

# Paloalto-Networks

## Exam Questions PCNSE

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



**NEW QUESTION 1**

Which three split tunnel methods are supported by a globalProtect gateway? (Choose three.)

- A. video streaming application
- B. Client Application Process
- C. Destination Domain
- D. Source Domain
- E. Destination user/group
- F. URL Category

**Answer:** ABC

**NEW QUESTION 2**

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

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

**Answer:** D

**NEW QUESTION 3**

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

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

**Answer:** A

**NEW QUESTION 4**

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

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

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

**Answer:** C

**NEW QUESTION 5**

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 6**

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 7**

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 8**

An administrator accidentally closed the commit window/screen before the commit was finished. Which two options could the administrator use to verify the progress or success of that commit task? (Choose two.)

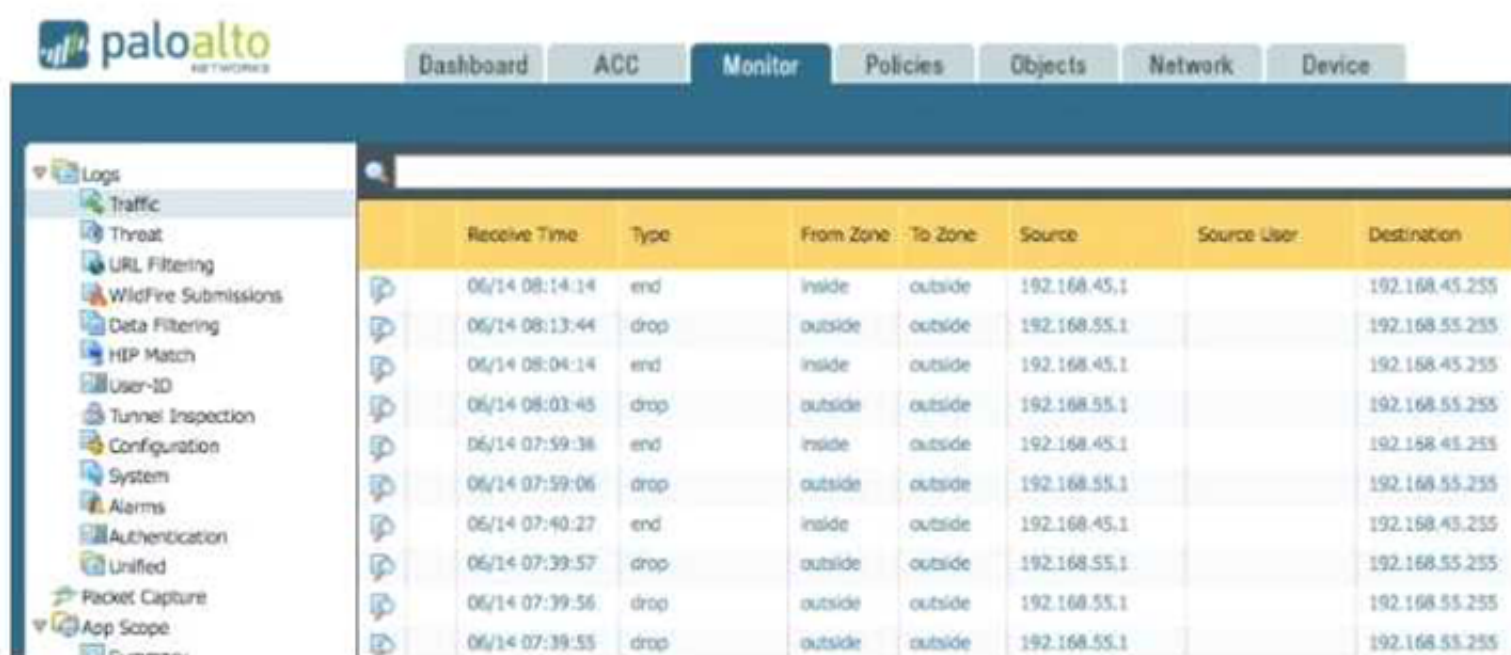
A



The screenshot shows the Palo Alto Networks management interface, specifically the 'Monitor' tab. On the left is a sidebar with a 'Logs' section expanded, showing various log categories like Traffic, Threat, URL Filtering, etc. The main area displays a table of log entries. The table has columns for 'Receive Time', 'Type', 'Severity', 'Event', 'Object', and 'Description'. The logs show a sequence of events including user logins, database upgrades, and a successful commit operation.

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

B

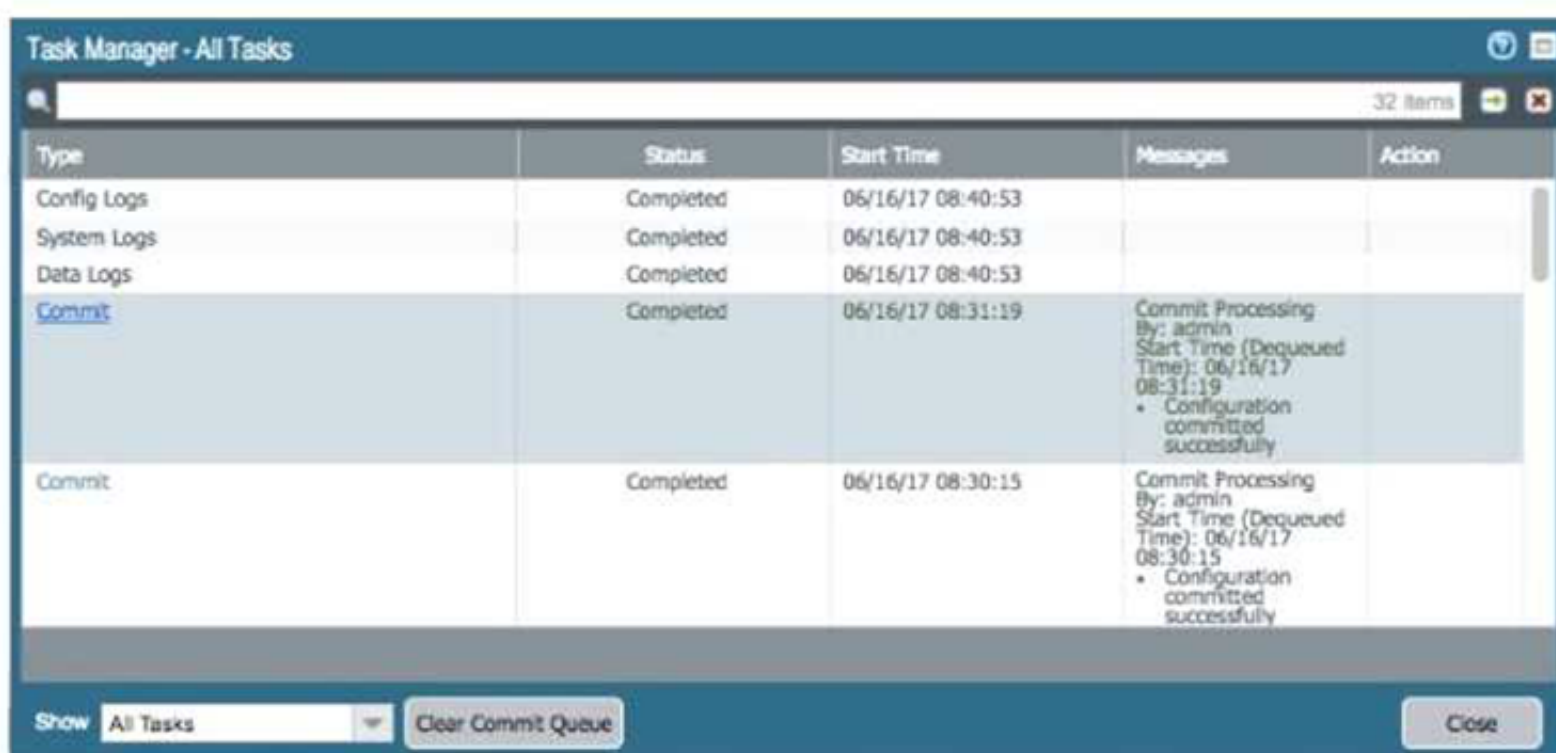


	Receive Time	Type	From Zone	To Zone	Source	Source User	Destination
	06/14 08:14:14	end	inside	outside	192.168.45.1		192.168.45.255
	06/14 08:13:44	drop	outside	outside	192.168.55.1		192.168.55.255
	06/14 08:04:14	end	inside	outside	192.168.45.1		192.168.45.255
	06/14 08:03:45	drop	outside	outside	192.168.55.1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

C

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

D



Type	Status	Start Time	Messages	Action
Config Logs	Completed	06/16/17 08:40:53		
System Logs	Completed	06/16/17 08:40:53		
Data Logs	Completed	06/16/17 08:40:53		
Commit	Completed	06/16/17 08:31:19	Commit Processing By: admin Start Time (Dequeued Time): 06/16/17 08:31:19 • Configuration committed successfully	
Commit	Completed	06/16/17 08:30:15	Commit Processing By: admin Start Time (Dequeued Time): 06/16/17 08:30:15 • Configuration committed successfully	

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

**Answer: AD**

#### NEW QUESTION 9

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

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

**Answer: C**

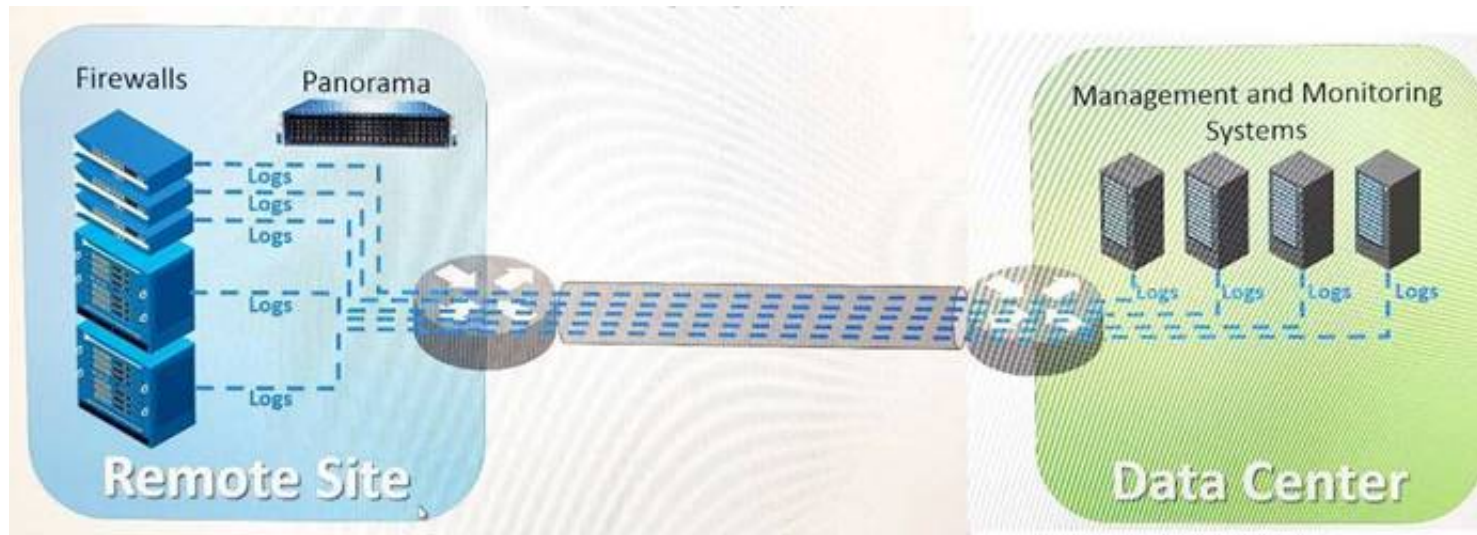
#### Explanation:

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

#### NEW QUESTION 10

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

#### NEW QUESTION 10

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 11

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

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 14

A company needs to preconfigure firewalls to be sent to remote sites with the least amount of reconfiguration. Once deployed, each firewall must establish secure tunnels back to multiple regional data centers to include the future regional data centers. Which VPN configuration would adapt to changes when deployed to the future site?

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

**Answer:** A

#### NEW QUESTION 15

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



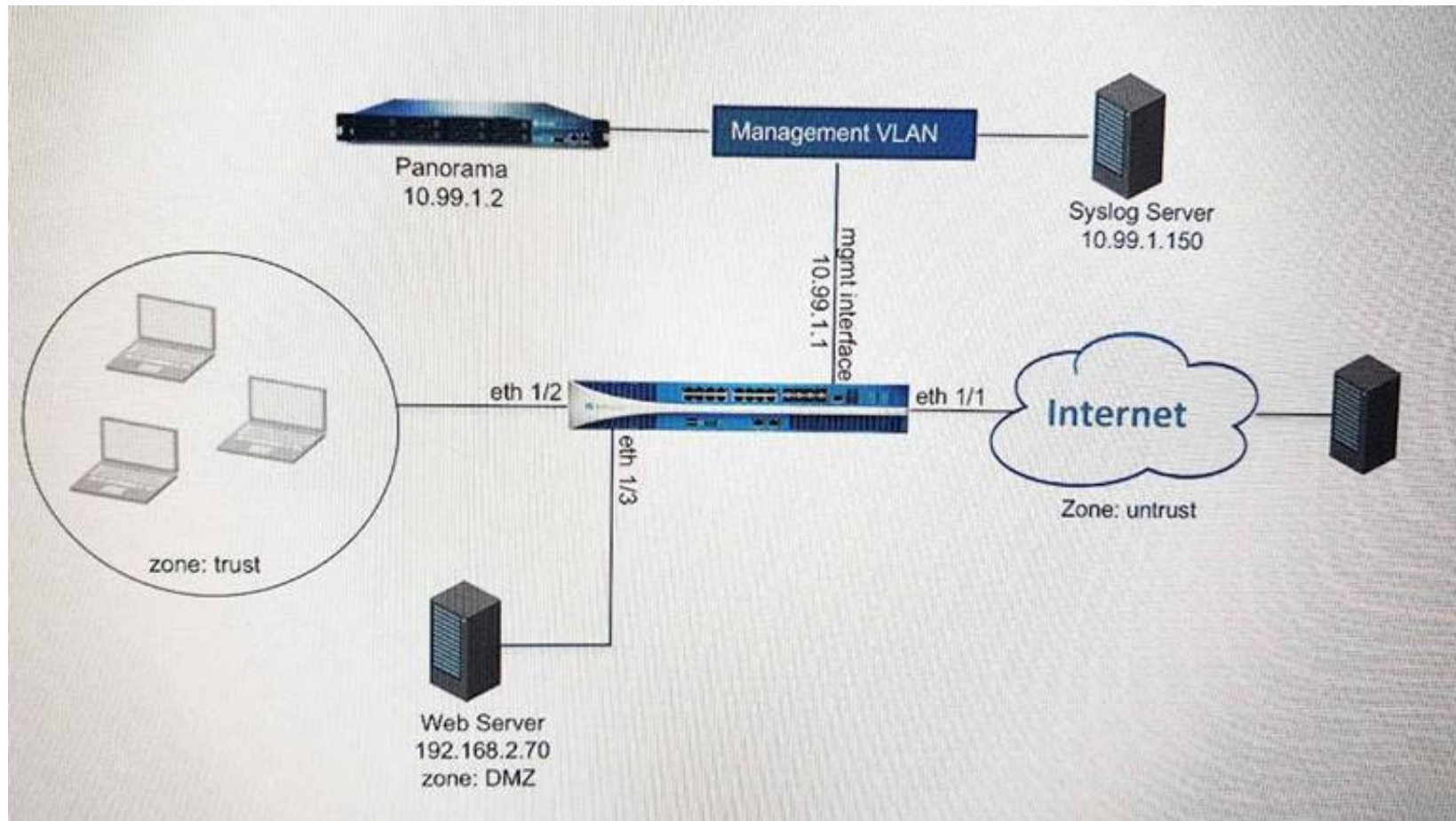
**Explanation:**

Reference:

[https://www.paloaltonetworks.com/content/dam/pan/en\\_US/assets/pdf/frame-maker/71/pan-os/pan-os/section\\_5.pdf](https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/frame-maker/71/pan-os/pan-os/section_5.pdf) (page 9)

**NEW QUESTION 18**

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)

**Panorama Settings**

**Panorama Servers**

10.99.1.21

Receive Timeout for Connection to Panorama (sec)	240
Send Timeout for Connection to Panorama (sec)	240
Retry Count for SSL Send to Panorama	25

☐ **Secure Client Communication**

Certificate Type: None

☐ Check Server Identity

B)



Security Policy Rule

General

Source

User

Destination

Application

Service/URL Category

Actions

Action Setting

Action

Allow

Send ICMP Unreachable

Profile Setting

Profile Type

Profiles

Antivirus

None

Vulnerability Protection

None

Anti-Spyware

None

URL Filtering

Filter1

File Blocking

None

Data Filtering

None

WildFire Analysis

None

Log Setting

Log at Session Start

☒

Log at Session End

☒

Log Forwarding

None

Other Settings

Schedule

None

QoS Marking

None

Disable Server Response Inspection

☐

OK

Cancel

C)

Syslog Server Profile

Name

SyslogProfile1

Servers

Custom Log Format

Name	Syslog Server	Transport	Port	Format	Facility
SyslogServer1	192.168.229.17	UDP	514	BSD	LOG_USER

Add

Delete

D)



**Panorama Settings**

Receive Timeout for Connection to Device (sec) 240

Send Timeout for Connection to Device (sec) 240

Retry Count for SSL Send to Device 25

☒ Share Unused Address and Service Objects with Devices

☐ Objects defined in ancestors will take higher precedence

**Secure Server Communication**

☐ Custom Certificate Only

SSL/TLS Service Profile None

Certificate Profile None

Authorization List

Identifier	Type	Value
0 items		

☐ Authorize Clients Based on Serial Number

☐ Check Authorization List

Connect Wait Time (min) [0 - 44640]

OK

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

**Answer: D**

#### NEW QUESTION 21

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 which 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 24

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

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

**Answer: A**

#### Explanation:

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/decryption/configure-ssl-inbound-inspection>



#### NEW QUESTION 27

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 29

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 33

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:** BC

#### NEW QUESTION 36

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

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

**Answer:** C

#### NEW QUESTION 37

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 42

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

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

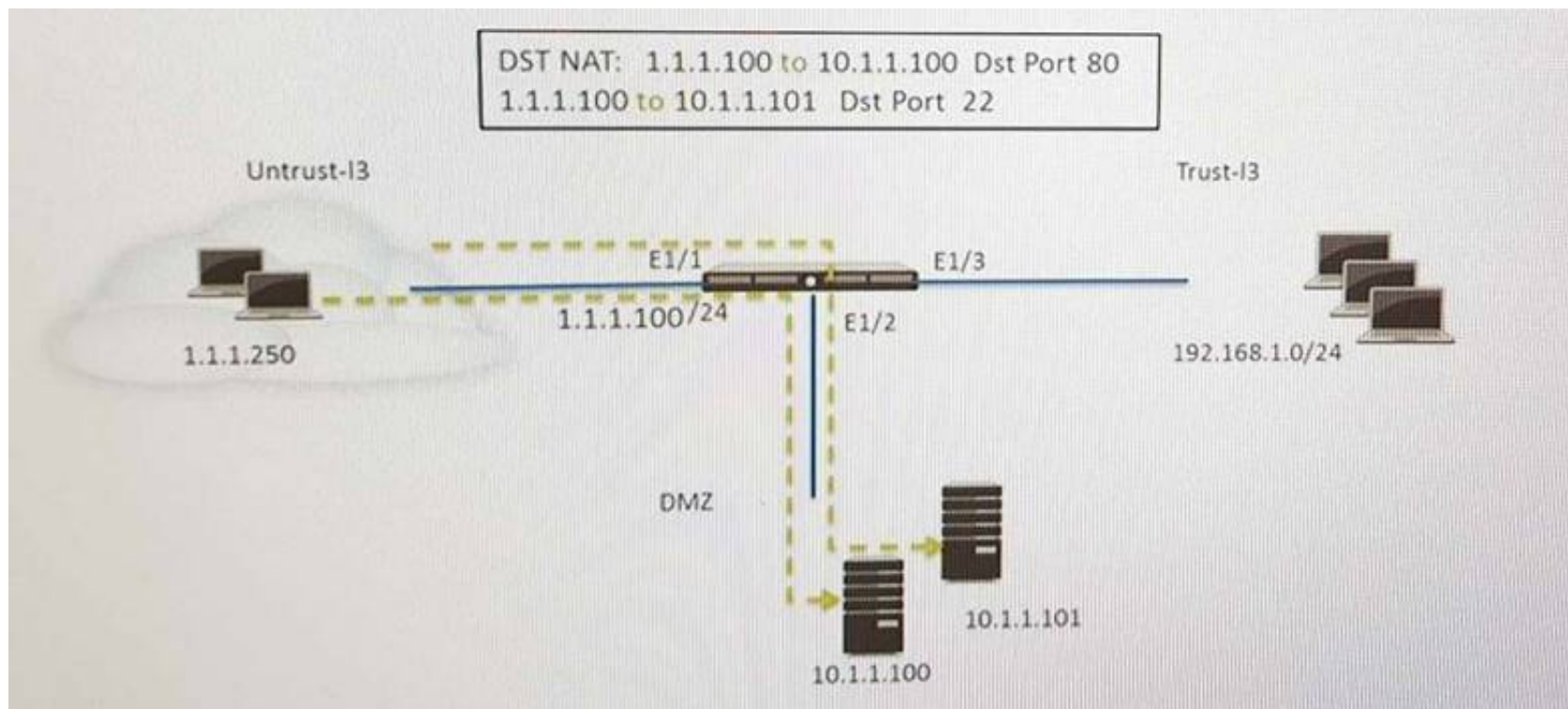
**Answer:** D

#### Explanation:

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

#### NEW QUESTION 43

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) receives 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), web-browsing -Allow
- B. Untrust (Any) to Untrust (10.1.1.1), ssh -Allow
- C. Untrust (Any) to DMZ (10.1.1.1), web-browsing -Allow
- D. Untrust (Any) to DMZ (10.1.1.1), ssh -Allow
- E. Untrust (Any) to DMZ (10.1.1.100.10.1.1.101), ssh, web-browsing -Allow

**Answer:** CD

#### NEW QUESTION 45

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:** ADE

#### NEW QUESTION 50

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

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

**Answer:** A

#### NEW QUESTION 51

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 54

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 58**

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

- A. dll
- B. exe
- C. src
- D. apk
- E. pdf
- F. jar

**Answer:** DEF

**Explanation:**

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

**NEW QUESTION 63**

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 64**

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 69**

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

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

**NEW QUESTION 73**

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 77**

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-ssltls-service-profile>

**NEW QUESTION 81**

If an administrator does not possess a website's certificate, which SSL decryption mode will allow the Palo Alto networks NGFW to inspect when users browse to HTTP(S) websites?

- A. SSL Forward Proxy
- B. SSL Inbound Inspection
- C. TLS Bidirectional proxy
- D. SSL Outbound Inspection

**Answer:** A

**NEW QUESTION 85**

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

Which option would achieve this result?

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

**Answer:** A

**NEW QUESTION 86**

The administrator has enabled BGP on a virtual router on the Palo Alto Networks NGFW, but new routes do not seem to be populating the virtual router. Which two options would help the administrator troubleshoot this issue? (Choose two.)

- A. View the System logs and look for the error messages about BGP.
- B. Perform a traffic pcap on the NGFW to see any BGP problems.
- C. View the Runtime Stats and look for problems with BGP configuration.
- D. View the ACC tab to isolate routing issues.

**Answer:** CD

**NEW QUESTION 91**

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

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

**Answer:** AB

**NEW QUESTION 94**

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 96**

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 99**

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
```

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

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

Answer: D

NEW QUESTION 101

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

- A. The firewall is in multi-vsyz mode.
- B. The traffic is offloaded.
- C. The traffic does not match the packet capture filter.
- D. The firewall's DP CPU is higher than 50%.

Answer: BC

Explanation:

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

NEW QUESTION 105

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

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

Answer: D

Explanation:

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

NEW QUESTION 106

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 108**

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 112**

Which feature can be configured on VM-Series firewalls?

- A. aggregate interfaces
- B. machine learning
- C. multiple virtual systems
- D. GlobalProtect

**Answer:** D

**NEW QUESTION 114**

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 117**

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

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

**Answer:** A

**NEW QUESTION 118**

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 120**

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 122**

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

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

**Answer:** ADF

**NEW QUESTION 123**

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 127**

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

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

**Answer:** AC

**NEW QUESTION 128**

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

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

**Answer:** ADE

**Explanation:**

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

**NEW QUESTION 131**

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

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

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

**NEW QUESTION 135**

A customer wants to set up a site-to-site VPN using tunnel interfaces? Which two formats are correct for naming tunnel interfaces? (Choose two.)

- A. Vpn-tunnel.1024
- B. vpn-tunne.1
- C. tunnel 1025
- D. tunne

E. 1

**Answer:** CD

#### NEW QUESTION 137

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 141

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 144

Which three firewall states are valid? (Choose three)

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

**Answer:** ABC

#### NEW QUESTION 145

An administrator wants to upgrade an NGFW from PAN-OS® 7 .1. 2 to PAN-OS® 8 .0.2 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

#### NEW QUESTION 149

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

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

**Answer:** D

#### NEW QUESTION 150

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 155

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-IDidentification
- B. Use of a "service" enables the firewall to take immediate action with the first observed packet based on port numbers Use ofan "application" allows the firewall to take action after enough packets allow for App-ID identification regardless of the portsbeing used.
- C. There are no differences between "service" or "application" Use of an "application" simplifies configuration by allowing use ofa 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 ofan "application" allows the firewall to take immediate action it the port being used is a member of the application standardport list



Answer: B

#### NEW QUESTION 156

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 157

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 158

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 161

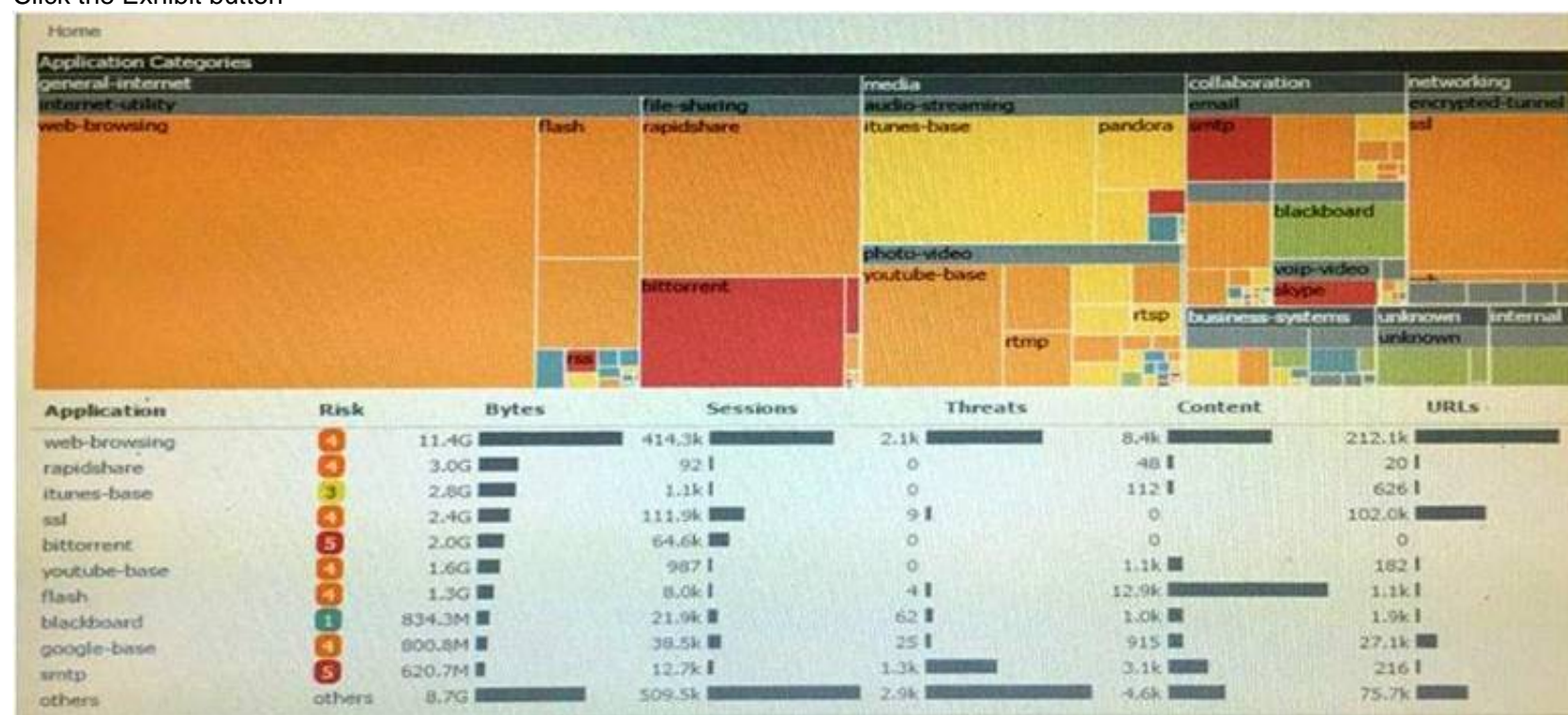
Which two mechanisms help prevent a split brain scenario an Active/Passive High Availability (HA) pair? (Choose two)

- 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 165

Click the Exhibit button



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

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

D. Click on the bittorrent application link to view network activity

**Answer: D**

#### NEW QUESTION 170

Which command can be used to validate a Captive Portal policy?

- A. eval captive-portal policy <criteria>
- B. request cp-policy-eval <criteria>
- C. test cp-policy-match <criteria>
- D. debug cp-policy <criteria>

**Answer: C**

#### NEW QUESTION 174

Which setting allow a DOS protection profile to limit the maximum concurrent sessions from a source IP address?

- A. Set the type to Aggregate, clear the session's box and set the Maximum concurrent Sessions to 4000.
- B. Set the type to Classified, clear the session's box and set the Maximum concurrent Sessions to 4000.
- C. Set the type Classified, check the Sessions box and set the Maximum concurrent Sessions to 4000.
- D. Set the type to aggregate, check the Sessions box and set the Maximum concurrent Sessions to 4000.

**Answer: C**

#### NEW QUESTION 177

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 181

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 186

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 190

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

less mp-log ikemgr.log:

```
less mp-log ikemgr.log:
```

```
2014-08-05 03:51:41 [INFO]: IPsec-SA request for 108.81.64.59 queued since no phase1 found
2014-08-05 03:51:41 [PROTO_NOTIFY]: <====> PHASE-1 NEGOTIATION STARTED AS INITIATOR, MAIN MODE <====
====> Initiated SA: 69.15.96.53[500]-108.81.64.59[500] cookie:09e85260f28f4e15:0000000000000000 <====
2014-08-05 03:52:33 [PROTO_NOTIFY]: <====> PHASE-1 NEGOTIATION FAILED AS INITIATOR, MAIN MODE <====
====> Failed SA: 69.15.96.53[500]-108.81.64.59[500] cookie:09e85260f28f4e15:0000000000000000 <==== Due to
timeout.
2014-08-05 03:52:33 [INFO]: <====> PHASE-1 SA DELETED <====
====> Deleted SA: 69.15.96.53[500]-108.81.64.59[500] cookie:09e85260f28f4e15:0000000000000000 <====
2014-08-05 03:53:02 [INFO]: IPsec-SA request for 108.81.64.59 queued since no phase1 found
2014-08-05 03:53:02 [PROTO_NOTIFY]: <====> PHASE-1 NEGOTIATION STARTED AS INITIATOR, MAIN MODE <====
====> Initiated SA: 69.15.96.53[500]-108.81.64.59[500] cookie:53351420a9a1aa47:0000000000000000 <====
2014-08-05 03:53:54 [PROTO_NOTIFY]: <====> PHASE-1 NEGOTIATION FAILED AS INITIATOR, MAIN MODE <====
====> Failed.SA: 69.15.96.53[500]-108.81.64.59[500] cookie:53351420a9a1aa47:0000000000000000 <==== Due to
timeout.
2014-08-05 03:53:54 [INFO]: <====> PHASE-1 SA DELETED <====
```

What could be the cause of this problem?

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

**Answer:** B

#### NEW QUESTION 195

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

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

**Answer:** D

#### Explanation:

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

#### NEW QUESTION 200

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

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 203

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 207

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

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

**Answer:** BD

#### NEW QUESTION 209



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 212

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

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

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

**Answer:** D

#### NEW QUESTION 214

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

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

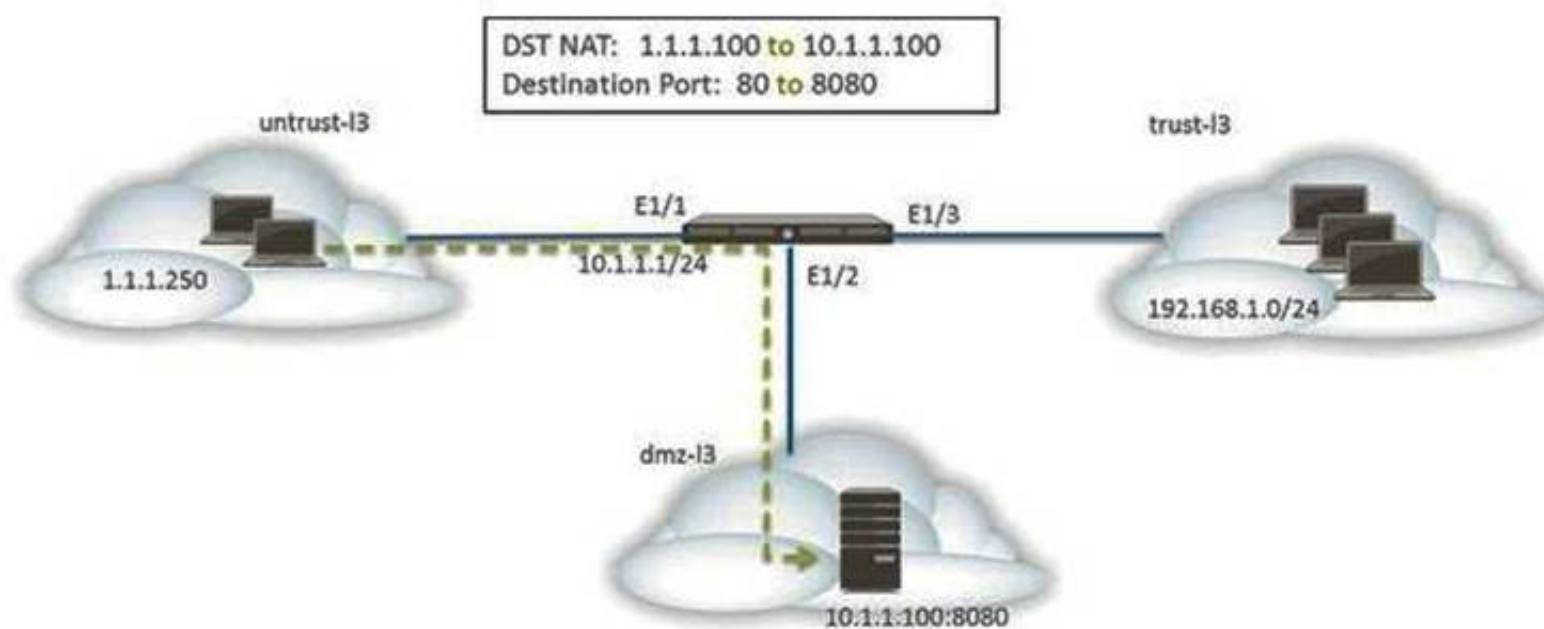
**Answer:** BE

#### Explanation:

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

#### NEW QUESTION 216

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-I3 Zone to a destination of 10.1.1.100 in dmz-I3 zone using web-browsing application
- B. A NAT rule with a source of any from untrust-I3 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-I3 zone to a destination of 1.1.1.100 in untrust-I3 zone using service-http service.
- D. A security policy with a source of any from untrust-I3 zone to a destination of 1.1.100 in dmz-I3 zone using web-browsing application.

**Answer:** BD

#### NEW QUESTION 221

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-Traffic-Flow/ta-p/53693>

**NEW QUESTION 222**

Palo Alto Networks maintains a dynamic database of malicious domains.

Which two Security Platform components use this database to prevent threats? (Choose two)

- A. Brute-force signatures
- B. BrightCloud Url Filtering
- C. PAN-DB URL Filtering
- D. DNS-based command-and-control signatures

**Answer:** CD

**NEW QUESTION 227**

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 230**

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 235**

A network administrator uses Panorama to push security polices 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 240**

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 241**

Which Security Policy Rule configuration option disables antivirus and anti-spyware scanning of server-to-client flows only?

- A. Disable Server Response Inspection
- B. Apply an Application Override
- C. Disable HIP Profile
- D. Add server IP Security Policy exception

**Answer:** A

**NEW QUESTION 244**

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 245**

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

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

**Answer:** BC

**NEW QUESTION 250**

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 255**

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 260**

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 263**

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 267**

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

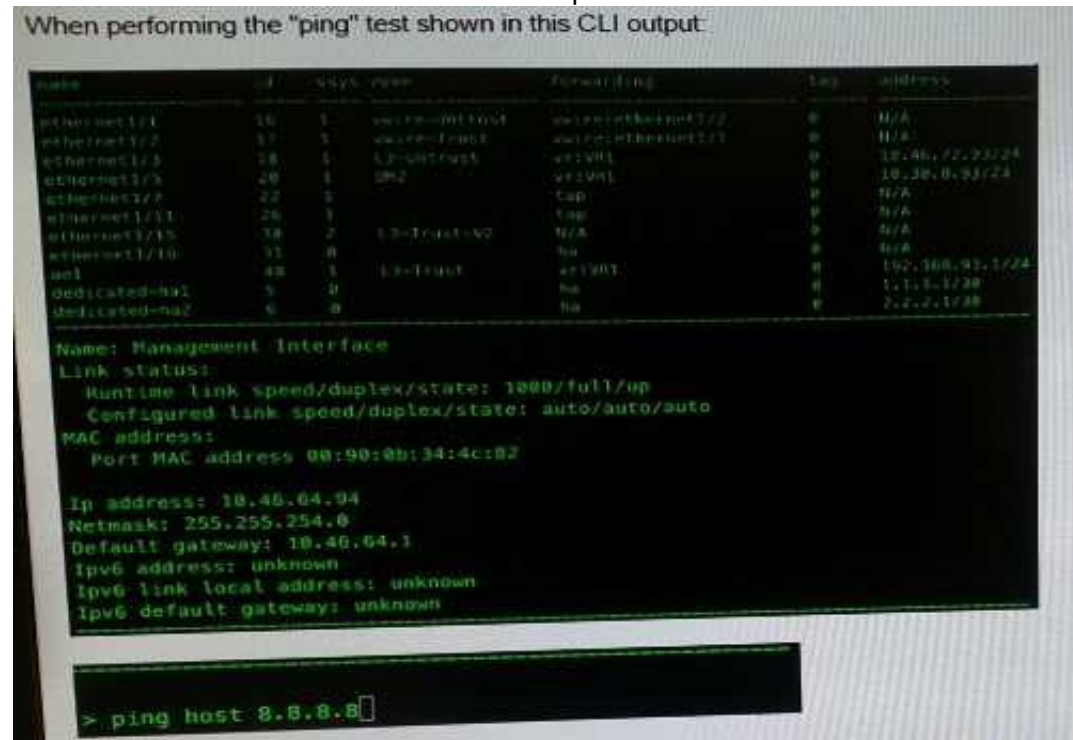
**Explanation:**

<https://live.paloaltonetworks.com/t5/Management-Articles/Show-System-Resource-Command-Displays-CPU-Utilization-of-9999/ta-p/58149>

**NEW QUESTION 268**



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 270

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 273

Which CLI command displays the current management plane memory utilization?

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

**Answer: D**

#### Explanation:

<https://live.paloaltonetworks.com/t5/Learning-Articles/How-to-Interpret-show-system-resources/ta-p/59364>

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

<https://live.paloaltonetworks.com/t5/Learning-Articles/How-to-Interpret-show-system-resources/ta-p/59364>

<https://live.paloaltonetworks.com/t5/Learning-Articles/How-to-Interpret-show-system-resources/ta-p/59364>

#### NEW QUESTION 274

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

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

**Answer: D**

#### NEW QUESTION 279

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

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

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

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

**Answer:** AB

**NEW QUESTION 281**

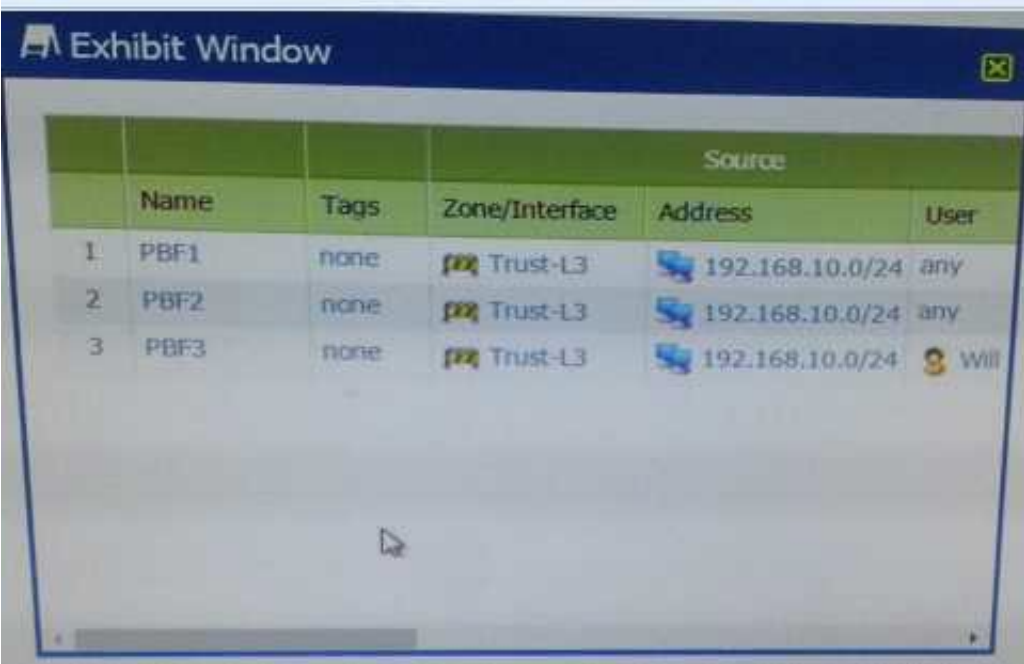
How can a Palo Alto Networks firewall be configured to send syslog messages in a format compatible with non-standard syslog servers?

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

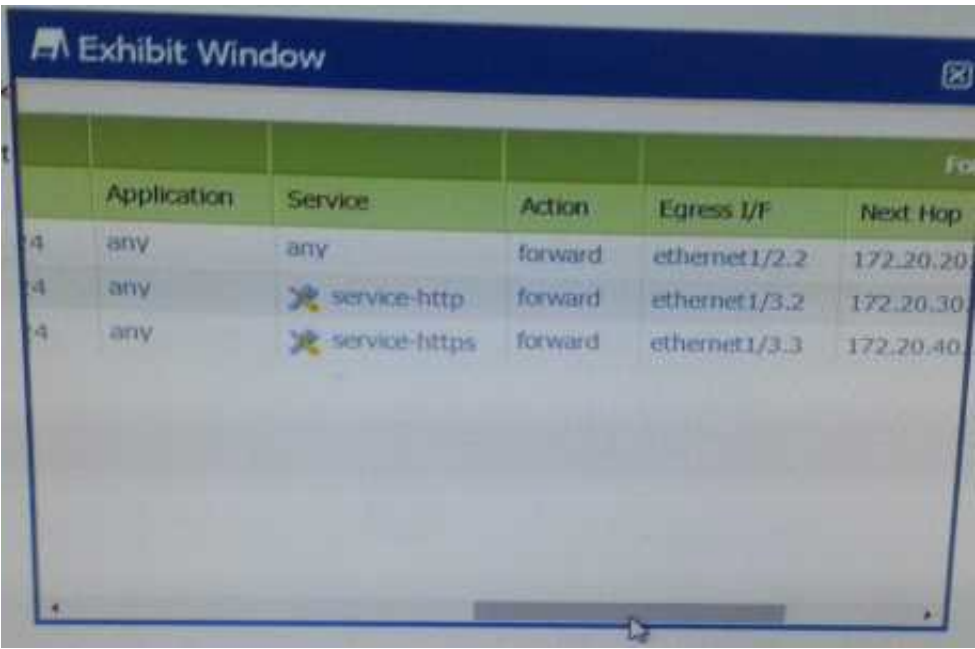
**Answer:** D

**NEW QUESTION 284**

Refer to Exhibit:



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



	Application	Service	Action	Egress I/F	Next Hop
4	any	any	forward	ethernet1/2.2	172.20.20
4	any	service-http	forward	ethernet1/3.2	172.20.30
4	any	service-https	forward	ethernet1/3.3	172.20.40

A firewall has three PDF rules and a default route with a next hop of 172.29.19.1 that is configured in the default VR. A user named XX-bes a PC with a 192.168.101.10 IP address.

He makes an HTTPS connection to 172.16.10.29.

What is the next hop IP address for the HTTPS traffic from Wills PC.

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

**Answer:** B

**NEW QUESTION 289**

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 292**

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 296**

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

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

**Answer:** AB

**NEW QUESTION 299**

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

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

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

**Answer:** D

**NEW QUESTION 304**

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 305**

.....



## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### PCNSE Practice Exam Features:

- \* PCNSE Questions and Answers Updated Frequently
- \* PCNSE Practice Questions Verified by Expert Senior Certified Staff
- \* PCNSE Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* PCNSE Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The PCNSE Practice Test Here](#)**