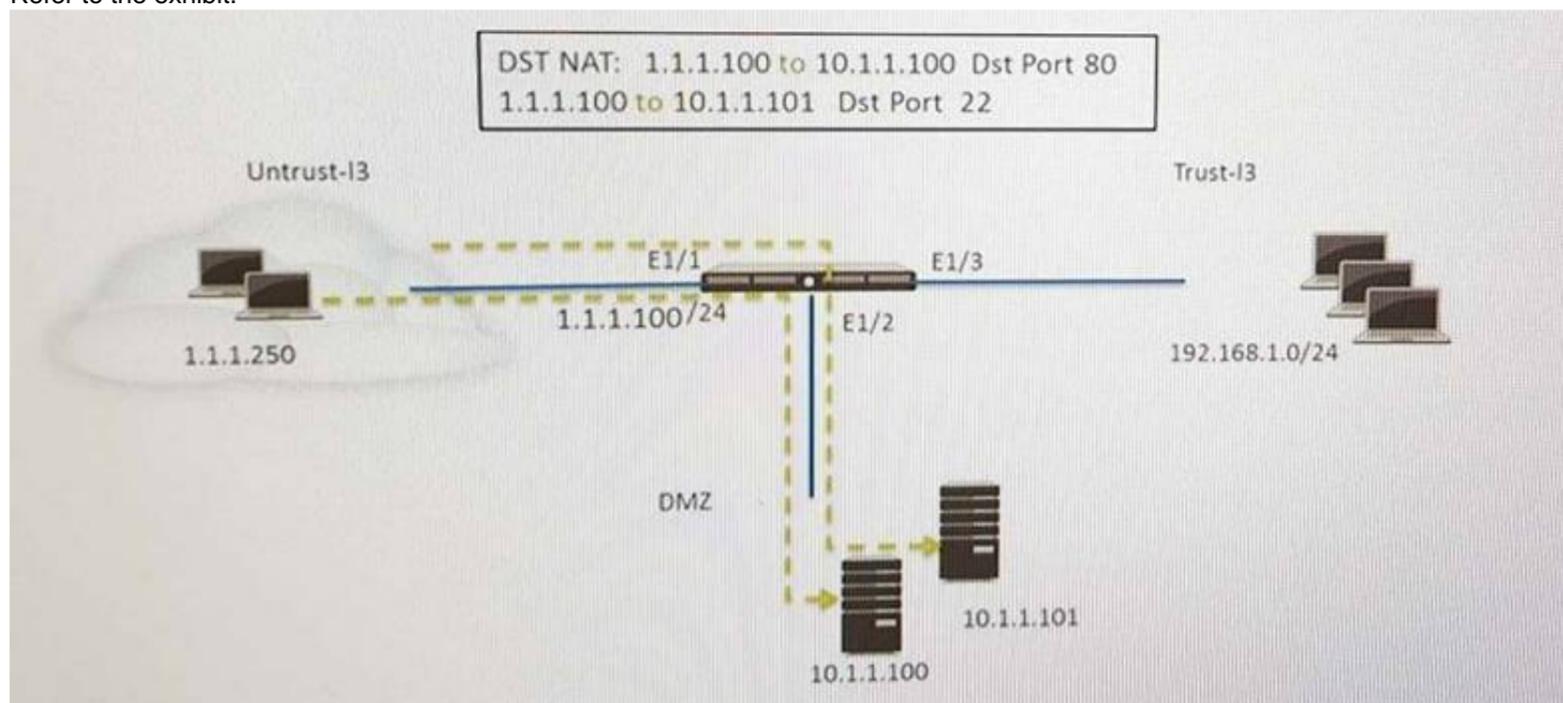
Which three firewall states are valid? (Choose three)

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

**Answer: ABC**

**NEW QUESTION 158**

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 162

Which is the maximum number of samples that can be submitted to WildFire per day, based on wildfire subscription?

- A. 15,000
- B. 10,000
- C. 75,00
- D. 5,000

**Answer:** B

#### NEW QUESTION 167

Which operation will impact the performance of the management plane?

- A. WildFire Submissions
- B. DoS Protection
- C. decrypting SSL Sessions
- D. Generating a SaaS Application Report.

**Answer:** C

#### NEW QUESTION 170

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 171

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

#### NEW QUESTION 174

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 179

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 183

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 186**

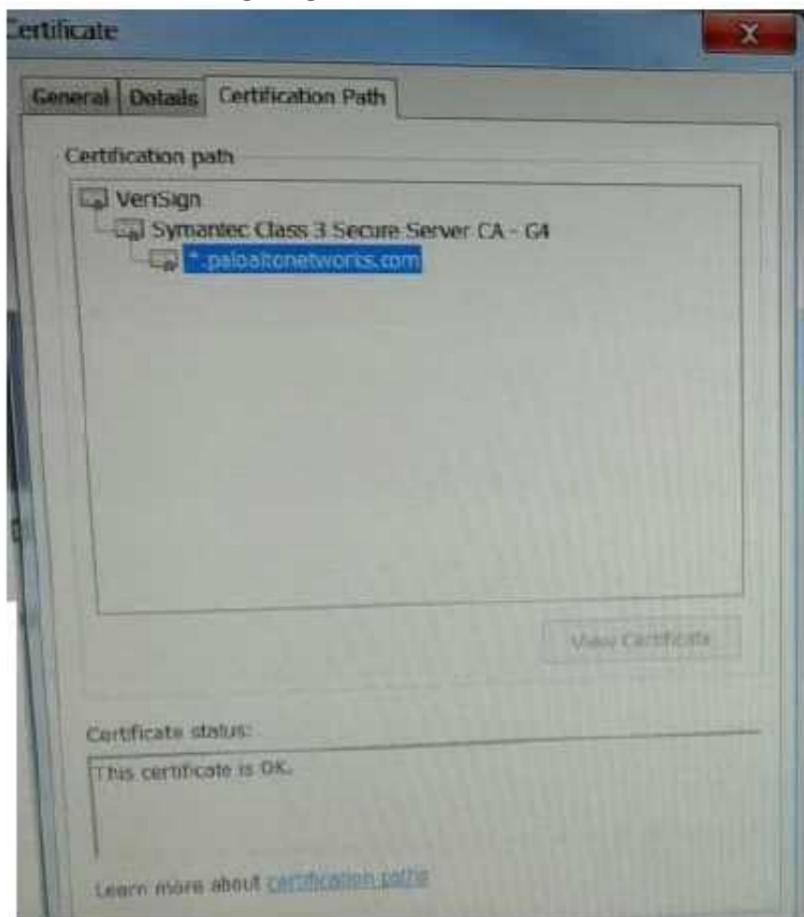
Which two settings can be configured only locally on the firewall and not pushed from a Panorama template or template stack? (Choose two)

- A. HA1 IP Address
- B. Network Interface Type
- C. Master Key
- D. Zone Protection Profile

**Answer: AB**

**NEW QUESTION 188**

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: D**

**NEW QUESTION 189**

A host attached to Ethernet 1/4 cannot ping the default gateway. The widget on the dashboard shows Ethernet 1/1 and Ethernet 1/4 to be green. The IP address of Ethernet 1/1 is 192.168.1.7 and the IP address of Ethernet 1/4 is 10.1.1.7. The default gateway is attached to Ethernet 1/1. A default route is properly configured. What can be the cause of this problem?

- A. No Zone has been configured on Ethernet 1/4.
- B. Interface Ethernet 1/1 is in Virtual Wire Mode.
- C. DNS has not been properly configured on the firewall.
- D. DNS has not been properly configured on the host.

**Answer: A**

**NEW QUESTION 193**

Given the following table.

Virtual Router - default

Routing | RIP | OSPF | OSPFv3 | BGP | Multicast

10 items

| Destination     | Next Hop     | Flags | Age   | Interface   |
|-----------------|--------------|-------|-------|-------------|
| 10.66.22.0/23   | 10.66.22.80  | A C   |       | ethernet1/5 |
| 10.66.22.80/32  | 0.0.0.0      | A H   |       |             |
| 10.66.24.0/23   | 0.0.0.0      | R     |       | ethernet1/3 |
| 10.66.24.0/23   | 0.0.0.0      | Oi    | 19567 | ethernet1/3 |
| 10.66.24.0/23   | 10.66.24.80  | A C   |       | ethernet1/3 |
| 10.66.24.80/32  | 0.0.0.0      | A H   |       |             |
| 192.168.80.0/24 | 192.168.80.1 | A C   |       | ethernet1/4 |
| 192.168.80.1/32 | 0.0.0.0      | A H   |       |             |
| 192.168.93.0/30 | 10.66.24.88  | R     |       | ethernet1/3 |
| 192.168.93.0/30 | 10.66.24.93  | A Oi  | 600   | ethernet1/3 |

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 195**

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 200**

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 204**

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 206**

A company hosts a publically 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 be NAT policy contain to allow users in the untrust-L3 zone to access the web server? (Choose two)

- A. Untrust-L3 for both Source and Destination zone
- B. Destination IP of 192.168.1.10

- C. Untrust-L3 for Source Zone and Trust-L3 for Destination Zone
- D. Destination IP of 23.54.6.10

**Answer:** CD

#### NEW QUESTION 211

Which two statements are correct for the out-of-box configuration for Palo Alto Networks NGFWs? (Choose two)

- A. The devices are pre-configured with a virtual wire pair out the first two interfaces.
- B. The devices are licensed and ready for deployment.
- C. The management interface has an IP address of 192.168.1.1 and allows SSH and HTTPS connections.
- D. A default bidirectional rule is configured that allows Untrust zone traffic to go to the Trust zone.
- E. The interface are pingable.

**Answer:** BC

#### NEW QUESTION 215

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/53623>  
<https://live.paloaltonetworks.com/t5/Configuration-Articles/File-Blocking-Rulebase-and-Action-Precedence/ta-p/53623>  
<https://live.paloaltonetworks.com/t5/Configuration-Articles/File-Blocking-Rulebase-and-Action-Precedence/ta-p/53623>

#### NEW QUESTION 218

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 222

The company's Panorama server (IP 10.10.10.5) is not able to manage a firewall that was recently deployed. The firewall's dedicated management port is being used to connect to the management network.

Which two commands may be used to troubleshoot this issue from the CLI of the new firewall? (Choose two)

- A. test panoramas-connect 10.10.10.5
- B. show panoramas-status
- C. show arp all | match 10.10.10.5
- D. topdump filter "host 10.10.10.5
- E. debug dataplane packet-diag set capture on

**Answer:** BD

#### NEW QUESTION 225

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 229

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/determine-panorama-log-storage-requirements](https://www.paloaltonetworks.com/documentation/60/panorama/panorama_adminguide/set-up-panorama/determine-panorama-log-storage-requirements))

**NEW QUESTION 233**

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 236**

Which three options are available when creating a security profile? (Choose three)

- A. Anti-Malware
- B. File Blocking
- C. Url Filtering
- D. IDS/ISP
- E. Threat Prevention
- F. Antivirus

**Answer:** ABF

**NEW QUESTION 241**

A Palo Alto Networks firewall is being targeted by an NTP Amplification attack and is being flooded with tens thousands of bogus UDP connections per second to a single destination IP address and port.

Which option when enabled with the correction threshold would mitigate this attack without dropping legitimate traffic to other hosts inside the network?

- A. Zone Protection Policy with UDP Flood Protection
- B. QoS Policy to throttle traffic below maximum limit
- C. Security Policy rule to deny traffic to the IP address and port that is under attack
- D. Classified DoS Protection Policy using destination IP only with a Protect action

**Answer:** D

**NEW QUESTION 246**

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 the 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-up-the-m-100-appliance](https://www.paloaltonetworks.com/documentation/60/panorama/panorama_adminguide/set-up-panorama/set-up-the-m-100-appliance))

**NEW QUESTION 248**

Company.com has an in-house application that the Palo Alto Networks device doesn't identify correctly. A Threat Management Team member has mentioned that this in-house application is very sensitive and all traffic being identified needs to be inspected by the Content-ID engine.

Which method should company.com use to immediately address this traffic on a Palo Alto Networks device?

- A. Create a custom Application without signatures, then create an Application Override policy that includes the source, Destination, Destination Port/Protocol and Custom Application of the traffic.
- B. Wait until an official Application signature is provided from Palo Alto Networks.
- C. Modify the session timer settings on the closest referenced application to meet the needs of the in-house application
- D. Create a Custom Application with signatures matching unique identifiers of the in-house application traffic

**Answer:** D

**NEW QUESTION 253**

Click the Exhibit button below,

**Exhibit Window**

|   |      | Source |                |                 | Destination |                |             |
|---|------|--------|----------------|-----------------|-------------|----------------|-------------|
|   | Name | Tags   | Zone/Interface | Address         | User        | Address        | Application |
| 1 | PBF1 | none   | Trust-L3       | 192.168.10.0/24 | any         | 172.16.10.0/24 | any         |
| 2 | PBF2 | none   | Trust-L3       | 192.168.10.0/24 | any         | 172.16.10.0/24 | any         |
| 3 | PBF3 | none   | Trust-L3       | 192.168.10.0/24 | Will        | 172.16.10.0/24 | any         |

| Forwarding    |         |               |             |                          |
|---------------|---------|---------------|-------------|--------------------------|
| Service       | Action  | Egress I/F    | Next Hop    | Enforce Symmetric Return |
| any           | forward | ethernet1/2.2 | 172.20.20.1 | false                    |
| service-http  | forward | ethernet1/3.2 | 172.20.30.1 | false                    |
| service-https | forward | ethernet1/3.3 | 172.20.40.1 | false                    |

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 256**

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 258**

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-HYPERLINK \"https://www.paloaltonetworks.com/documentation/70/pan-os/newfeaturesguide/wildfire-features/wildfire-grayware-verdict\"/os/newfeaturesguide/wildfire-features/wildfire-grayware-verdict](https://www.paloaltonetworks.com/documentation/70/pan-HYPERLINK \)

**NEW QUESTION 263**

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 266**

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 268**

Which interface configuration will accept specific VLAN IDs?

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

**Answer:** B

**NEW QUESTION 273**

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.

|   | Source |          |         |      | Destination |         |             |                     |        |         |         |
|---|--------|----------|---------|------|-------------|---------|-------------|---------------------|--------|---------|---------|
|   | Name   | Zone     | Address | User | Zone        | Address | Application | Service             | Action | Profile | Options |
| 1 | rule1  | Trust-L3 | any     | any  | UnTrust-L3  | any     | Known Good  | application-Default | Allow  | None    |         |
| 2 | rule2  | Trust-L3 | any     | any  | UnTrust-L3  | any     | Known Bad   | any                 | Deny   | None    |         |
| 3 | rule3  | Trust-L3 | any     | any  | UnTrust-L3  | any     | any         | any                 | Deny   | None    |         |

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 277**

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 280**

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 285**

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 286**

Which option is an IPv6 routing protocol?

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

**Answer:** B

#### NEW QUESTION 289

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 292

When is it necessary to activate a license when provisioning a new Palo Alto Networks firewall?

- A. When configuring Certificate Profiles
- B. When configuring GlobalProtect portal
- C. When configuring User Activity Reports
- D. When configuring Antivirus Dynamic Updates

**Answer:** D

#### NEW QUESTION 296

Which authentication source requires the installation of Palo Alto Networks software, other than PAN-OS 7x, to obtain a username-to-IP-address mapping?

- A. Microsoft Active Directory
- B. Microsoft Terminal Services
- C. Aerohive Wireless Access Point
- D. Palo Alto Networks Captive Portal

**Answer:** B

#### NEW QUESTION 297

People are having intermittent quality issues during a live meeting via web application.

- A. Use QoS profile to define QoS Classes
- B. Use QoS Classes to define QoS Profile
- C. Use QoS Profile to define QoS Classes and a QoS Policy
- D. Use QoS Classes to define QoS Profile and a QoS Policy

**Answer:** C

#### NEW QUESTION 298

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 301

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 304

Which CLI command displays the current management plan memory utilization?



\* 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 322**

How can a Palo Alto Networks firewall be configured to send syslog messages in a format compatible with non-standard syslog servers?

- A. Enable support for non-standard syslog messages under device management
- B. Check the custom-format check box in the syslog server profile
- C. Select a non-standard syslog server profile
- D. Create a custom log format under the syslog server profile

**Answer: D**

**NEW QUESTION 325**

Which Device Group option is assigned by default in Panorama whenever a new device group is created to manage a Firewall?

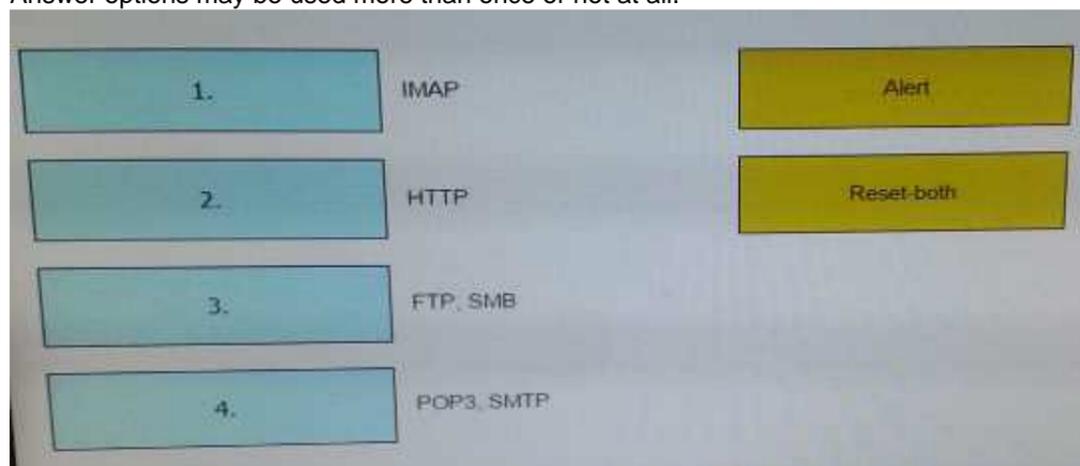
- A. Master
- B. Universal
- C. Shared
- D. Global

**Answer: C**

**NEW QUESTION 330**

DRAG DROP

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 333**

.....

## 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/>