



# 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)

An Administrator is configuring Authentication Enforcement and they would like to create an exemption rule to exempt a specific group from authentication. Which authentication enforcement object should they select?

- A. default-browser-challenge
- B. default-authentication-bypass
- C. default-web-format
- D. default-no-captive-portal

**Answer:** D

#### NEW QUESTION 3

- (Exam Topic 2)

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 4

- (Exam Topic 2)

Refer to the exhibit.

A web server in the DMZ is being mapped to a public address through DNAT. Which Security policy rule will allow traffic to flow to the web server?

- A. Untrust (any) to Untrust (10. 1.1. 100), web browsing – Allow
- B. Untrust (any) to Untrust (1. 1. 1. 100), web browsing – Allow
- C. Untrust (any) to DMZ (1. 1. 1. 100), web browsing – Allow
- D. Untrust (any) to DMZ (10. 1. 1. 100), web browsing – Allow

**Answer:** C

#### Explanation:

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

#### NEW QUESTION 5

- (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 6

- (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 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)

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 9

- (Exam Topic 2)

Which DoS protection mechanism detects and prevents session exhaustion attacks?

- A. Packet Based Attack Protection
- B. Flood Protection
- C. Resource Protection
- D. TCP Port Scan Protection

**Answer:** C

**Explanation:**

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

#### NEW QUESTION 10

- (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-inte>

#### NEW QUESTION 10

- (Exam Topic 2)

Starting 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 13

- (Exam Topic 2)

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

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

**Answer:** B

#### NEW QUESTION 16

- (Exam Topic 2)

Refer to the exhibit.

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

Which two security policy rules will accomplish this configuration? (Choose two)

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

**Answer:** CD

#### NEW QUESTION 20

- (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 24

- (Exam Topic 2)

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

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

**Answer:** DE

#### Explanation:

Reference:

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

#### NEW QUESTION 27

- (Exam Topic 2)

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:** D

#### Explanation:

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

#### NEW QUESTION 28

- (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 33

- (Exam Topic 2)

SD-WAN is designed to support which two network topology types? (Choose two.)

- A. ring
- B. point-to-point
- C. hub-and-spoke
- D. full-mesh

**Answer:** CD

#### NEW QUESTION 38

- (Exam Topic 2)

To more easily reuse templates and template slacks , you can create term plate variables in place of firewall-specific and appliance-specific IP literals in your configurations

Which one is the correct configuration?

- A. @Panorama
- B. #Pancrama
- C. &Panorama
- D. \$Panorama

**Answer:** D

#### NEW QUESTION 42

- (Exam Topic 2)

An administrator is defining protection settings on the Palo Alto Networks NGFW to guard against resource exhaustion. When platform utilization is considered, which steps must the administrator take to configure and apply packet buffer protection?

- A. Enable and configure the Packet Buffer protection thresholds.Enable Packet Buffer Protection per ingress zone.
- B. Enable and then configure Packet Buffer thresholdsEnable Interface Buffer protection.
- C. Create and Apply Zone Protection Profiles in all ingress zones.Enable Packet Buffer Protection per ingress zone.
- D. Configure and apply Zone Protection Profiles for all egress zones.Enable Packet Buffer Protection pre egress zone.
- E. Enable per-vsyz Session Threshold alerts and triggers for Packet Buffer Limits.Enable Zone Buffer Protection per zone.

**Answer:** A

#### NEW QUESTION 43

- (Exam Topic 2)

How does Panorama prompt VMWare NSX to quarantine an infected VM?

- A. HTTP Server Profile
- B. Syslog Server Profile
- C. Email Server Profile
- D. SNMP Server Profile

**Answer:** A

#### NEW QUESTION 46

- (Exam Topic 2)

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:** B

#### NEW QUESTION 48

- (Exam Topic 2)

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

How quickly will the firewall receive back a verdict?

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

**Answer:** D

#### NEW QUESTION 53

- (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 58

- (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 61

- (Exam Topic 2)

A Security policy rule is configured with a Vulnerability Protection Profile and an action of ‘Deny’. Which action will this cause configuration on the matched traffic?

- A. The configuration is invalid
- B. The Profile Settings section will be grayed out when the Action is set to “Deny”.
- C. The configuration will allow the matched session unless a vulnerability signature is detected
- D. The “Deny” action will supersede the per-severity defined actions defined in the associated Vulnerability Protection Profile.
- E. The configuration is invalid
- F. It will cause the firewall to skip this Security policy rule
- G. A warning will be displayed during a commit.
- H. The configuration is valid
- I. It will cause the firewall to deny the matched session
- J. Any configured Security Profiles have no effect if the Security policy rule action is set to “Deny.”

**Answer:** D

#### Explanation:

“Security profiles are not used in the match criteria of a traffic flow. The security profile is applied to scan traffic after the application or category is allowed by the security policy.”

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/policy/security-profiles.html#>

#### NEW QUESTION 63

- (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 66**

- (Exam Topic 2)

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

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

**Answer:** C

**Explanation:**

Reference:

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

**NEW QUESTION 70**

- (Exam Topic 2)

Which three authentication services can administrator use to authenticate admins into the Palo Alto Networks NGFW without defining a corresponding admin account on the local firewall? (Choose three.)

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

**Answer:** ACF

**Explanation:**

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

The administrative accounts are defined on an external SAML, TACACS+, or RADIUS server. The server performs both authentication and authorization. For authorization, you define Vendor-Specific Attributes (VSAs) on the TACACS+ or RADIUS server, or SAML attributes on the SAML server. PAN-OS maps the attributes to administrator roles, access domains, user groups, and virtual systems that you define on the firewall. For details, see:

Configure SAML AuthenticationConfigure TACACS+ AuthenticationConfigure RADIUS Authentication

**NEW QUESTION 71**

- (Exam Topic 2)

A customer wants to set up a VLAN interface for a Layer 2 Ethernet port.

Which two mandatory options are used to configure a VLAN interface? (Choose two.)

- A. Virtual router
- B. Security zone
- C. ARP entries
- D. Netflow Profile

**Answer:** AB

**Explanation:**

Reference:

<https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/network/network-interfaces/pa-layer-2-interface#idd2bcaacc-54b9-4ec9-a1dd-8064499f5b9d>

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIRqCAK>

VLAN interface is not necessary but in this scenario we assume it is. Create VLAN object, VLAN interface and VLAN Zone. Attach VLAN interface to VLAN object together with two L2 interfaces then attach VLAN interface to virtual router. Without VLAN interface you can pass traffic between interfaces on the same network and with VLAN interface you can route traffic to other networks.

**NEW QUESTION 76**

- (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 80**

- (Exam Topic 2)

Refer to exhibit.



An organization has Palo Alto Networks NGFWs that send logs to remote monitoring and security management platforms. The network team has reported excessive traffic on the corporate WAN.

How could the Palo Alto Networks NGFW administrator reduce WAN traffic while maintaining support for all existing monitoring/ security platforms?

- A. Forward logs from firewalls only to Panorama and have Panorama forward logs to other external services.
- B. Forward logs from external sources to Panorama for correlation, and from Panorama send them to the NGFW.
- C. Configure log compression and optimization features on all remote firewalls.
- D. Any configuration on an M-500 would address the insufficient bandwidth concerns.

**Answer:** A

**Explanation:**

<https://docs.paloaltonetworks.com/panorama/8-1/panorama-admin/panorama-overview/centralized-logging-and>

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIKFCA0>

"When this has to be done over a WAN link with bandwidth limitation, it is necessary to consider reducing the number of log streams that are sent over the link"

"With this configuration, firewalls will forward logs to Panorama, assuming that log forwarding was configured correctly on the firewall. The logs are forwarded to the syslog server, thus reducing the number of log streams significantly."

**NEW QUESTION 84**

- (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 85**

- (Exam Topic 2)

If the firewall is configured for credential phishing prevention using the "Domain Credential Filter" method, which login will be detected as credential theft?

- A. Mapping to the IP address of the logged-in user.
- B. First four letters of the username matching any valid corporate username.
- C. Using the same user's corporate username and password.
- D. Matching any valid corporate username.

**Answer:** A

**Explanation:**

<https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-new-features/content-inspection-features/credential-phishi>

Reference:

<https://www.paloaltonetworks.com/documentation/80/pan-os/newfeaturesguide/content-inspection-features/cred-phishing-prevention>

**NEW QUESTION 89**

- (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 92**

- (Exam Topic 2)

Which PAN-OS® policy must you configure to force a user to provide additional credentials before he is allowed to access an internal application that contains highly-sensitive business data?

- A. Security policy
- B. Decryption policy
- C. Authentication policy
- D. Application Override policy

**Answer:** C

**NEW QUESTION 96**

- (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 98

- (Exam Topic 2)

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

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

**Answer:** AD

#### Explanation:

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

#### NEW QUESTION 101

- (Exam Topic 2)

When configuring a GlobalProtect Portal, what is the purpose of specifying an Authentication Profile?

- A. To enable Gateway authentication to the Portal
- B. To enable Portal authentication to the Gateway
- C. To enable user authentication to the Portal
- D. To enable client machine authentication to the Portal

**Answer:** C

#### Explanation:

The additional options of Browser and Satellite enable you to specify the authentication profile to use for specific scenarios. Select Browser to specify the authentication profile to use to authenticate a user accessing the portal from a web browser with the intent of downloading the GlobalProtect agent (Windows and Mac). Select Satellite to specify the authentication profile to use to authenticate the satellite.

Reference

<https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/globalprotect/network-globalpr>

#### NEW QUESTION 103

- (Exam Topic 2)

Refer to the exhibit.

An administrator cannot see any of the Traffic logs from the Palo Alto Networks NGFW on Panorama. The configuration problem seems to be on the firewall side. Where is the best place on the Palo Alto Networks NGFW to check whether the configuration is correct?

- A)
- B)
- C)
- D)

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

**Answer:** A

**Explanation:**

<https://docs.paloaltonetworks.com/panorama/9-0/panorama-admin/manage-log-collection/configure-log-forward>

**NEW QUESTION 104**

- (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 108**

- (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 109**

- (Exam Topic 2)

Which Captive Portal mode must be configured to support MFA authentication?

- A. NTLM
- B. Redirect
- C. Single Sign-On
- D. Transparent

**Answer:** B

**Explanation:**

Reference:

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

**NEW QUESTION 112**

- (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 117

- (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 118

- (Exam Topic 2)

At which stage of the cyber-attack lifecycle would the attacker attach an infected PDF file to an email?

- A. exploitation
- B. IP command and control
- C. delivery
- D. reconnaissance

**Answer:** D

#### NEW QUESTION 120

- (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 125

- (Exam Topic 2)

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> <https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/monitoring/take-packet-captures/take-a-packet-capt>

#### NEW QUESTION 126

- (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 130

- (Exam Topic 2)

Which User-ID method maps IP addresses to usernames for users connecting through an 802.1x-enabled wireless network device that has no native integration with PAN-OS® software?

- A. XML API
- B. Port Mapping
- C. Client Probing
- D. Server Monitoring

**Answer:** A

**Explanation:**

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/user-id/user-id-concepts/user-mapping/xml-api.html>

#### NEW QUESTION 132

- (Exam Topic 1)

An administrator needs to gather information about the CPU utilization on both the management plane and the data plane. Where does the administrator view the desired data?

- A. Monitor > Utilization
- B. Resources Widget on the Dashboard
- C. Support > Resources
- D. Application Command and Control Center

**Answer:** A

#### NEW QUESTION 135

- (Exam Topic 1)

A variable name must start with which symbol?

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

**Answer:** A

**Explanation:**

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

#### NEW QUESTION 139

- (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 140

- (Exam Topic 1)

When an in-band data port is set up to provide access to required services, what is required for an interface that is assigned to service routes?

- A. The interface must be used for traffic to the required services
- B. You must enable DoS and zone protection
- C. You must set the interface to Layer 2 Layer 3. or virtual wire
- D. You must use a static IP address

**Answer:** A

#### NEW QUESTION 142

- (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 143

- (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 148

- (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 153

- (Exam Topic 1)

During SSL decryption which three factors affect resource consumption? (Choose three )

- A. TLS protocol version
- B. transaction size
- C. key exchange algorithm
- D. applications that use non-standard ports
- E. certificate issuer

**Answer:** ABC

#### Explanation:

<https://docs.paloaltonetworks.com/best-practices/8-1/decryption-best-practices/decryption-best-practices/plan-ss>

#### NEW QUESTION 158

- (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 161

- (Exam Topic 1)

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

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

**Answer:** B

#### NEW QUESTION 164

- (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 167

- (Exam Topic 1)

An administrator cannot see any Traffic logs from the Palo Alto Networks NGFW in Panorama reports. The configuration problem seems to be on the firewall Which settings, if configured incorrectly, most likely would stop only Traffic logs from being sent from the NGFW to Panorama?

- A)
- B)
- C)
- D)



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

**Answer:** B

#### NEW QUESTION 171

- (Exam Topic 1)

The SSL Forward Proxy decryption policy is configured. The following four certificate authority (CA) certificates are installed on the firewall.  
An end-user visits the untrusted website [https //www firewall-do-not-trust-website com](https://www.firewall-do-not-trust-website.com)

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

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

**Answer:** B

#### NEW QUESTION 173

- (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 177

- (Exam Topic 1)

Which configuration task is best for reducing load on the management plane?

- A. Disable logging on the default deny rule
- B. Enable session logging at start
- C. Disable pre-defined reports
- D. Set the URL filtering action to send alerts

**Answer:** A

#### NEW QUESTION 182

- (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 184

- (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 187

- (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 191

- (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 196

- (Exam Topic 1)

In a Panorama template, which three types of objects are configurable? (Choose three)

- A. HIP objects
- B. QoS profiles
- C. interface management profiles
- D. certificate profiles
- E. security profiles

**Answer:** ACE

#### NEW QUESTION 200

- (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 204

- (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 208

- (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 210

- (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](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 214**

- (Exam Topic 2)

Which two actions would be part of an automatic solution that would block sites with untrusted certificates without enabling SSL Forward Proxy? (Choose two.)

- A. Create a no-decrypt Decryption Policy rule.
- B. Configure an EDL to pull IP addresses of known sites resolved from a CRL.
- C. Create a Dynamic Address Group for untrusted sites
- D. Create a Security Policy rule with vulnerability Security Profile attached.
- E. Enable the "Block sessions with untrusted issuers" setting.

**Answer:** DE

**NEW QUESTION 219**

- (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 224**

- (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 228**

- (Exam Topic 2)

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 interfaced 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:** D

**Explanation:**

"By default, the firewall uses management interface to communicate to various servers including DNS, Email, Palo Alto Updates, User-ID agent, Syslog, Panorama etc. Service routes are used so that the communication between the firewall and servers go through the dataplane." <https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIGJCA0>

"The firewall uses the service route to connect to the Update Server and checks for new content release versions and, if there are updates available, displays them at the top of the list." <https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-web-interface-help/device/device-dynamic-updates#>

**NEW QUESTION 229**

- (Exam Topic 2)

When backing up and saving configuration files, what is achieved using only the firewall and is not available in Panorama?

- A. Load named configuration snapshot
- B. Load configuration version
- C. Save candidate config
- D. Export device state

**Answer:** D

#### NEW QUESTION 230

- (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 234

- (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 235

- (Exam Topic 2)

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

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

**Answer:** C

#### Explanation:

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

#### NEW QUESTION 240

- (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 243

- (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 244**

- (Exam Topic 3)

Which two actions are required to make Microsoft Active Directory users appear in a firewall traffic log? (Choose two.)

- A. Run the User-ID Agent using an Active Directory account that has "event log viewer" permissions
- B. Enable User-ID on the zone object for the destination zone
- C. Run the User-ID Agent using an Active Directory account that has "domain administrator" permissions
- D. Enable User-ID on the zone object for the source zone
- E. Configure a RADIUS server profile to point to a domain controller

**Answer:** AD

**NEW QUESTION 248**

- (Exam Topic 3)

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 253**

- (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 254**

- (Exam Topic 3)

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

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

IMAP , POP3 , SMTP - > Alert  
HTTP,FTP,SMB -> Reset-both

**NEW QUESTION 259**

- (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 262**

- (Exam Topic 3)

A network Administrator needs to view the default action for a specific spyware signature. The administrator follows the tabs and menus through Objects> Security Profiles> Anti-Spyware and select default profile.

What should be done next?

- A. Click the simple-critical rule and then click the Action drop-down list.
- B. Click the Exceptions tab and then click show all signatures.
- C. View the default actions displayed in the Action column.
- D. Click the Rules tab and then look for rules with "default" in the Action column.

**Answer:** B

**NEW QUESTION 267**

- (Exam Topic 3)

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

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

**Answer:** D

**NEW QUESTION 268**

- (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 271**

- (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 273**

- (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 275**

- (Exam Topic 3)

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 279**

- (Exam Topic 3)

Which Panorama feature allows for logs generated by Panorama to be forwarded to an external Security Information and Event Management(SIEM) system?

- A. Panorama Log Settings
- B. Panorama Log Templates
- C. Panorama Device Group Log Forwarding
- D. Collector Log Forwarding for Collector Groups

**Answer:** A

**Explanation:**

[https://www.paloaltonetworks.com/documentation/61/panorama/panorama\\_adminguide/manage-log-collection/e](https://www.paloaltonetworks.com/documentation/61/panorama/panorama_adminguide/manage-log-collection/e)

**NEW QUESTION 284**

- (Exam Topic 3)

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

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

**Answer:** ABC

**Explanation:**

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

**NEW QUESTION 289**

- (Exam Topic 3)

The IT department has received complaints about VoIP call jitter when the sales staff is making or receiving calls. QoS is enabled on all firewall interfaces, but there is no QoS policy written in the rulebase. The IT manager wants to find out what traffic is causing the jitter in real time when a user reports the jitter. Which feature can be used to identify, in real time, the applications taking up the most bandwidth?

- A. QoS Statistics
- B. Applications Report
- C. Application Command Center (ACC)
- D. QoS Log

**Answer:** A

**NEW QUESTION 294**

- (Exam Topic 3)

A network engineer has revived a report of problems reaching 98.139.183.24 through vr1 on the firewall. The routing table on this firewall is extensive and complex.

Which CLI command will help identify the issue?

- A. test routing fib virtual-router vr1
- B. show routing route type static destination 98.139.183.24
- C. test routing fib-lookup ip 98.139.183.24 virtual-router vr1
- D. show routing interface

**Answer:** C



#### NEW QUESTION 295

- (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 300

- (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 304

- (Exam Topic 3)

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

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

**Answer:** B

#### NEW QUESTION 305

- (Exam Topic 3)

A critical US-CERT notification is published regarding a newly discovered botnet. The malware is very evasive and is not reliably detected by endpoint antivirus software. Furthermore, SSL is used to tunnel malicious traffic to command-and-control servers on the internet and SSL Forward Proxy Decryption is not enabled. Which component once enabled on a perimeter firewall will allow the identification of existing infected hosts in an environment?

- A. Anti-Spyware profiles applied outbound security policies with DNS Query action set to sinkhole
- B. File Blocking profiles applied to outbound security policies with action set to alert
- C. Vulnerability Protection profiles applied to outbound security policies with action set to block
- D. Antivirus profiles applied to outbound security policies with action set to alert

**Answer:** A

#### NEW QUESTION 309

- (Exam Topic 3)

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

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

**Answer:** ABF

#### NEW QUESTION 310

- (Exam Topic 3)

What will be the source address in the ICMP packet?

- A. 10.30.0.93
- B. 10.46.72.93
- C. 10.46.64.94
- D. 192.168.93.1

**Answer:** C

#### NEW QUESTION 312

- (Exam Topic 3)

What must be used in Security Policy Rule that contain addresses where NAT policy applies?

- A. Pre-NAT addresse and Pre-NAT zones
- B. Post-NAT addresse and Post-Nat zones
- C. Pre-NAT addresse and Post-Nat zones
- D. Post-Nat addresses and Pre-NAT zones

**Answer:** C

#### NEW QUESTION 316

- (Exam Topic 3)

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

Which interface type and configuration setting will support this design?

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

**Answer:** D

#### NEW QUESTION 317

- (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 319

- (Exam Topic 3)

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 321

- (Exam Topic 3)

Which CLI command displays the current management plan memory utilization?

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

**Answer:** B

#### Explanation:

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

#### NEW QUESTION 324

- (Exam Topic 3)

Which operation will impact performance of the management plane?

- A. DoS protection
- B. WildFire submissions
- C. generating a SaaS Application report
- D. decrypting SSL sessions

**Answer:** C

#### NEW QUESTION 329

- (Exam Topic 3)

Starting with PAN-OS version 9.1, application dependency information is now reported in which new locations? (Choose two.)

- A. On the App Dependency tab in the Commit Status window
- B. On the Application tab in the Security Policy Rule creation window
- C. On the Objects > Applications browsers pages
- D. On the Policy Optimizer's Rule Usage page

**Answer:** AB

#### NEW QUESTION 330

- (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 335

- (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 336

- (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 341

- (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 346

- (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 350

- (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 353

.....

## 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/>