

## PCNSE Dumps

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

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



**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**

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

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

**Answer:** A

**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**

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**

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


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

**Answer:** A

**NEW QUESTION 7**

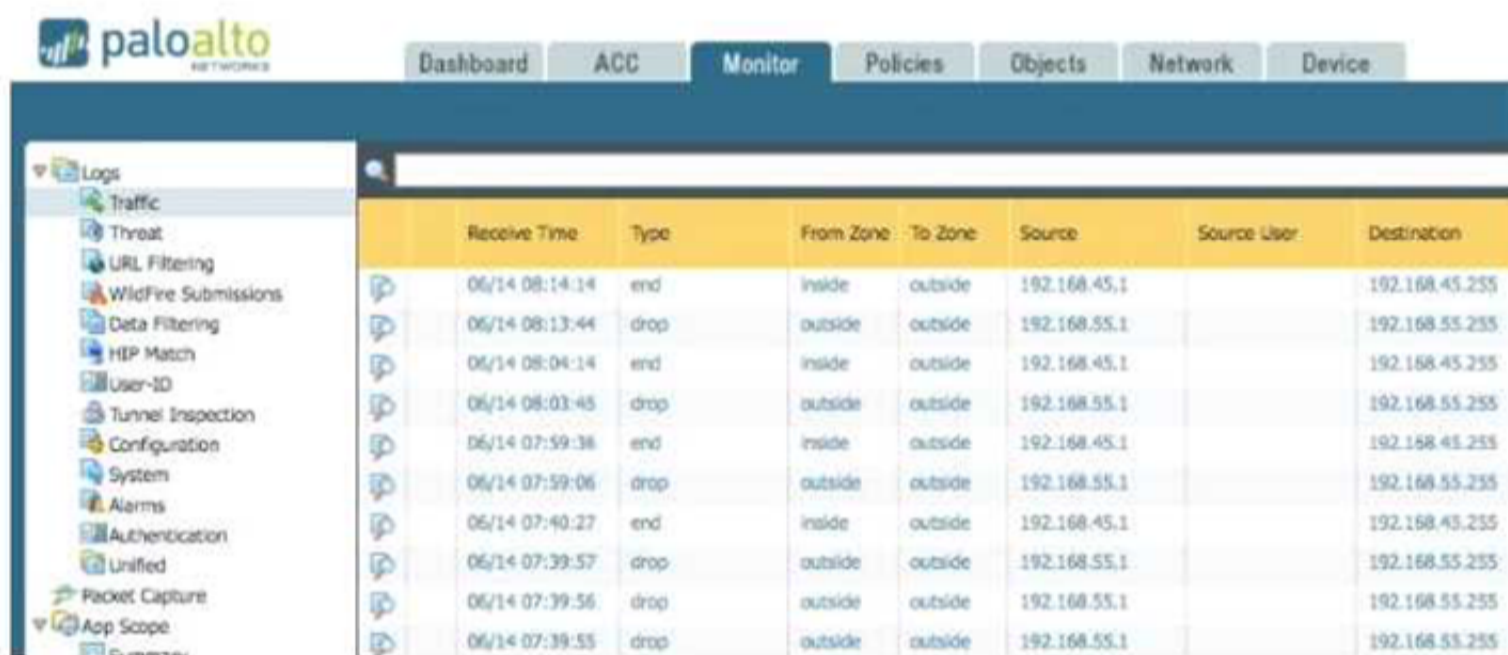
An administrator accidentally closed the commit window/screen before the commit was finished. Which two options could the administrator use to verify the progress or success of that commit task? (Choose two.)

A



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

B

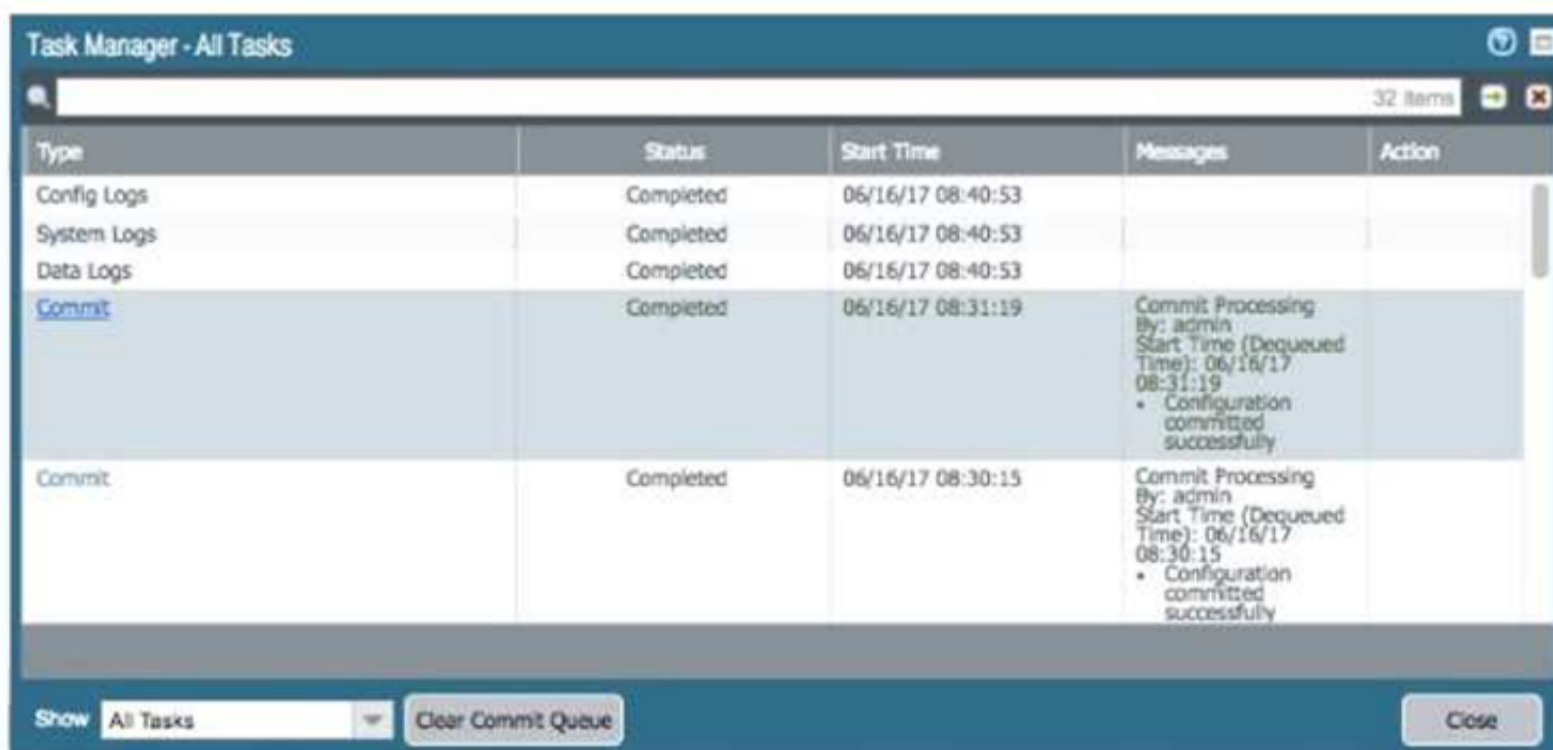


| Receive Time   | Type | From Zone | To Zone | Source       | Source User | Destination    |
|----------------|------|-----------|---------|--------------|-------------|----------------|
| 06/14 08:14:14 | end  | inside    | outside | 192.168.45.1 |             | 192.168.45.255 |
| 06/14 08:13:44 | 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<br>Start Time (Dequeued Time): 06/16/17 08:31:19<br>• Configuration committed successfully |        |
| Commit      | Completed | 06/16/17 08:30:15 | Commit Processing By: admin<br>Start Time (Dequeued Time): 06/16/17 08:30:15<br>• Configuration committed successfully |        |

A. Exhibit A

B. Exhibit B

C. Exhibit C

D. Exhibit D

**Answer:** AD

#### NEW QUESTION 8

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 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

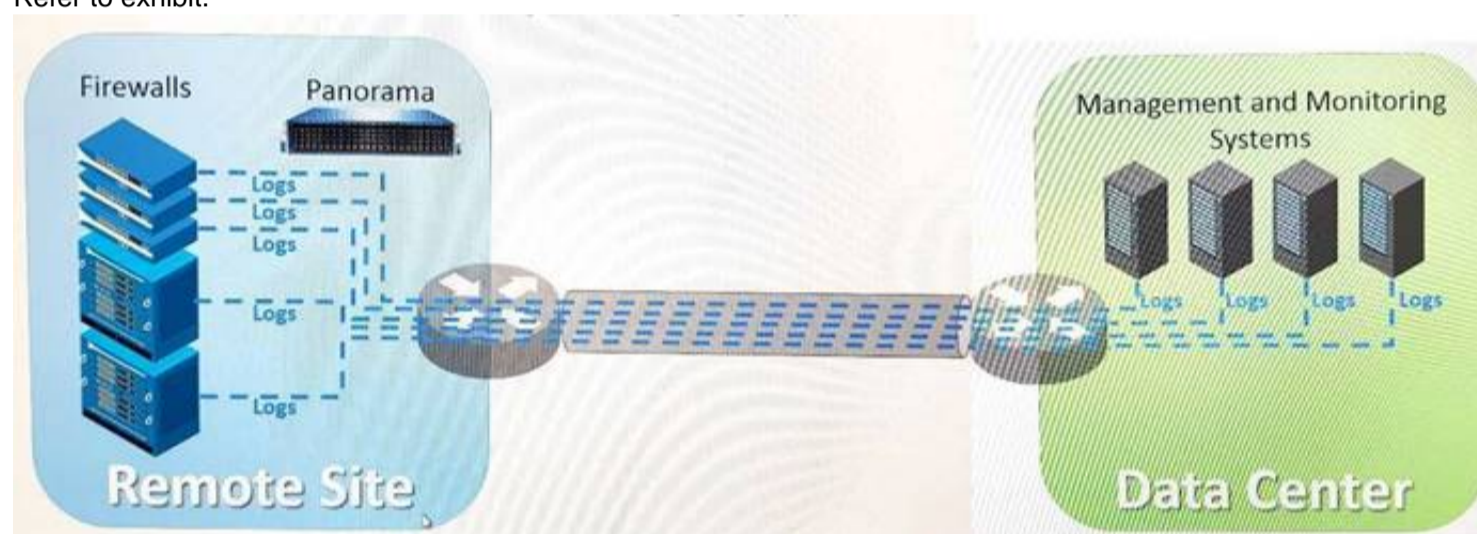
**Answer:** C

#### Explanation:

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

#### NEW QUESTION 10

Refer to exhibit.



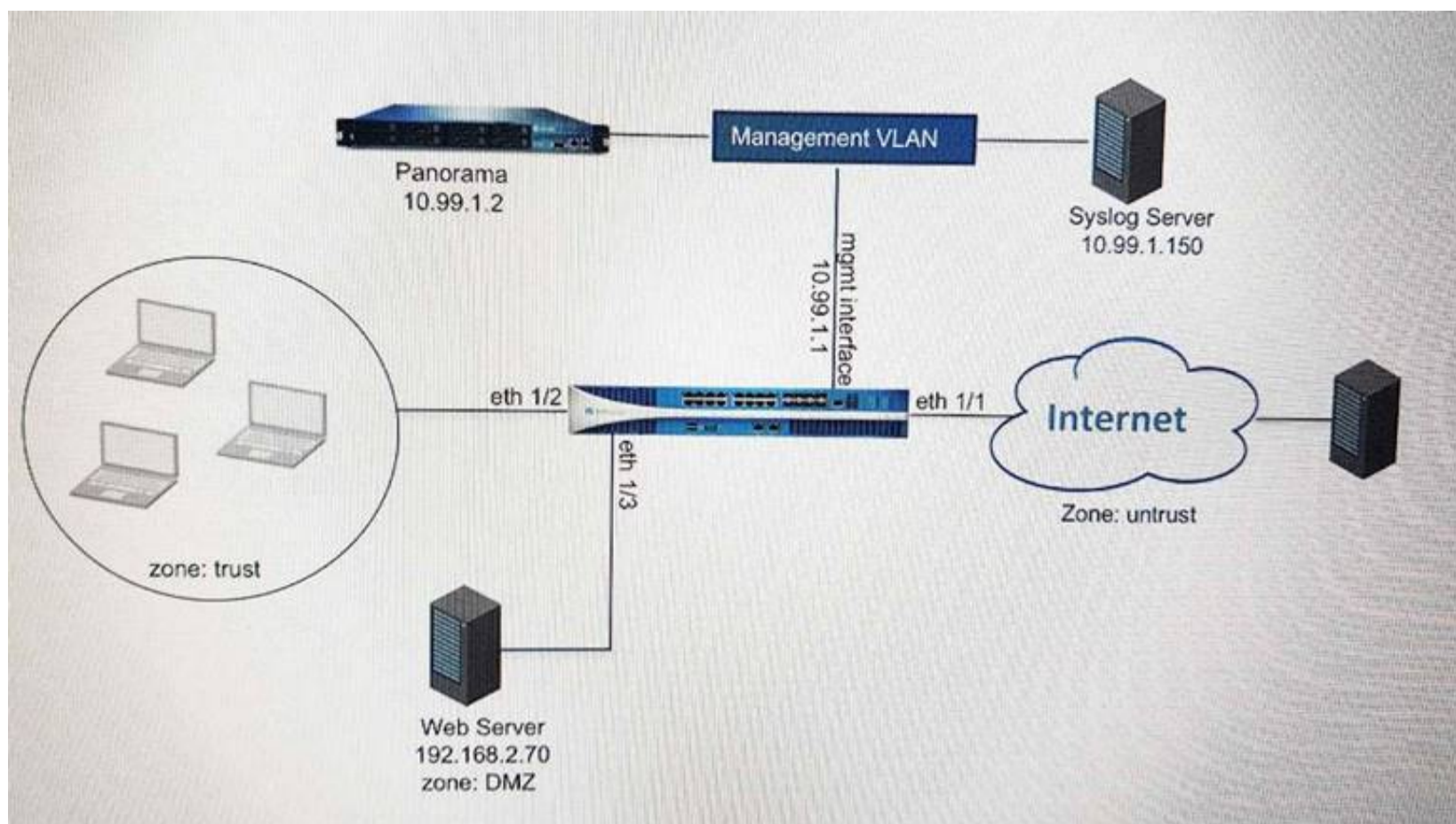
An organization has Palo Alto Networks NGFWs that send logs to remote monitoring and security management platforms. The network team has reported excessive traffic on the corporate WAN. How could the Palo Alto Networks NGFW administrator reduce WAN traffic while maintaining support for all existing monitoring/ 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

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 |
|------------|------|-------|
|------------|------|-------|

☐ Authorize Clients Based on Serial Number

☐ Check Authorization List

Connect Wait Time (min) [0 - 44640]

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

**Answer:** D

**NEW QUESTION 15**

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 18**

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 20**

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

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

**Answer:** A

**Explanation:**

Captive Portal and the other standard user mapping methods might not work for certain types of user access. For example, the standard methods cannot add mappings of users connecting from a third-party VPN solution or users connecting to a 802.1x-enabled wireless network. For such cases, you can use the PAN-OS XML API to capture login events and send them to the PAN-OS integrated User-ID agent Reference: <https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/user-id/user-id-concepts>

**NEW QUESTION 22**

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 24**

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

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

**Answer:** C

**NEW QUESTION 25**

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 30**

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 32**

A web server is hosted in the DMZ, and the server is configured to listen for incoming connections only on TCP port 8080. A Security policy rule allowing access from the Trust zone to the DMZ zone need to be configured to enable web browsing access to the server. Which application and service need to be configured to allow only cleartext web-browsing traffic to this server on tcp/8080.

- A. application: web-browsing; service: application-default
- B. application: web-browsing; service: service-https
- C. application: ssl; service: any
- D. application: web-browsing; service: (custom with destination TCP port 8080)

**Answer:** A

**NEW QUESTION 33**

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. Redistribution of user mappings
- C. Virtual Wire mode
- D. Content inspection

**Answer:** B

#### NEW QUESTION 35

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 39

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

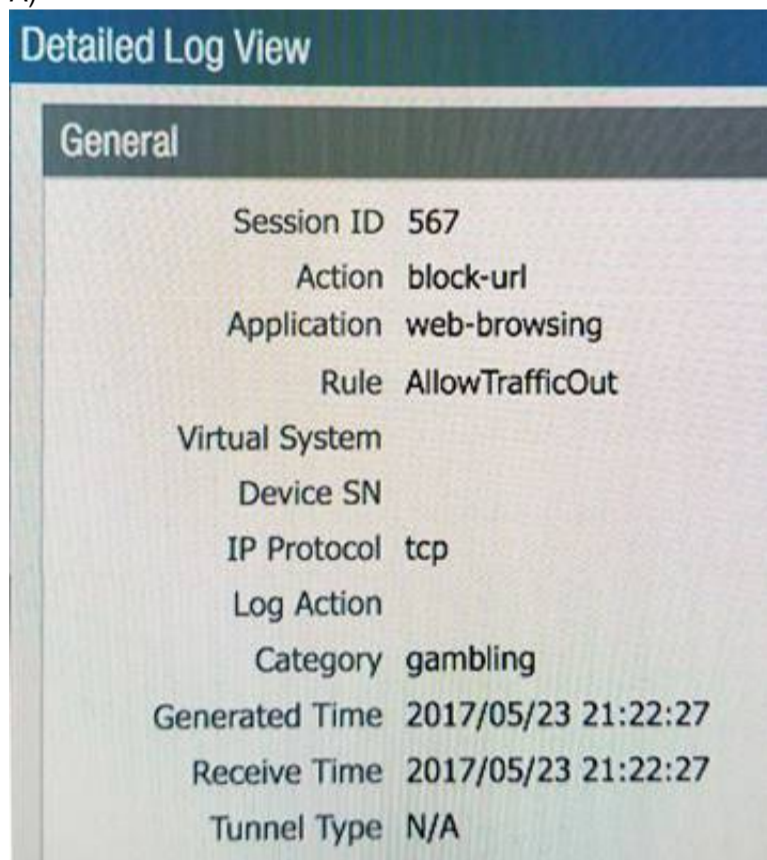
#### Explanation:

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

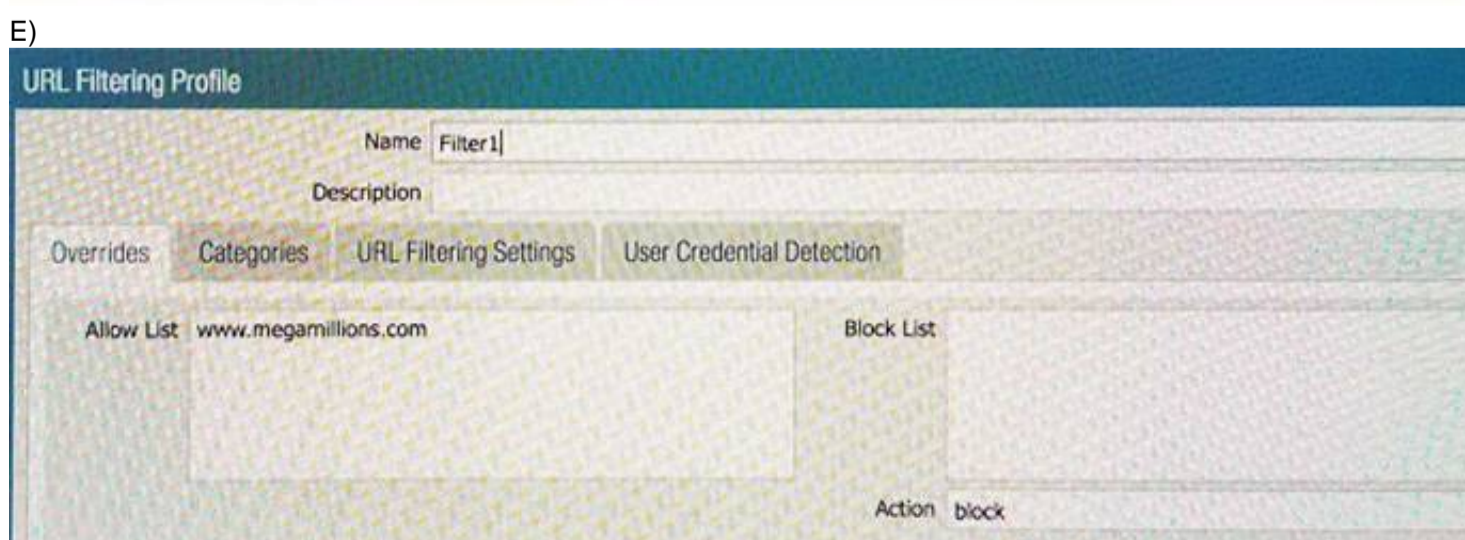
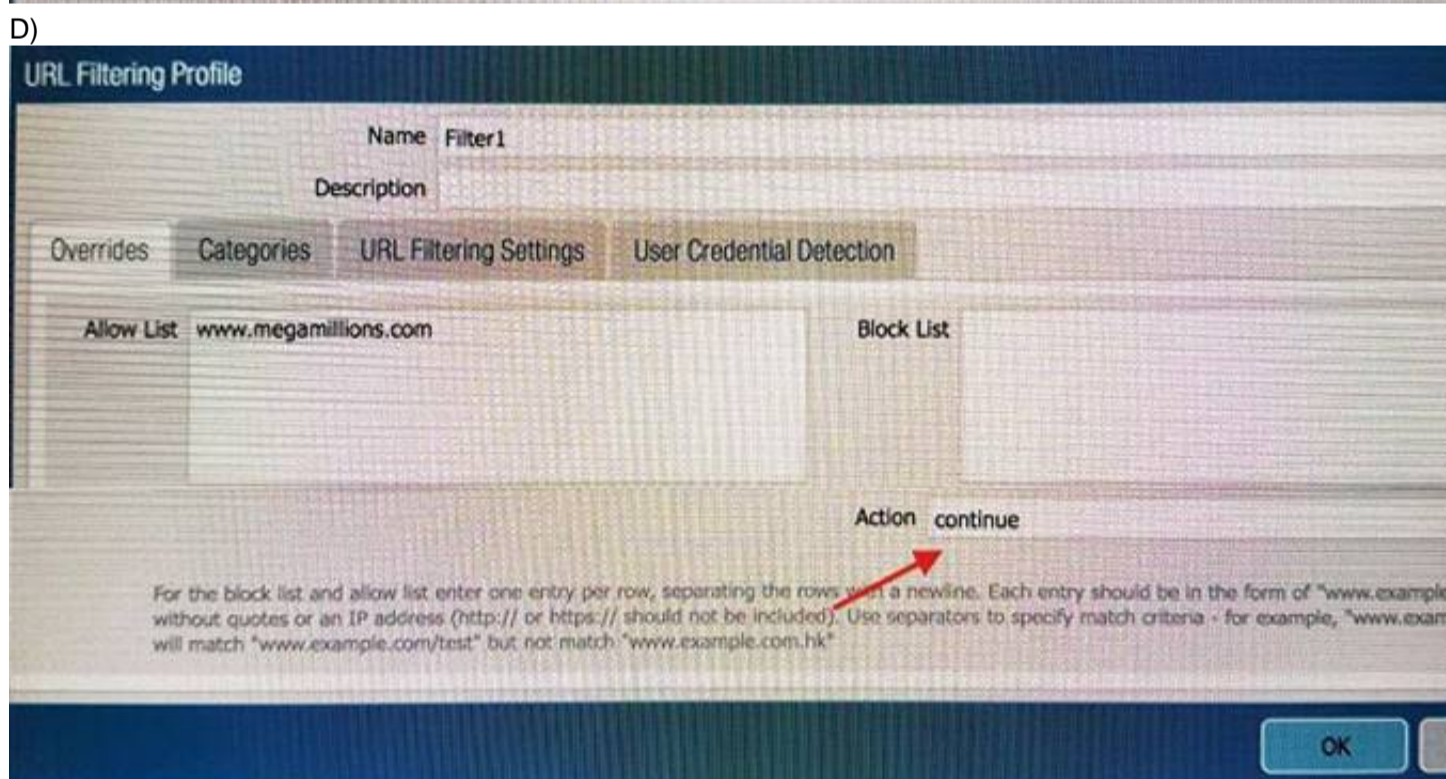
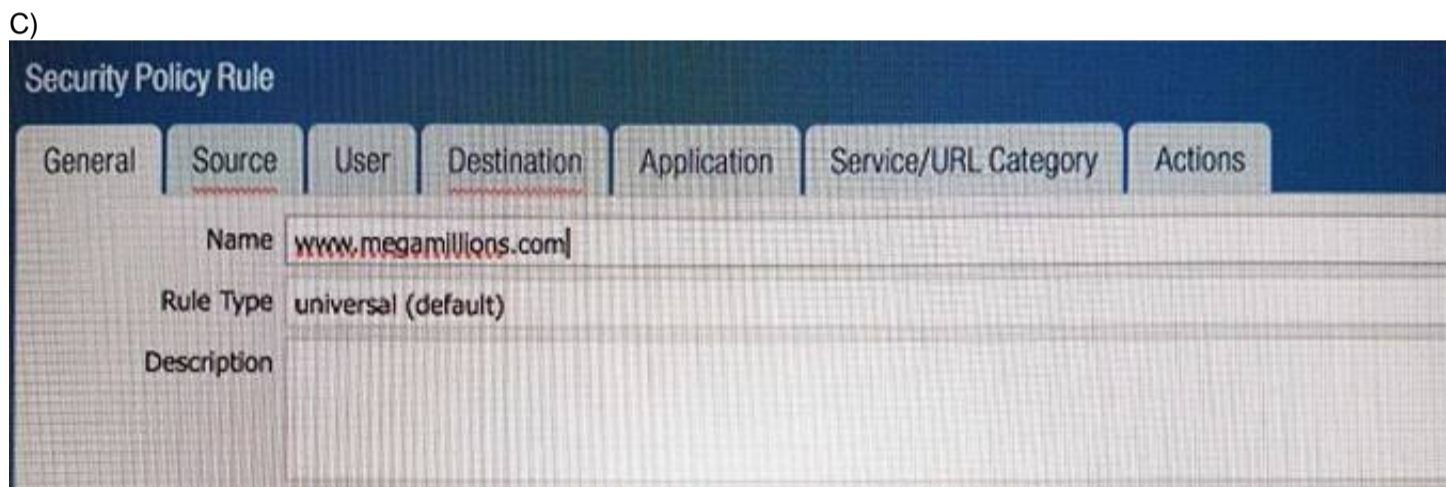
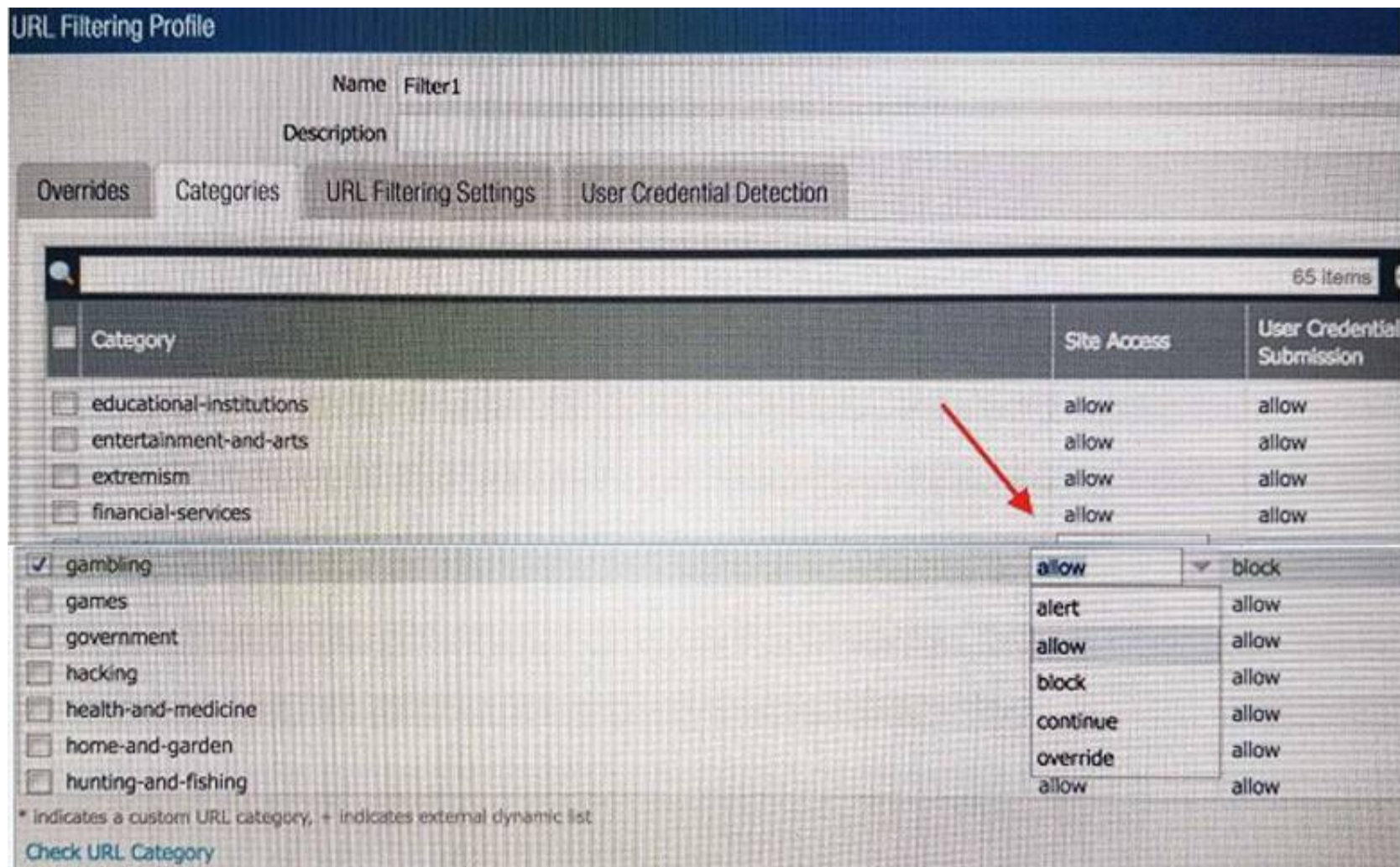
#### NEW QUESTION 41

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

A)



B)



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

**Answer:** B

#### NEW QUESTION 44

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 49

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

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

**Answer:** ABC

#### NEW QUESTION 50

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 PanoramaA.

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 51

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

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

**Answer:** A

#### NEW QUESTION 55

Which Palo Alto Networks VM-Series firewall is valid?

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

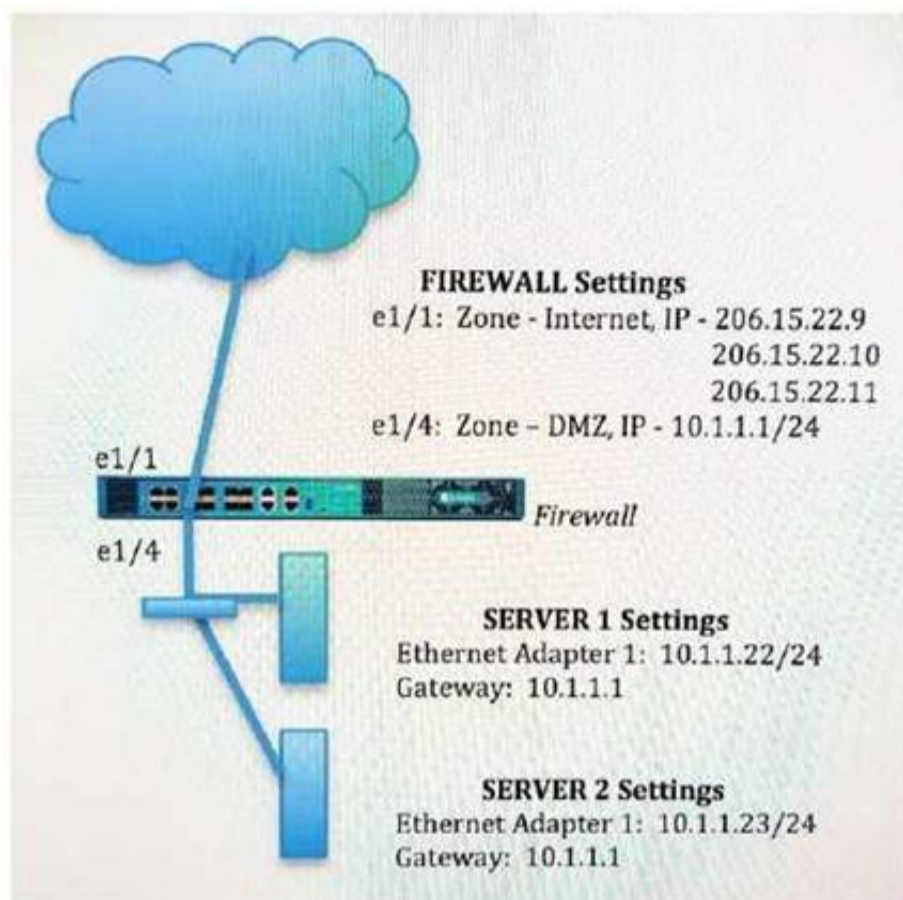
**Answer:** C

#### Explanation:

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

#### NEW QUESTION 60

An administrator wants multiple web servers in the DMZ to receive connections initiated from the internet. Traffic destined for 206.15.22.9 port 80/TCP needs to be forwarded to the server at 10.1.1.22



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

A)

Source IP: Any  
Destination IP: 206.15.22.9  
Source Zone: Internet  
Destination Zone: DMZ  
Destination Service: 80/TCP  
Action: Destination NAT  
Translated IP: 10.2.2.23  
Translated Port: 53/UDP

B)

Source IP: Any  
Destination IP: 206.15.22.9  
Source Zone: Internet  
Destination Zone: Internet  
Destination Service: 80/TCP  
Action: Destination NAT  
Translated IP: 10.1.1.22  
Translated Port: 53/UDP

C)

Source IP: Any  
Destination IP: 206.15.22.9  
Source Zone: Internet  
Destination Zone: Internet  
Destination Service: 80/TCP  
Action: Destination NAT  
Translated IP: 10.1.1.22  
Translated Port: None

D)

Source IP: Any  
Destination IP: 206.15.22.9  
Source Zone: Internet  
Destination Zone: DMZ  
Destination Service: 80/TCP  
Action: Destination NAT  
Translated IP: 10.1.1.22  
Translated Port: 80/TCP

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

**Answer: D**

**NEW QUESTION 63**

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 67**

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 70**

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 73**

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

- A. Deny application facebook-chat before allowing application facebook

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

**Answer:** A

**Explanation:**

Reference: <https://live.paloaltonetworks.com/t5/Configuration-Articles/Failed-to-Block-Facebook-Chat-Consistently/ta-p/115673>

**NEW QUESTION 78**

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 82**

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

- A. Security policy rule
- B. CRL
- C. Service route
- D. Scheduler

**Answer:** A

**NEW QUESTION 84**

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

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

**Answer:** D

**NEW QUESTION 88**

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

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

**NEW QUESTION 89**

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 94**

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 95**

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

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

**Answer: B**

**Explanation:**

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

**NEW QUESTION 96**

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

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

**Answer: D**

**Explanation:**

Reference:

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

**NEW QUESTION 98**

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 102**

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 104**

When is the content inspection performed in the packet flow process?

- A. after the application has been identified
- B. before session lookup
- C. before the packet forwarding process
- D. after the SSL Proxy re-encrypts the packet

**Answer: A**

**Explanation:**

Reference:

<https://live.paloaltonetworks.com/t5/Learning-Articles/Packet-Flow-Sequence-in-PAN-OS/ta-p/56081>

**NEW QUESTION 105**

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

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

**Answer:** A

**Explanation:**

Reference: <https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Implement-and-Test-SSL-Decryption/ta-p/59719>

**NEW QUESTION 109**

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 110**

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
```

```
#####
```

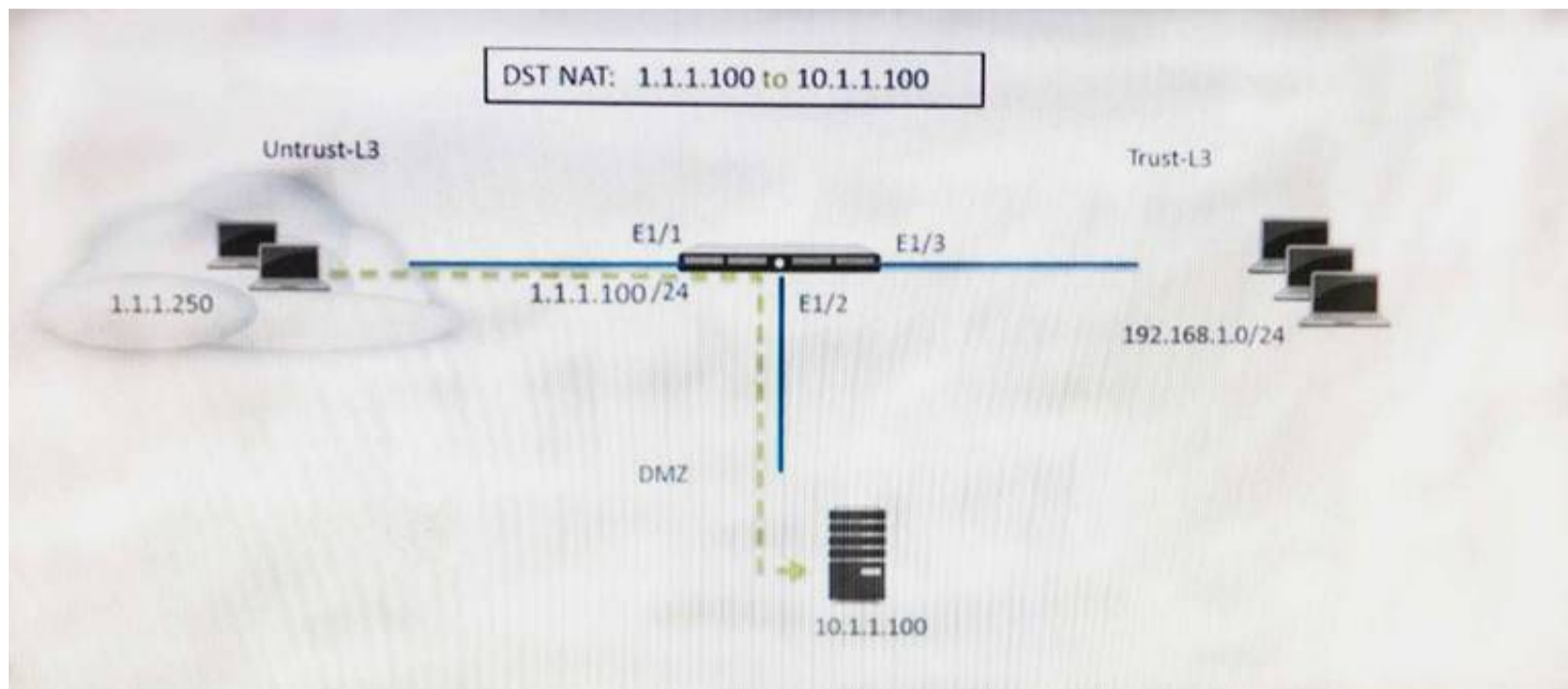
What will be the egress interface if the traffic's ingress interface is ethernet1/6 sourcing from 192.168.111.3 and to the destination 10.46.41.113 during the time shown in the image?

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

**Answer:** D

**NEW QUESTION 113**

Refer to the exhibit.



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

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

**Answer: B**

#### NEW QUESTION 114

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 117

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 120

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 123

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 128

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 133

The firewall identifies a popular application as an unknown-tcp.

Which two options are available to identify the application? (Choose two.)

- A. Create a custom application.
- B. Create a custom object for the custom application server to identify the custom application.
- C. Submit an Apple-ID request to Palo Alto Networks.
- D. Create a Security policy to identify the custom application.

**Answer:** AB

**Explanation:**

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/app-id/use-application-objects-in-policy/create-a-custom-application>

#### NEW QUESTION 134

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

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

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

#### NEW QUESTION 137

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 141

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 144

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 145

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](https://live.paloaltonetworks.com/t5/Featured-Articles/Best-Practices-for-PAN-OS-Upgrade/ta-p/111045)

#### NEW QUESTION 150

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 154

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 159

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 161

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

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

**Answer:** B

#### NEW QUESTION 165

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

- A. App Scope

- B. ACC
- C. Session Browser
- D. System Logs

**Answer:** C

#### NEW QUESTION 168

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 172

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 176

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

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

**Answer:** B

#### NEW QUESTION 181

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 183

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

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

**Answer:** B

#### NEW QUESTION 187

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 188

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 191

An administrator just submitted a newly found piece of spyware for WildFire analysis. The spyware passively monitors behavior without the user's knowledge. What is the expected verdict from WildFire?

- A. Gray ware
- B. Malware
- C. Spyware
- D. Phishing

**Answer:** A

#### NEW QUESTION 194

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

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

**Answer:** CD

#### NEW QUESTION 199

A client has a sensitive application server in their data center and is particularly concerned about session flooding because of denial of-service attacks. How can the Palo Alto Networks NGFW be configured to specifically protect this server against session floods originating from a single IP address?

- A. Define a custom App-ID to ensure that only legitimate application traffic reaches the server
- B. Add QoS Profiles to throttle incoming requests
- C. Add a tuned DoS Protection Profile
- D. Add an Anti-Spyware Profile to block attacking IP address

**Answer:** C

#### NEW QUESTION 201

Which Panorama administrator types require the configuration of at least one access domain? (Choose two)

- A. Dynamic
- B. Custom Panorama Admin
- C. Role Based
- D. Device Group E.Template Admin

**Answer:** DE

#### NEW QUESTION 205

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 207

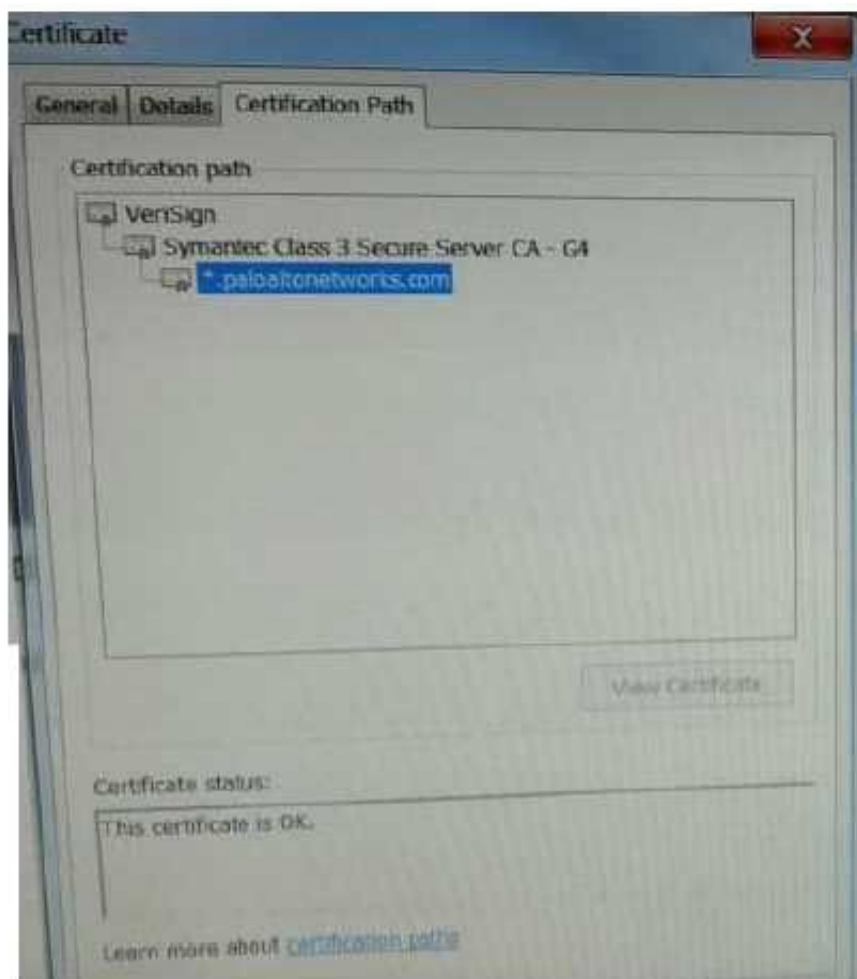
Which two settings can be configured only locally on the firewall and not pushed from a Panorama template or template stack? (Choose two)

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

**Answer:** AB

#### NEW QUESTION 209

Based on the following image,



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

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

**Answer: D**

#### NEW QUESTION 212

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 215

Site-A and Site-B have a site-to-site VPN set up between them. OSPF is configured to dynamically create the routes between the sites. The OSPF configuration in Site-A is configured properly, but the route for the tunnel is not being established. The Site-B interfaces in the graphic are using a broadcast Link Type. The administrator has determined that the OSPF configuration in Site-B is using the wrong Link Type for one of its interfaces.

| Virtual Router - OSPF - Area |              |                                     |                          |              |        |          |
|------------------------------|--------------|-------------------------------------|--------------------------|--------------|--------|----------|
| Area ID                      |              | 0.0.0.0                             |                          |              |        |          |
| Type                         | Range        | Interface                           |                          | Virtual Link |        |          |
|                              |              | Enable                              | Passive                  | Link Type    | Metric | Priority |
| <input type="checkbox"/>     | tunnel.10    | <input checked="" type="checkbox"/> | <input type="checkbox"/> | broadcast    | 10     | 1        |
| <input type="checkbox"/>     | ethernet1/21 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | broadcast    | 10     | 1        |

Which Link Type setting will correct the error?

- A. Set tunne
- B. 1 to p2p
- C. Set tunne
- D. 1 to p2mp
- E. Set Ethernet 1/1 to p2mp
- F. Set Ethernet 1/1 to p2p

**Answer: A**

#### NEW QUESTION 216

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

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

**Answer:** BCD

#### Explanation:

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

#### NEW QUESTION 217

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 220

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.

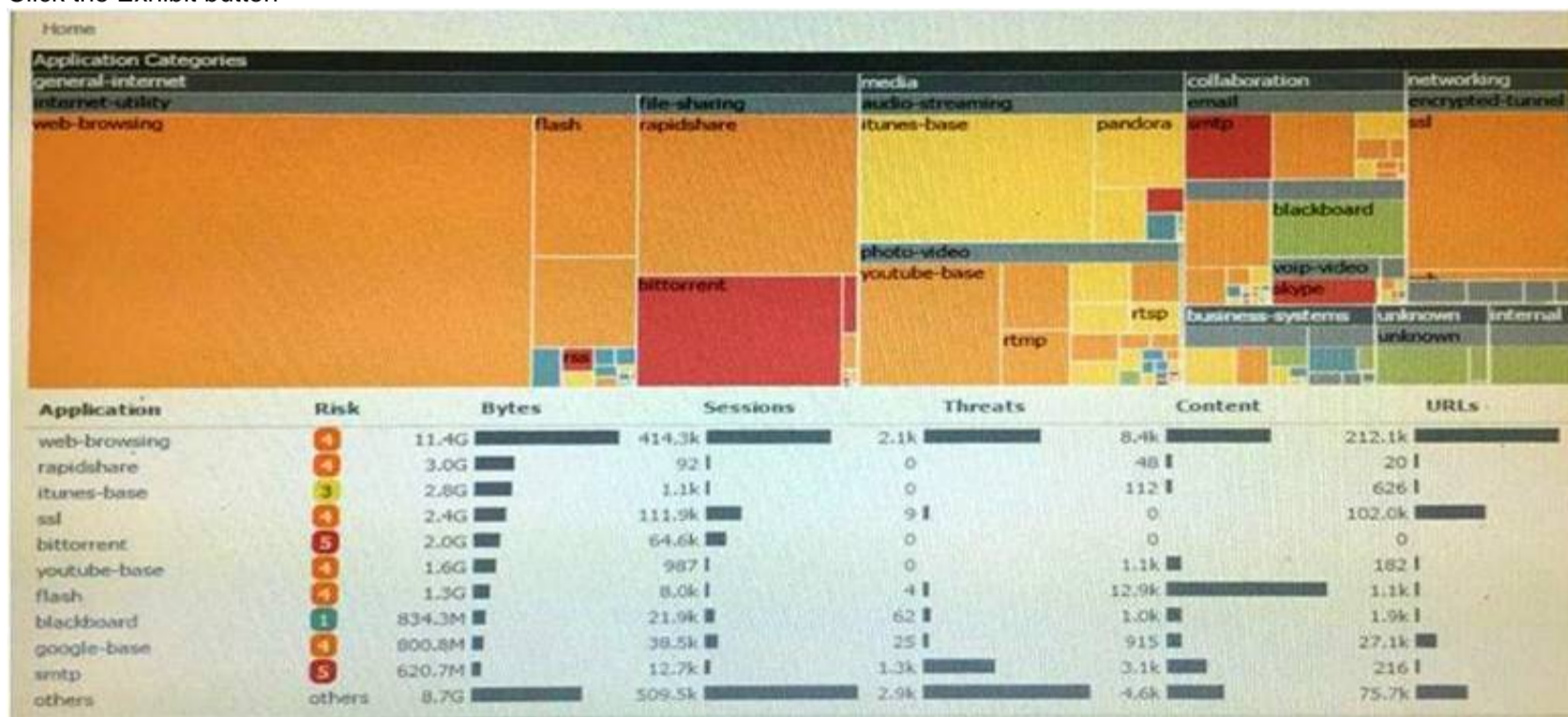
What should be done next?

- 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 221

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 226

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 228

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 229

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 234

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 238

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 then 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 240

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 242

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 246**

A company has a web server behind a Palo Alto Networks next-generation firewall that it wants to make accessible to the public at 1.1.1.1. The company has decided to configure a destination NAT Policy rule.

Given the following zone information:

- DMZ zone: DMZ-L3
- Public zone: Untrust-L3
- Guest zone: Guest-L3
- Web server zone: Trust-L3
- Public IP address (Untrust-L3): 1.1.1.1
- Private IP address (Trust-L3): 192.168.1.50

What should be configured as the destination zone on the Original Packet tab of NAT Policy rule?

- A. Untrust-L3
- B. DMZ-L3
- C. Guest-L3
- D. Trust-L3

**Answer:** A

**NEW QUESTION 250**

A network security engineer has been asked to analyze Wildfire activity. However, the Wildfire Submissions item is not visible form the Monitor tab.

What could cause this condition?

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

**Answer:** B

**NEW QUESTION 251**

Click the Exhibit button below,

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

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

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

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

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

**Answer:** C

**NEW QUESTION 254**

Which three function are found on the dataplane of a PA-5050? (Choose three)

- A. Protocol Decoder
- B. Dynamic routing
- C. Management
- D. Network Processing
- E. Signature Match

**Answer:** BDE

**NEW QUESTION 259**

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

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

**Answer:** BEF

**Explanation:**

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

**NEW QUESTION 263**

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 265**

How are IPV6 DNS queries configured to user interface ethernet1/3?

- A. Network > Virtual Router > DNS Interface
- B. Objects > CustomerObjects > DNS
- C. Network > Interface Mgrnt
- D. Device > Setup > Services > Service Route Configuration

**Answer:** D

**NEW QUESTION 268**

A firewall administrator is troubleshooting problems with traffic passing through the Palo Alto Networks firewall. Which method shows the global counters associated with the traffic after configuring the appropriate packet filters?

- A. From the CLI, issue the show counter global filter pcap yes command.
- B. From the CLI, issue the show counter global filter packet-filter yes command.
- C. From the GUI, select show global counters under the monitor tab.
- D. From the CLI, issue the show counter interface command for the ingress interface.

**Answer:** B

**NEW QUESTION 271**

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

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

**Answer:** B

**NEW QUESTION 274**

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

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

D. Certificate Profile

**Answer:** A

**Explanation:**

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

**NEW QUESTION 276**

Which interface configuration will accept specific VLAN IDs?

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

**Answer:** B

**NEW QUESTION 280**

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 285**

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

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

**Answer:** C

**NEW QUESTION 287**

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 290**

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 294**

Which option is an IPv6 routing protocol?

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

**Answer:** B

**NEW QUESTION 299**

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 303

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 306

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 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 308

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 312

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

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

**Answer:** B

#### NEW QUESTION 316

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 317

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 322

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 323

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

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

**Answer: A**

**Explanation:**

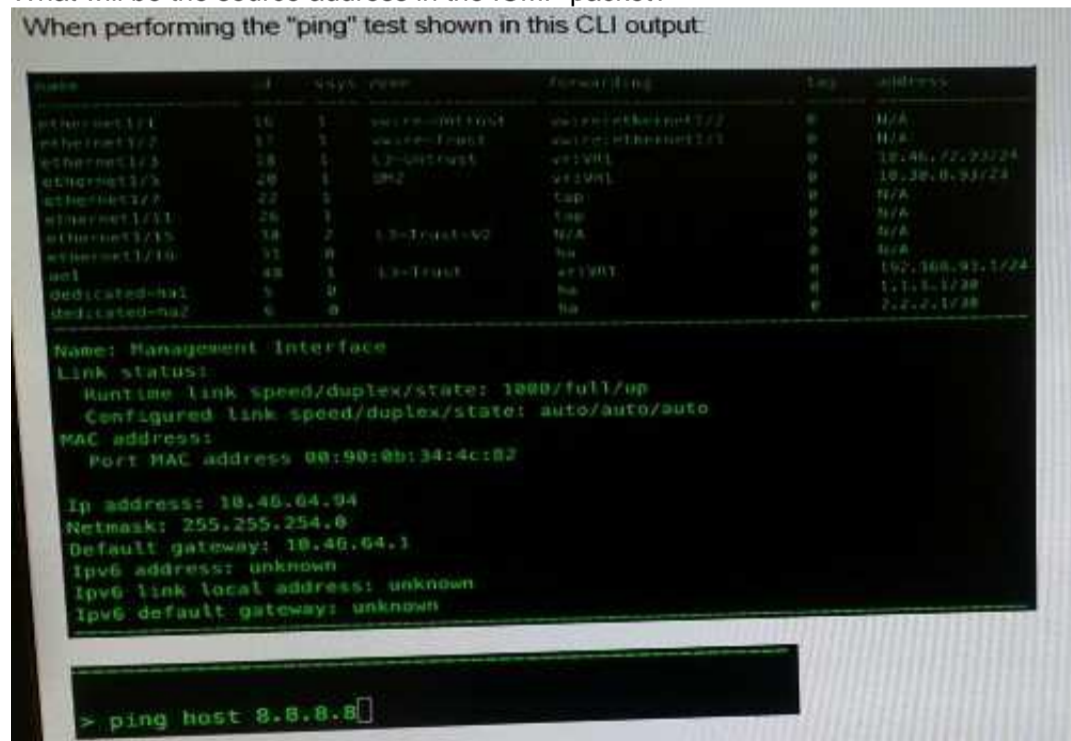
[https://www.paloaltonetworks.com/documentation/61/panorama/panorama\\_adminHYPERLINK](https://www.paloaltonetworks.com/documentation/61/panorama/panorama_adminHYPERLINK)

"[https://www.paloaltonetworks.com/documentation/61/panorama/panorama\\_adminguide/manag-e-log-collection/enable-log-forwarding-from-panorama-to-external-destinations](https://www.paloaltonetworks.com/documentation/61/panorama/panorama_adminguide/manag-e-log-collection/enable-log-forwarding-from-panorama-to-external-destinations)"nguidHYPERLINK "[https://www.paloaltonetworks.com/documentation/61/panorama/panorama\\_adminguide/manag-e-log-collection/enable-log-forwarding-from-panorama-to-external-destinations](https://www.paloaltonetworks.com/documentation/61/panorama/panorama_adminguide/manag-e-log-collection/enable-log-forwarding-from-panorama-to-external-destinations)"e/manage-log-collection/enable-log-forwarding-from-panorama-to-external-destinaHYPERLINK

"[https://www.paloaltonetworks.com/documentation/61/panorama/panorama\\_adminguide/manag-e-log-collection/enable-log-forwarding-from-panorama-to-external-destinations](https://www.paloaltonetworks.com/documentation/61/panorama/panorama_adminguide/manag-e-log-collection/enable-log-forwarding-from-panorama-to-external-destinations)"tions

#### NEW QUESTION 324

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 326

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>"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>"paloHYPERLINK

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

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

**NEW QUESTION 327**

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 331**

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 332**

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

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

**Answer:** C

**NEW QUESTION 337**

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 340**

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

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

- \* ethernet1/1, Zone: Untrust (Internet-facing)
- \* ethernet1/2, Zone: Trust (client-facing)

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

Which setting for class 6 will throttle YouTube traffic?

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

**Answer:** D

**NEW QUESTION 341**

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:
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:09e85260f22f4e15:0000000000000000 <====>
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:09e85260f22f4e15:0000000000000000 <====> 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:09e85260f22f4e15:0000000000000000 <====>
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:33351420a9a1aa47:0000000000000000 <====>
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:33351420a9a1aa47:0000000000000000 <====> Due to
timeout.
2014-08-05 03:53:54 [INFO]: <====> PHASE-1 SA DELETED <====>
```

What could be the cause of this problem?

- A. The dead peer detection settings do not match between the Palo Alto Networks Firewall and the ASA.
- B. The Proxy IDs on the Palo Alto Networks Firewall do not match the setting on the ASA.
- C. The public IP addresses do not match for both the Palo Alto Networks Firewall and the ASA.
- D. The shared secrets do not match between the Palo Alto Networks Firewall and the ASA.

**Answer: C**

#### NEW QUESTION 342

.....

## 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>