

## PCNSE Dumps

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

<https://www.certleader.com/PCNSE-dumps.html>



**NEW QUESTION 1**

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 2**

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

The screenshot shows the 'External Dynamic Lists' configuration window. The 'Name' field is 'TORexitNodes-MM'. The 'Type' is 'IP List'. The 'Source' is 'https://MineMeld/feeds/TORexitOut'. The 'Server Authentication' section shows 'Certificate Profile' set to 'None (Disable Cert profile)'. The 'Repeat' interval is 'Hourly'. There are buttons for 'Test Source URL', 'OK', and 'Cancel'.

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

**Answer:** D

**NEW QUESTION 3**

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

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

**Answer:** AC

**NEW QUESTION 4**

Which administrative authentication method supports authorization by an external service?

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

**Answer:** C

**NEW QUESTION 5**

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 6

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

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

**Answer:** B

#### NEW QUESTION 7

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:** AD

#### NEW QUESTION 8

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-7000-series-layer-2-interface#idd2bcaacc-54b9-4ec9-a1dd-8064499f5b9d>

#### 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

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-globalprotect-portals>

#### NEW QUESTION 10

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

- A. The settings assigned to the template that is on top of the stack.
- B. The administrator will be prompted to choose the settings for that chosen firewall.
- C. All the settings configured in all templates.

D. Depending on the firewall location, Panorama decides with settings to send.

**Answer:** B

**Explanation:**

Reference:

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

**NEW QUESTION 11**

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://www.paloaltonetworks.com/documentation/80/pan-os/pan-os-policy/register-ip-addresses-and-tags-dynamically>

**NEW QUESTION 13**

Which two virtualization platforms officially support the deployment of Palo Alto Networks VM- Series firewalls? (Choose two.)

- A. Red Hat Enterprise Virtualization (RHEV)
- B. Kernel Virtualization Module (KVM)
- C. Boot Strap Virtualization Module (BSVM)
- D. Microsoft Hyper-V

**Answer:** BD

**Explanation:**

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

**NEW QUESTION 15**

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

- A. web-browsing and 443
- B. SSL and 80
- C. SSL and 443
- D. web-browsing and 80

**Answer:** A

**NEW QUESTION 19**

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

**NEW QUESTION 23**

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 28**

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 29

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 32

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 33

An administrator creates a custom application containing Layer 7 signatures. The latest application and threat dynamic update is downloaded to the same NGFW. The update contains an application that matches the same traffic signatures as the custom application. Which application should be used to identify traffic traversing the NGFW?

- A. Custom application
- B. System logs show an application error and neither signature is used.
- C. Downloaded application
- D. Custom and downloaded application signature files are merged and both are used

**Answer:** A

#### NEW QUESTION 38

Refer to the exhibit.



```
#####
```

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

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

```
#####
```

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

```
total virtual-wire shown:
```

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

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

```
#####
```

Which will be the egress interface if the traffic's ingress interface is ethernet 1/7 sourcing from 192.168.111.3 and to the destination 10.46.41.113?

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

**Answer:** D

#### NEW QUESTION 40

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:** DEF

#### NEW QUESTION 45

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 49

A client is concerned about resource exhaustion because of denial-of-service attacks against their DNS servers. Which option will protect the individual servers?

- A. Enable packet buffer protection on the Zone Protection Profile.
- B. Apply an Anti-Spyware Profile with DNS sinkholing.
- C. Use the DNS App-ID with application-default.
- D. Apply a classified DoS Protection Profile.

**Answer:** A

**NEW QUESTION 54**

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 57**

An administrator creates an SSL decryption rule decrypting traffic on all ports. The administrator also creates a Security policy rule allowing only the applications DNS, SSL, and web-browsing.

The administrator generates three encrypted BitTorrent connections and checks the Traffic logs. There are three entries. The first entry shows traffic dropped as application Unknown. The next two entries show traffic allowed as application SSL.

Which action will stop the second and subsequent encrypted BitTorrent connections from being allowed as SSL?

- A. Create a decryption rule matching the encrypted BitTorrent traffic with action “No-Decrypt,” and place the rule at the top of the Decryption policy.
- B. Create a Security policy rule that matches application “encrypted BitTorrent” and place the rule at the top of the Security policy.
- C. Disable the exclude cache option for the firewall.
- D. Create a Decryption Profile to block traffic using unsupported cyphers, and attach the profile to the decryption rule.

**Answer:** D

**NEW QUESTION 60**

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 64**

An administrator has configured the Palo Alto Networks NGFW’s management interface to connect to the internet through a dedicated path that does not traverse back through the NGFW itself.

Which configuration setting or step will allow the firewall to get automatic application signature updates?

- A. A scheduler will need to be configured for application signatures.
- B. A Security policy rule will need to be configured to allow the update requests from the firewall to the update servers.
- C. A Threat Prevention license will need to be installed.
- D. A service route will need to be configured.

**Answer:** D

**Explanation:**

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.

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/device/device-dynamic-updates>

**NEW QUESTION 67**

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 71**

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-amp-Tricks-How-to-Use-the-Application-Command-Center-ACC/ta-p/67342>

**NEW QUESTION 74**

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

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

**Answer:** ADE

**Explanation:**

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

**NEW QUESTION 77**

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 82**

An administrator has been asked to create 100 virtual firewalls in a local, on-premise lab environment (not in “the cloud”). Bootstrapping is the most expedient way to perform this task. Which option describes deployment of a bootstrap package in an on-premise virtual environment?

- A. Use config-drive on a USB stick.
- B. Use an S3 bucket with an ISO.
- C. Create and attach a virtual hard disk (VHD).
- D. Use a virtual CD-ROM with an ISO.

**Answer:** D

**Explanation:**

Reference: <https://www.paloaltonetworks.com/documentation/71/pan-os/newfeaturesguide/management-features/bootstrapping-firewalls-for-rapid-deployment.html>

**NEW QUESTION 85**

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:** ABC

**Explanation:**

Reference: <https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/decryption/create-a-decryption-profile>

**NEW QUESTION 86**



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 90

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

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

**Answer:** A

**Explanation:**

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

#### NEW QUESTION 95

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:** BD

**Explanation:**

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

#### NEW QUESTION 100

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 102

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 105

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

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

**Answer:** A

**NEW QUESTION 110**

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 112**

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 116**

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 120**

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 124**

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 128**

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

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

**Answer:** BCEF

**NEW QUESTION 129**

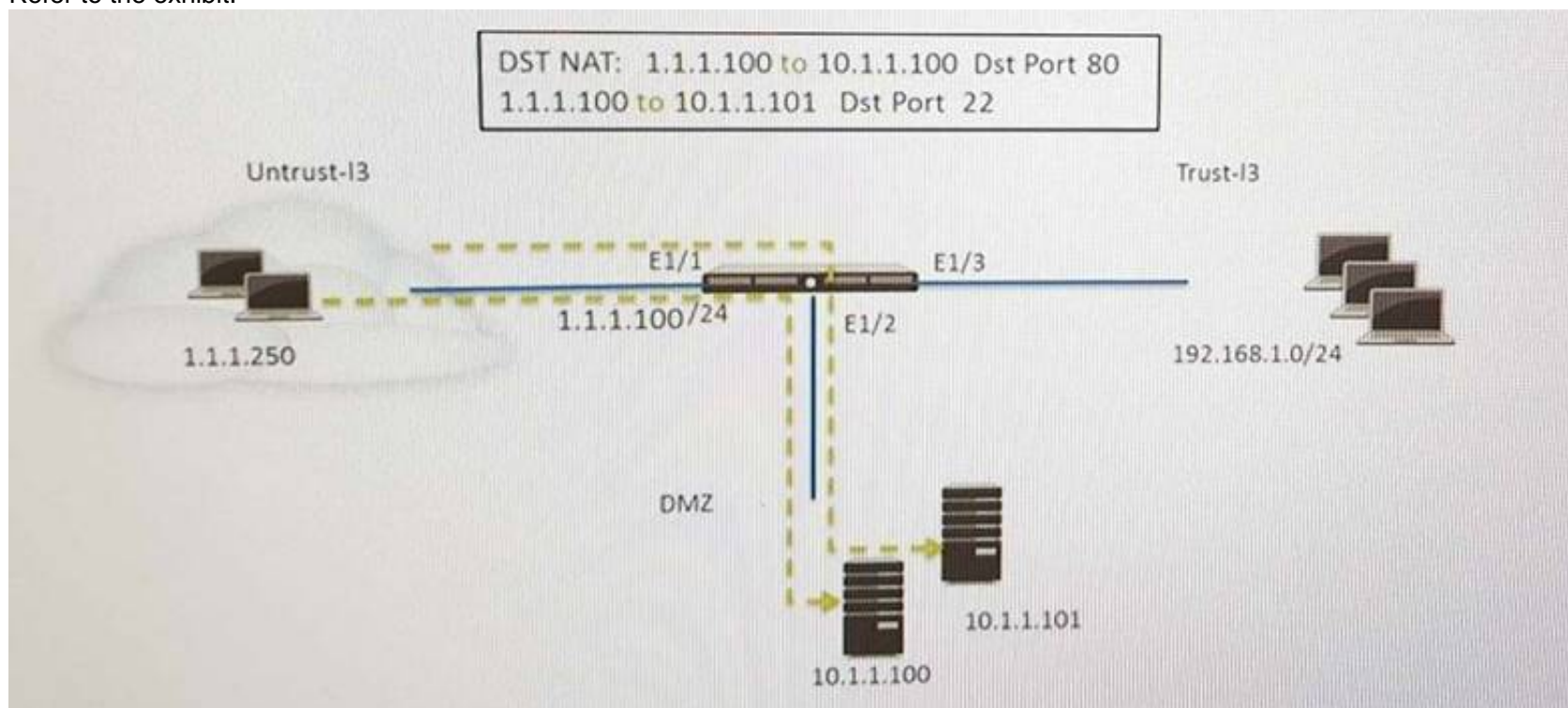
Which log file can be used to identify SSL decryption failures?

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

**Answer: C**

#### NEW QUESTION 134

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 135

An administrator has configured a QoS policy rule and a QoS profile that limits the maximum allowable bandwidth for the YouTube application. However, YouTube is consuming more than the maximum bandwidth allotment configured. Which configuration step needs to be configured to enable QoS?

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

**Answer: C**

#### NEW QUESTION 136

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 141

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: A**

#### NEW QUESTION 146

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**

#### NEW QUESTION 150

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 152

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 156

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

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

**Answer: B**

#### NEW QUESTION 160

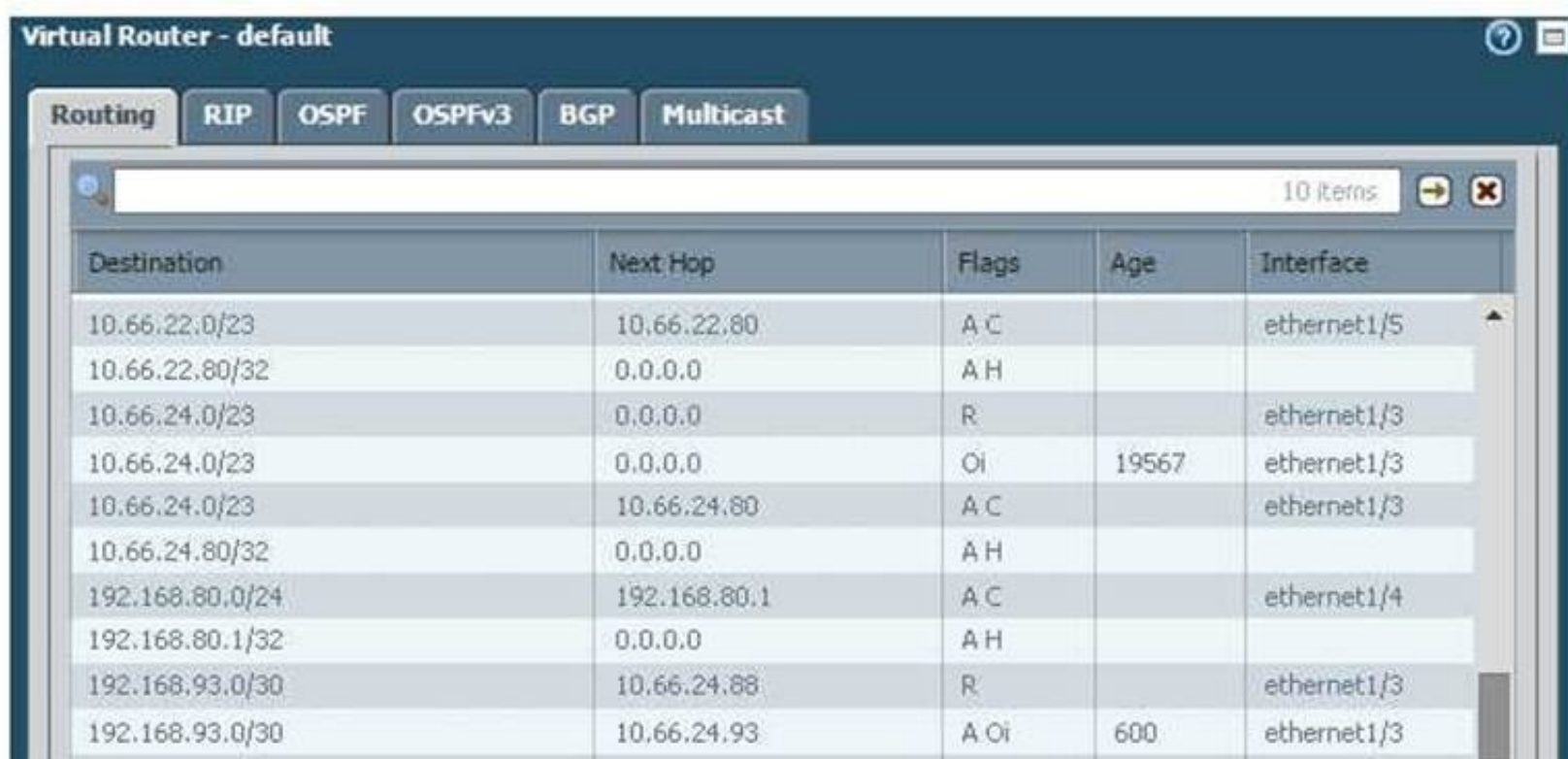
A host attached to Ethernet 1/4 cannot ping the default gateway. The widget on the dashboard shows Ethernet 1/1 and Ethernet 1/4 to be green. The IP address of Ethernet 1/1 is 192.168.1.7 and the IP address of Ethernet 1/4 is 10.1.1.7. The default gateway is attached to Ethernet 1/1. A default route 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 161

Given the following table.



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 163**

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 167**

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

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

**Answer:** BC

**Explanation:**

([httpHYPERLINK "https://live.paloaltonetworks.com/t5/Management-Articles/Panorama-Sizing-and-Design-Guide/ta-p/72181"s://live.paloaltonetworks.com/t5/Management-Articles/Panorama-Sizing- and-Design-Guide/ta-p/72181](https://live.paloaltonetworks.com/t5/Management-Articles/Panorama-Sizing-and-Design-Guide/ta-p/72181))

**NEW QUESTION 168**

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 169**

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 170**

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 173**

How is the Forward Untrust Certificate used?

- A. It issues certificates encountered on the Untrust security zone when clients attempt to connect to a site that has be decrypted/
- B. It is used when web servers request a client certificate.
- C. It is presented to clients when the server they are connecting to is signed by a certificate authority that is not trusted by firewall.
- D. It is used for Captive Portal to identify unknown users.

**Answer:** C

**NEW QUESTION 175**

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"les/File-Blocking-RulebHYPERLINK "https://live.paloaltonetworks.com/t5/Configuration-Articles/File-Blocking-Rulebase-and-Action-Precedence/ta-p/53623"ase-and-Action-Precedence/ta-p/53623

**NEW QUESTION 177**

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 178**

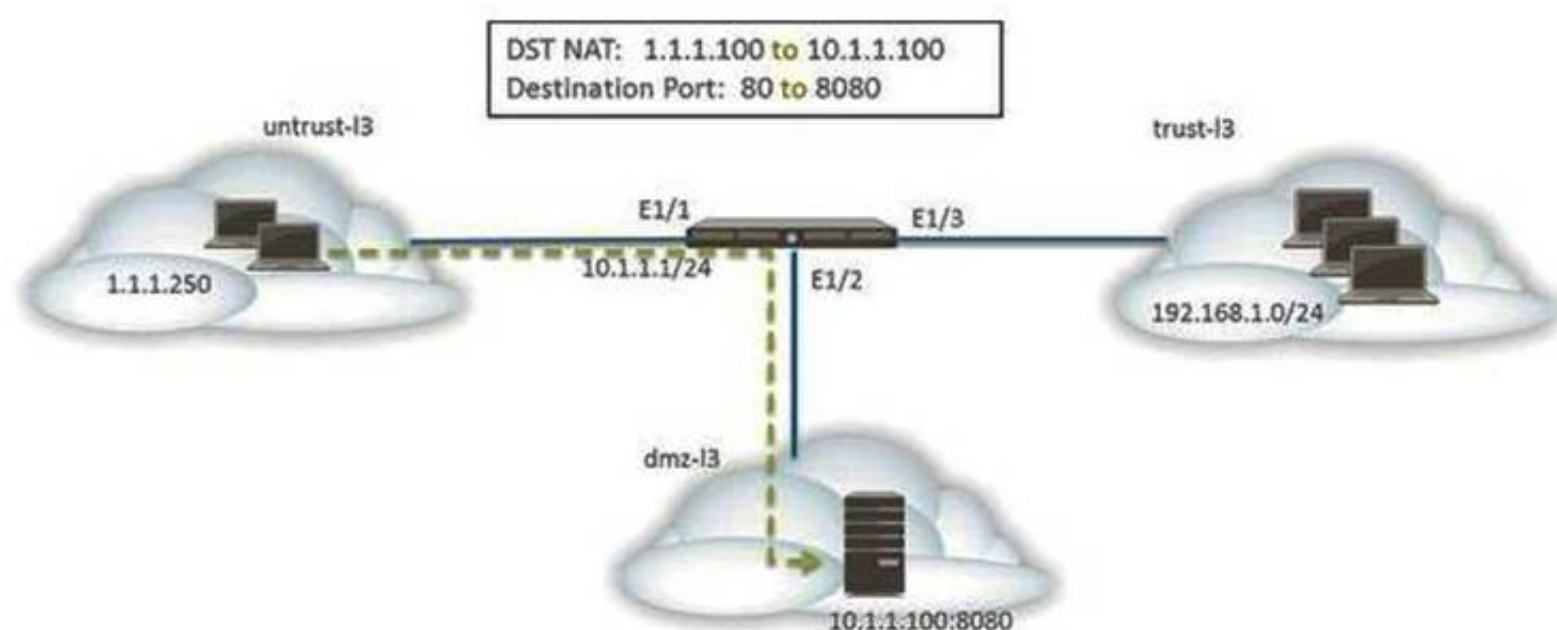
Which three options are available when creating a security profile? (Choose three)

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

**Answer:** ABF

**NEW QUESTION 181**

The web server is configured to listen for HTTP traffic on port 8080. The clients access the web server using the IP address 1.1.1.100 on TCP Port 80. The destination NAT rule is configured to translate both IP address and port to 10.1.1.100 on TCP Port 8080.



Which NAT and security rules must be configured on the firewall? (Choose two)

- A. A security policy with a source of any from untrust-l3 Zone to a destination of 10.1.1.100 in dmz-l3 zone using web-browsing application
- B. A NAT rule with a source of any from untrust-l3 zone to a destination of 10.1.1.100 in dmz-zone using service-http service.
- C. A NAT rule with a source of any from untrust-l3 zone to a destination of 1.1.1.100 in untrust-l3 zone using service-http service.
- D. A security policy with a source of any from untrust-l3 zone to a destination of 1.1.100 in dmz-l3 zone using web-browsing application.

**Answer:** BD

**NEW QUESTION 185**

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 187

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 191

What can missing SSL packets when performing a packet capture on dataplane interfaces?

A. The packets are hardware offloaded to the offloaded processor on the dataplane

B. The missing packets are offloaded to the management plane CPU

C. The packets are not captured because they are encrypted

D. There is a hardware problem with offloading FPGA on the management plane

**Answer:** A

#### NEW QUESTION 196

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	int-Trust-L3	any	any	int-UnTrust-L3	any	Known Good	application-default	allow	log	
2	rule2	int-Trust-L3	any	any	int-UnTrust-L3	any	Known Bad	any	deny	none	
3	rule3	int-Trust-L3	any	any	int-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 198

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 201

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 202

Firewall administrators cannot authenticate to a firewall GUI.

Which two logs on that firewall will contain authentication-related information useful in troubleshooting this issue? (Choose two.)

A. ms log

B. authd log

C. System log

- D. Traffic log
- E. dp-monitor .log

**Answer:** BC

#### NEW QUESTION 205

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 209

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 211

What are two prerequisites for configuring a pair of Palo Alto Networks firewalls in an active/passive High Availability (HA) pair? (Choose two.)

- A. The firewalls must have the same set of licenses.
- B. The management interfaces must to be on the same network.
- C. The peer HA1 IP address must be the same on both firewalls.
- D. HA1 should be connected to HA1. Either directly or with an intermediate Layer 2 device.

**Answer:** AD

#### NEW QUESTION 213

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 216

A network design change requires an existing firewall to start accessing Palo Alto Updates from a data plane interface address instead of the management interface.

Which configuration setting needs to be modified?

- A. Service route
- B. Default route
- C. Management profile
- D. Authentication profile

**Answer:** A

#### NEW QUESTION 217

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 221

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 225

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 229

A network security engineer has a requirement to allow an external server to access an internal web server. The internal web server must also initiate connections with the external server.

What can be done to simplify the NAT policy?

- A. Configure ECMP to handle matching NAT traffic
- B. Configure a NAT Policy rule with Dynamic IP and Port
- C. Create a new Source NAT Policy rule that matches the existing traffic and enable the Bi-directional option
- D. Create a new Destination NAT Policy rule that matches the existing traffic and enable the Bi-directional option

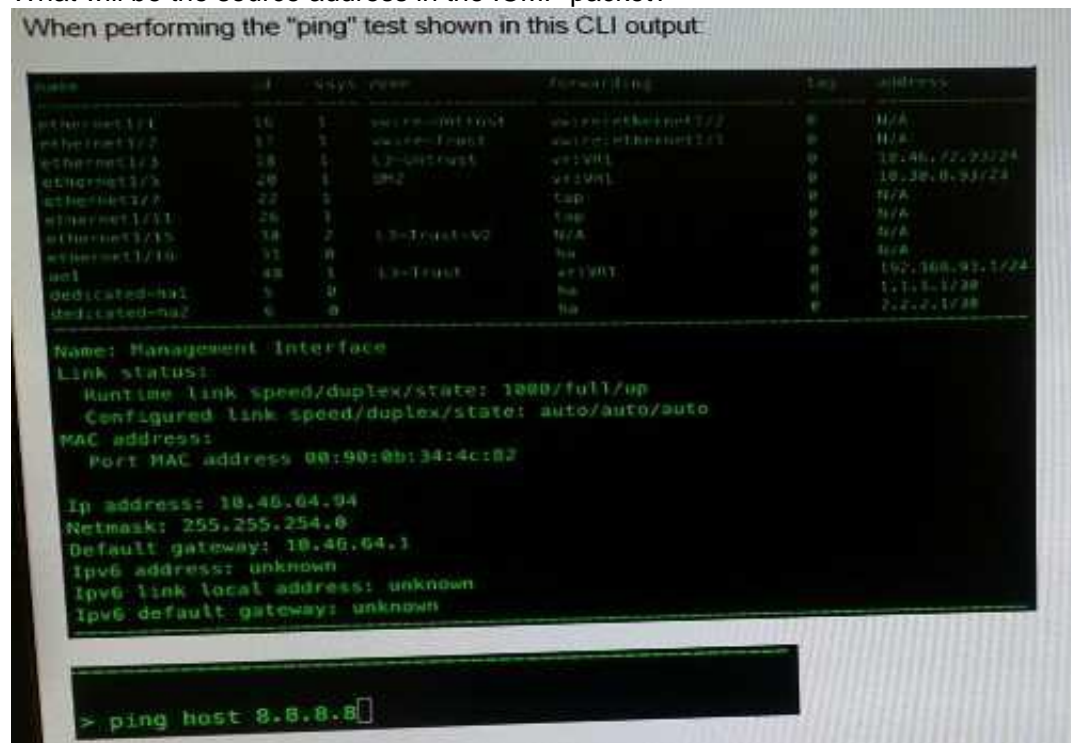
**Answer: C**

#### Explanation:

<https://www.paloaltonetworks.com/documentation/70/pan-os/pan-os/networking/nat-configuration-examples>

#### NEW QUESTION 230

What will be the source address in the ICMP packet?





**NEW QUESTION 237**

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

What should be done first?

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

**Answer: C**

**NEW QUESTION 240**

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 243**

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

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

**Answer: B**

**NEW QUESTION 247**

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

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

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

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

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

Which setting for class 6 with throttle YouTube traffic?

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

**Answer: D**

**NEW QUESTION 248**

.....



## Thank You for Trying Our Product

\* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

\* One year free update

You can enjoy free update one year. 24x7 online support.

\* Trusted by Millions

We currently serve more than 30,000,000 customers.

\* Shop Securely

All transactions are protected by VeriSign!

**100% Pass Your PCNSE Exam with Our Prep Materials Via below:**

<https://www.certleader.com/PCNSE-dumps.html>