

## PCNSE

Number: PCNSE  
Passing Score: 800  
Time Limit: 120 min  
File Version: 1

PCNSE



**Website:** <https://vceplus.com>

**VCE to PDF Converter:** <https://vceplus.com/vce-to-pdf/>

**Facebook:** <https://www.facebook.com/VCE.For.All.VN/>

**Twitter :** [https://twitter.com/VCE\\_Plus](https://twitter.com/VCE_Plus)

<https://vcceplus.com/>

## Exam A

### QUESTION 1

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



<https://vceplus.com/>

- D. sim

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

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

### QUESTION 2

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

Which NGFW receives the configuration from Panorama?

- A. The passive firewall, which then synchronizes to the active firewall
- B. The active firewall, which then synchronizes to the passive firewall
- C. Both the active and passive firewalls, which then synchronize with each other

D. Both the active and passive firewalls independently, with no synchronization afterward

**Correct Answer:** C

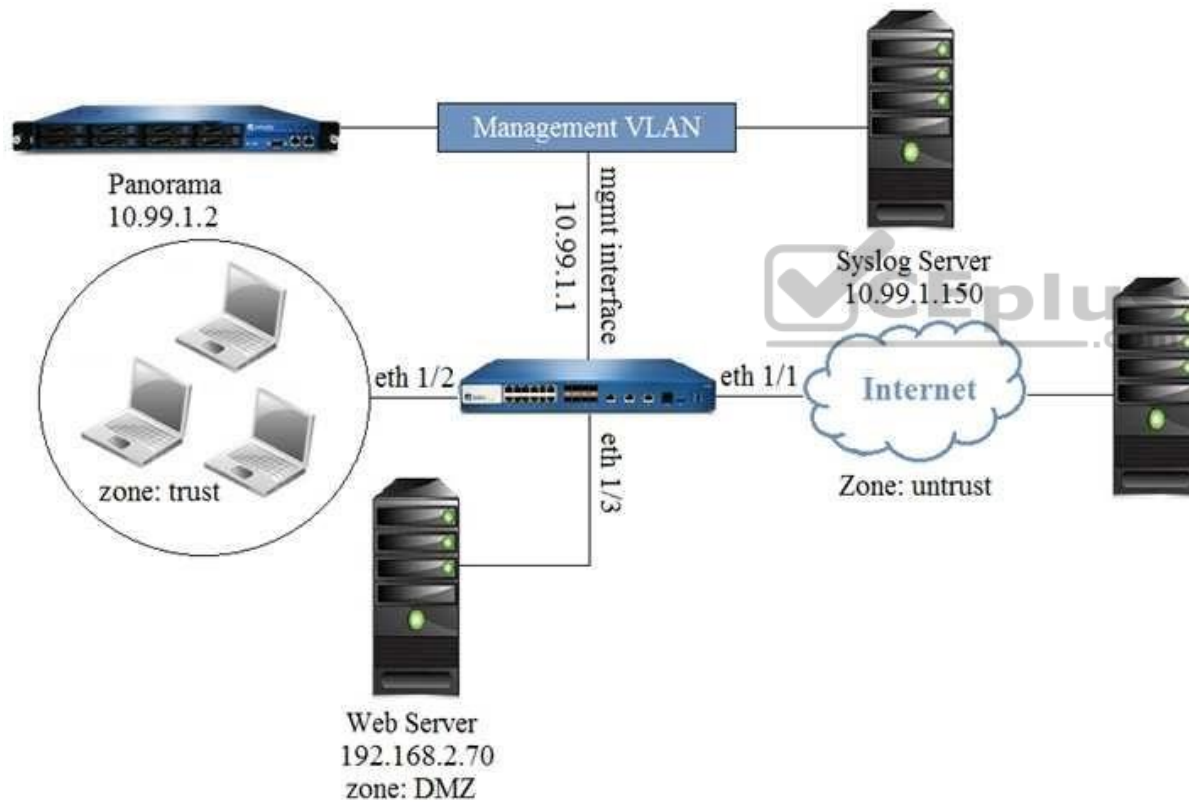
**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 3

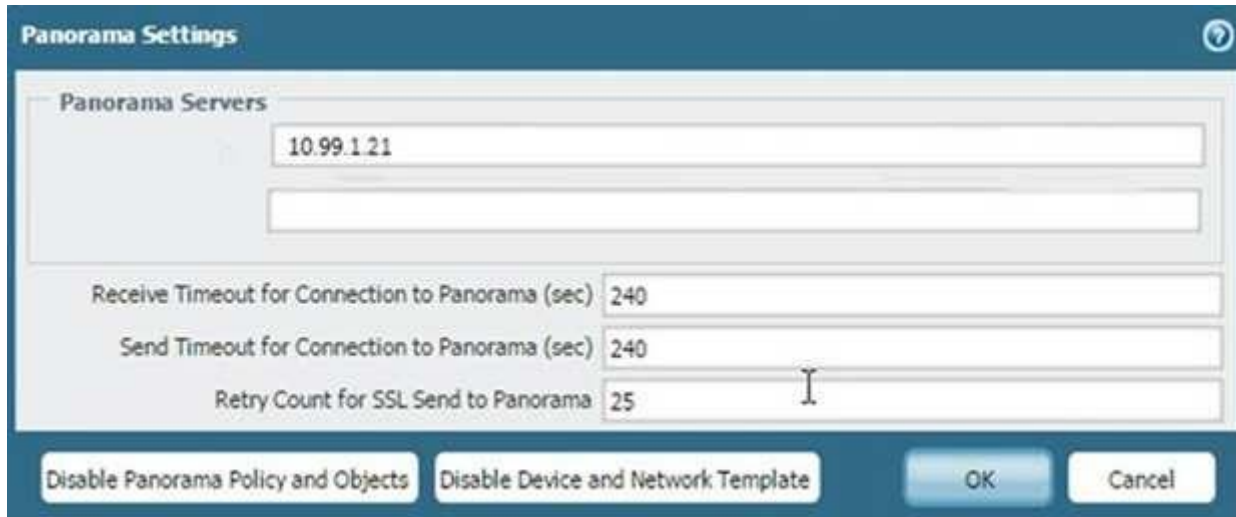
Refer to the exhibit.



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



A.



The image shows a 'Panorama Settings' dialog box with a dark blue header and a light blue body. The title bar says 'Panorama Settings' and there is a help icon on the right. The main area is divided into sections. The first section is 'Panorama Servers', which contains two text input fields; the first field has the IP address '10.99.1.21' and the second is empty. Below this, there are three rows of settings, each with a label and a text input field: 'Receive Timeout for Connection to Panorama (sec)' with '240', 'Send Timeout for Connection to Panorama (sec)' with '240', and 'Retry Count for SSL Send to Panorama' with '25'. At the bottom of the dialog, there are four buttons: 'Disable Panorama Policy and Objects', 'Disable Device and Network Template', 'OK', and 'Cancel'.

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



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


☒ Panorama

**Servers** **Custom Log Format**

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

 Add  Delete

Enter the IP address or FQDN of the Syslog server

 OK Cancel

D.

**Panorama Settings**

Receive Timeout for Connection to Panorama (sec) 240

Send Timeout for Connection to Panorama (sec) 240

Retry Count for SSL Send to Panorama 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		

+ Add - Delete

☐ Authorize Clients Based on Serial Number

☐ Check Authorization List

Disconnect Wait Time (min) [0-44640]

OK Cancel



E.

**Correct Answer:** D

**Section:** (none)



**Explanation****Explanation/Reference:****QUESTION 4**

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

- A. The settings assigned to the template that is on top of the stack.
- B. The administrator will be prompted to choose the settings for that chosen firewall.
- C. All the settings configured in all templates.
- D. Depending on the firewall location, Panorama decides with settings to send.

**Correct Answer:** A

**Section:** (none)

**Explanation****Explanation/Reference:****QUESTION 5**

How does an administrator schedule an Applications and Threats dynamic update while delaying installation of the update for a certain amount of time?

- A. Configure the option for “Threshold”.
- B. Disable automatic updates during weekdays.
- C. Automatically “download only” and then install Applications and Threats later, after the administrator approves the update.
- D. Automatically “download and install” but with the “disable new applications” option used.

**Correct Answer:** C

**Section:** (none)

**Explanation****Explanation/Reference:****QUESTION 6**

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

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/80/pan-os/pan-os/user-id/user-id-concepts/group-mapping#id93306080-fd9b-4f1b-96a64bfe1c8e69df>

## QUESTION 7

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

## QUESTION 8

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

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 9

A Security policy rule is configured with a Vulnerability Protection Profile and an action of 'Deny'.

Which action will this cause configuration on the matched traffic?

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 10

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

**Correct Answer:** BC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 11**

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

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

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

#### **QUESTION 12**

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 13**

A speed/duplex negotiation mismatch is between the Palo Alto Networks management port and the switch port which it connects.

How would an administrator configure the interface to 1Gbps?

- A. set deviceconfig interface speed-duplex 1Gbps-full-duplex
- B. set deviceconfig system speed-duplex 1Gbps-duplex
- C. set deviceconfig system speed-duplex 1Gbps-full-duplex
- D. set deviceconfig Interface speed-duplex 1Gbps-half-duplex

**Correct Answer: C**

**Section: (none)**

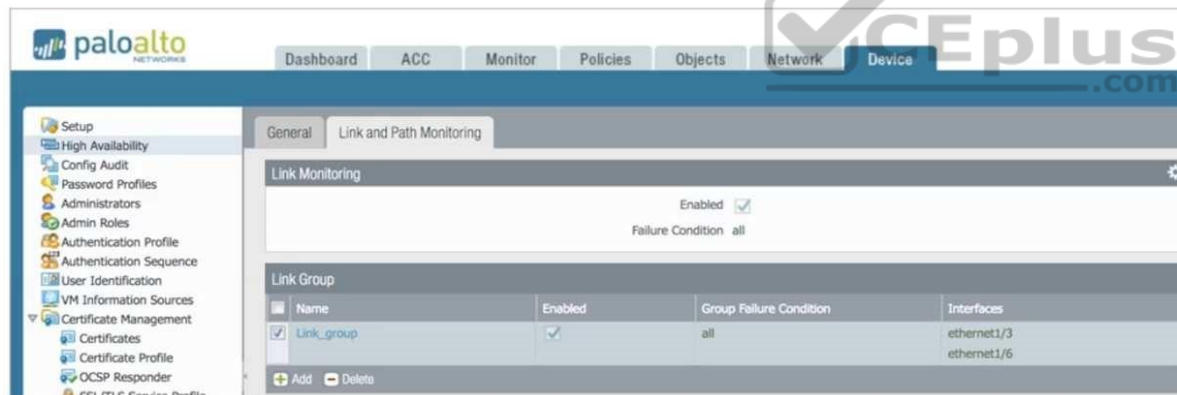
**Explanation**

**Explanation/Reference:**

Reference: <https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Change-the-Speed-and-Duplex-of-the-Management-Port/ta-p/59034>

#### QUESTION 14

If the firewall has the following link monitoring configuration, what will cause a failover?



- A. ethernet1/3 and ethernet1/6 going down
- B. ethernet1/3 going down
- C. ethernet1/3 or ethernet1/6 going down
- D. ethernet1/6 going down

**Correct Answer: A**

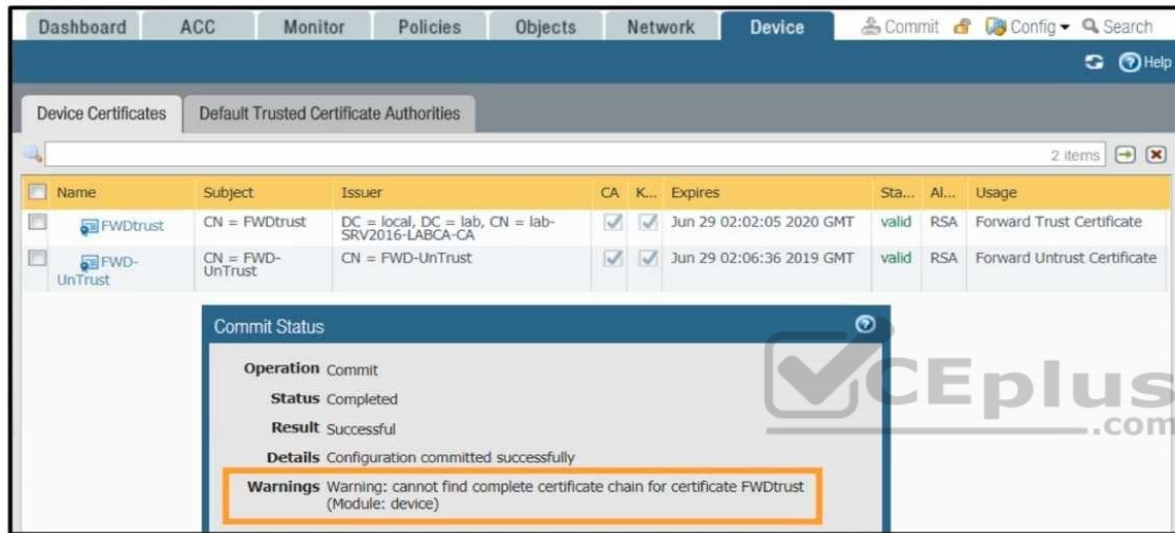
Section: (none)

Explanation

Explanation/Reference:

### QUESTION 15

In the image, what caused the commit warning?



- A. The CA certificate for FWDtrust has not been imported into the firewall.
- B. The FWDtrust certificate has not been flagged as Trusted Root CA.
- C. SSL Forward Proxy requires a public certificate to be imported into the firewall.
- D. The FWDtrust certificate does not have a certificate chain.

**Correct Answer: D**

Section: (none)

Explanation

Explanation/Reference:

### QUESTION 16

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 17**

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



**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/quality-of-service/qos-concepts/qos-for-applications-and-users#daed4e749-80b44641-a37c-c741aba562e9>

#### **QUESTION 18**

A session in the Traffic log is reporting the application as "incomplete."





<https://vcceplus.com/> What does

"incomplete" mean?

- A. The three-way TCP handshake was observed, but the application could not be identified.
- B. The three-way TCP handshake did not complete.
- C. The traffic is coming across UDP, and the application could not be identified.
- D. Data was received but was instantly discarded because of a Deny policy was applied before App-ID could be applied.

**Correct Answer:** B

**Section:** (none)

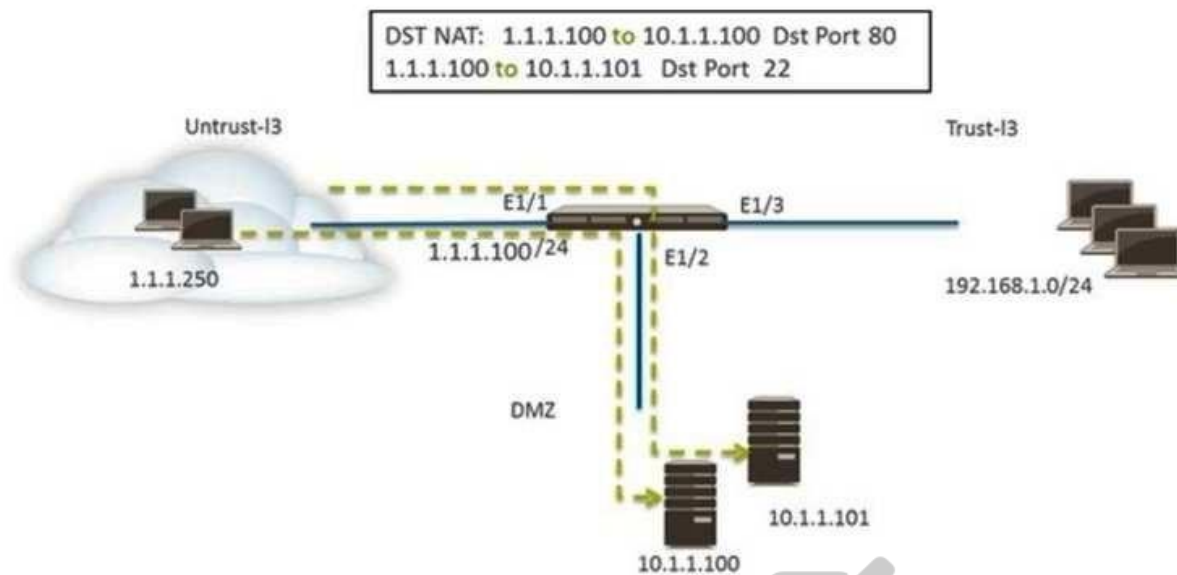
**Explanation**

**Explanation/Reference:**

#### QUESTION 19

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 (10.1.1.100), web-browsing - Allow
- B. Untrust (Any) to Untrust (10.1.1.101), ssh - Allow
- C. Untrust (Any) to DMZ (10.1.1.100), web-browsing - Allow
- D. Untrust (Any) to DMZ (10.1.1.100), ssh - Allow
- E. Untrust (Any) to DMZ (10.1.1.100, 10.1.1.101), ssh, web-browsing - Allow

**Correct Answer:** CD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 20**

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 21

Which Palo Alto Networks VM-Series firewall is valid?

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



**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

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

#### QUESTION 22

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

Which application should be used to identify traffic traversing the NGFW?

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 23

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



**Correct Answer:** DEF

**Section:** (none)

**Explanation**

**Explanation/Reference:**

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)

### QUESTION 24

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 : 1

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 ethernet1/7 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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 25**

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

- A. Threat-ID processing time is decreased.
- B. The Palo Alto Networks NGFW stops App-ID processing at Layer 4.
- C. The application name assigned to the traffic by the security rule is written to the Traffic log.
- D. App-ID processing time is increased.

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

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

**QUESTION 26**

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

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

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

**QUESTION 27**

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.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 28

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

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



**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

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

#### QUESTION 29

An administrator has users accessing network resources through Citrix XenApp 7.x.

Which User-ID mapping solution will map multiple users who are using Citrix to connect to the network and access resources?

- A. Client Probing
- B. Terminal Services agent
- C. GlobalProtect
- D. Syslog Monitoring

**Correct Answer:** B

**Section: (none)**

**Explanation**

**Explanation/Reference:**

### **QUESTION 30**

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

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**



### **QUESTION 31**

Which feature prevents the submission of corporate login information into website forms?

- A. Data filtering
- B. User-ID
- C. File blocking
- D. Credential phishing prevention

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Reference: <https://www.paloaltonetworks.com/cyberpedia/how-the-next-generation-security-platform-contributes-to-gdpr-compliance>



### QUESTION 32

Refer to the exhibit.

Device Certificates									
Default Trusted Certificate Authorities									
1 item									
Name	Location	Subject	Issuer	CA	Key	Expires	Status	Algorithm	Usage
Domain-Root-Cert	vsys1	DC = local, DC = lab, CN = lab-DEMO-2008R2-CA	DC = local, DC = lab, CN = lab-DEMO-2008R2-CA	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Nov 1 00:34:47 2021 GMT	valid	RSA	Trusted Root CA Certificate
Domain Sub-CA	vsys1	CN = sca.lab.local	DC = local, DC = lab, CN = lab-DEMO-2008R2-CA	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Jun 6 20:59:38 2019 GMT	valid	RSA	
Forward_Trust	vsys1	CN = fwdtrust.la...	CN = sca.lab.local	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Jun 6 21:09:49 2018 GMT	valid	RSA	

Which certificates can be used as a Forward Trust certificate?

- A. Certificate from Default Trust Certificate Authorities
- B. Domain Sub-CA
- C. Forward\_Trust
- D. Domain-Root-Cert



**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 33

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.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

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

#### **QUESTION 34**

Which menu 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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**



#### **QUESTION 35**

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

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

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

The firewall uses the service route to connect to the Update Server and checks for new content release versions and, if there are updates available, displays them at the top of the list.

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

### QUESTION 36

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://live.paloaltonetworks.com/t5/Learning-Articles/Quick-Reference-Guide-Helpful-Commands/ta-p/56511>

### QUESTION 37

During the packet flow process, which two processes are performed in application identification? (Choose two.)

- A. Pattern based application identification
- B. Application override policy match
- C. Application changed from content inspection
- D. Session application identified.

**Correct Answer:** BD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 38

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

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

### QUESTION 39

Which three steps will reduce the CPU utilization on the management plane? (Choose three.)

- A. Disable SNMP on the management interface.
- B. Application override of SSL application.
- C. Disable logging at session start in Security policies.
- D. Disable predefined reports.
- E. Reduce the traffic being decrypted by the firewall.



**Correct Answer:** CDE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 40

Which feature must you configure to prevent users from accidentally submitting their corporate credentials to a phishing website?

- A. URL Filtering profile
- B. Zone Protection profile
- C. Anti-Spyware profile
- D. Vulnerability Protection profile

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/threat-prevention/prevent-credential-phishing>

#### QUESTION 41

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.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

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

#### QUESTION 42

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

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 43**

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.

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 44**

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

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

**Correct Answer:** ADE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

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

**QUESTION 45**

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

- A. Heartbeat Monitoring
- B. Failover

- C. Path Monitoring
- D. Ping-Path

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/policy/policy-based-forwarding/pbf/path-monitoring-for-pbf>

#### QUESTION 46

An administrator has a requirement to export decrypted traffic from the Palo Alto Networks NGFW to a third-party, deep-level packet inspection appliance.



<https://vcceplus.com/>

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/decryption/decryption-concepts/decryption-mirroring>

<https://vcceplus.com/>

**QUESTION 47**

An administrator has been asked to configure a Palo Alto Networks NGFW to provide protection against external hosts attempting to exploit a flaw in an operating system on an internal system.

Which Security Profile type will prevent this attack?

- A. Vulnerability Protection
- B. Anti-Spyware
- C. URL Filtering
- D. Antivirus

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/objects/objects-security-profiles-vulnerability-protection>

**QUESTION 48**

An administrator using an enterprise PKI needs to establish a unique chain of trust to ensure mutual authentication between Panorama and the managed firewalls and Log Collectors.

How would the administrator establish the chain of trust?

- A. Use custom certificates
- B. Enable LDAP or RADIUS integration
- C. Set up multi-factor authentication
- D. Configure strong password authentication

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

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



**QUESTION 49**

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?



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

```
Thu Jun  8 12:49:55 PDT 2017
```

```
#####
```

```
admin@Lab33-111-PA-3060(active)# show vsys vsys1 rulebase pbf rules test-pbf
```

```
test-pbf {
  action {
    forward {
      egress-interface ethernet1/5;
    }
  }
  from {
    zone L3-Trust;
  }
  enforce-symmetric-return {
    enabled no;
  }
  source 192.168.111.3;
  destination 10.46.41.113;
  source-user any;
  application any;
  service any;
  schedule schedule-pbf;
}
```

```
#####
```

```
admin@Lab33-111-PA-3060(active)# show vsys vsys1 schedule schedule-pbf
```

```
schedule-pbf {
  schedule-type {
    recurring {
      daily 16:00-21:00;
    }
  }
}
```

```
#####
```

```
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
67	10.10.20.0/24	0.0.0.0	u	ethernet1/7	1500
66	10.10.20.111/32	0.0.0.0	uh	ethernet1/7	1500
46	10.46.40.0/23	0.0.0.0	u	ethernet1/3	1500
49	10.46.44.0/23	0.0.0.0	u	ethernet1/5	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
48	10.46.45.111/32	0.0.0.0	uh	ethernet1/5	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

A. ethernet1/7

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 50

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.



**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://www.paloaltonetworks.com/documentation/80/virtualization/virtualization/set-up-the-vm-series-firewall-on-kvm/install-the-vm-series-firewall-onkvm/use-an-iso-file-to-deploy-the-vm-series-firewall>

#### QUESTION 51

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

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

### QUESTION 52

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.

**Correct Answer:** A

**Section:** (none)

**Explanation**



**Explanation/Reference:**

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

### QUESTION 53

If an administrator wants to decrypt SMTP traffic and possesses the server's certificate, which SSL decryption mode will allow the Palo Alto Networks NGFW to inspect traffic to the server?

- A. TLS Bidirectional Inspection
- B. SSL Inbound Inspection
- C. SSH Forward Proxy
- D. SMTP Inbound Decryption

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

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

**QUESTION 54**

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. Define a custom App-ID to ensure that only legitimate application traffic reaches the server.
- B. Add a Vulnerability Protection Profile to block the attack.
- C. Add QoS Profiles to throttle incoming requests.
- D. Add a DoS Protection Profile with defined session count.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/zone-protection-and-dos-protection/zone-defense/dos-protection-profiles-andpolicy-rules/dos-protection-profiles>

**QUESTION 55**

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

**Correct Answer:** CD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

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

#### QUESTION 56

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

**Correct Answer:** ADF

**Section:** (none)

**Explanation**

**Explanation/Reference:**



#### QUESTION 57

What is exchanged through the HA2 link?

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/high-availability/ha-concepts/ha-links-and-backup-links>

#### QUESTION 58

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.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/decryption/configure-ssh-proxy>

#### QUESTION 59

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 60

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 61

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. tunnel.1
- B. vpn-tunnel.1
- C. tunnel.1025
- D. vpn-tunnel.1024



**Correct Answer:** AC

**Section:** (none)

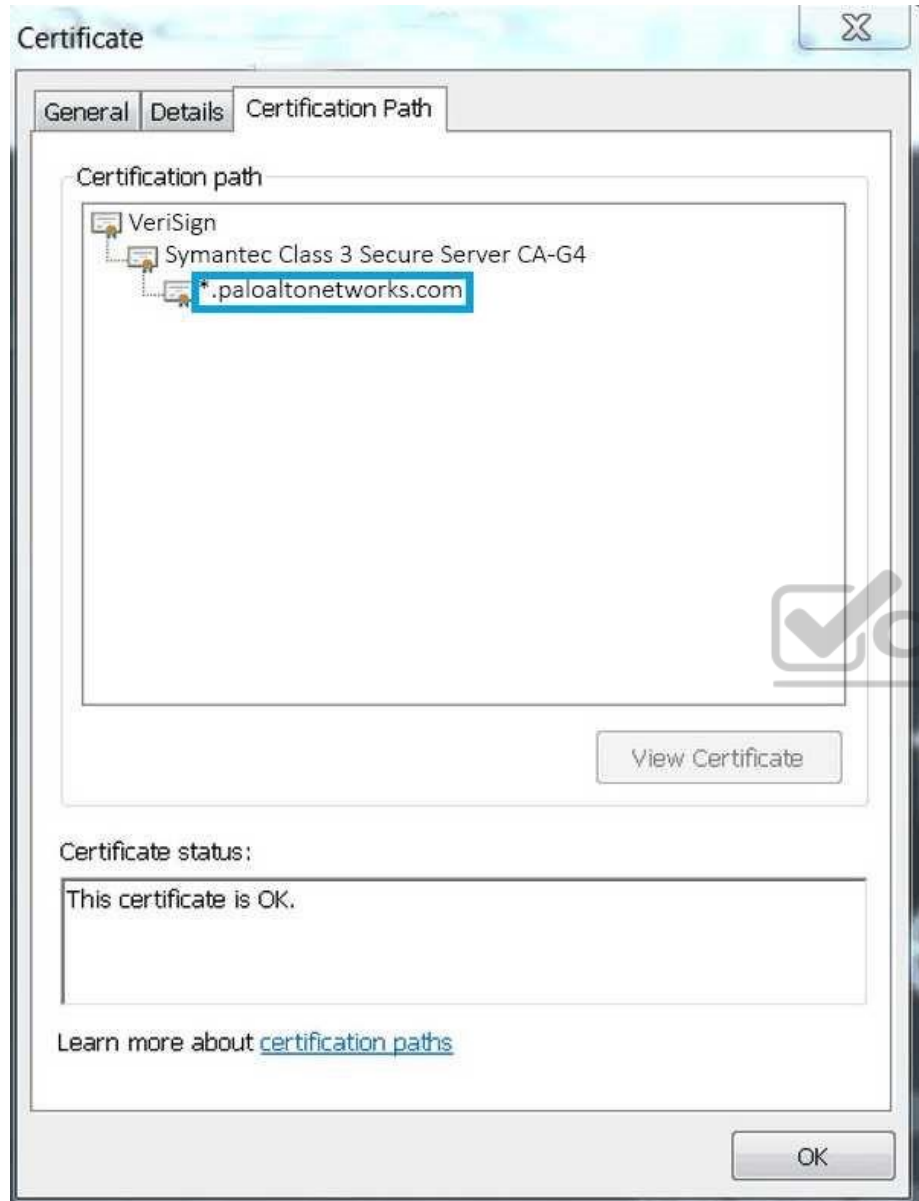
**Explanation**

**Explanation/Reference:**

#### QUESTION 62

Based on the following image, what is the correct path of root, intermediate, and end-user certificate?





A. Palo Alto Networks > Symantec > VeriSign

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 63

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. Download and install application updates cannot be done automatically if the MGT port cannot reach the Internet.
- B. 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.
- C. 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.
- D. Configure a Security policy rule to allow all traffic to and from the update servers.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 64

A company wants to install a NGFW 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 option differentiates multiple VLANs into separate zones?

- A. Create V-Wire objects with two V-Wire interfaces and define a range of "0-4096" in the "Tag Allowed" field of the V-Wire object.

- B. Create V-Wire objects with two V-Wire subinterfaces and assign only a single VLAN ID to the “Tag Allowed” field of the V-Wire object. Repeat for every additional VLAN and use a VLAN ID of 0 for untagged traffic. Assign each interface/subinterface to a unique zone.
- C. Create Layer 3 subinterfaces that are each assigned to a single VLAN ID and a common virtual router. The physical Layer 3 interface would handle untagged traffic. Assign each interface/subinterface to a unique zone. Do not assign any interface an IP address.
- D. Create VLAN objects for each VLAN and assign VLAN interfaces matching each VLAN ID. Repeat for every additional VLAN and use a VLAN ID of 0 for untagged traffic. Assign each interface/subinterface to a unique zone.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 65

Where can an administrator see both the management plane and data plane CPU utilization in the WebUI?

- A. System Utilization log
- B. System log
- C. Resources widget
- D. CPU Utilization widget



**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 66

Which two features does PAN-OS® software use to identify applications? (Choose two.)

- A. transaction characteristics
- B. session number
- C. port number
- D. application layer payload

**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 67**

An administrator wants to upgrade an NGFW from PAN-OS® 7.1.2 to PAN-OS® 8.1.0. The firewall is not a part of an HA pair.

What needs to be updated first?

- A. Applications and Threats
- B. XML Agent
- C. WildFire
- D. PAN-OS® Upgrade Agent

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**



**QUESTION 68**

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

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 69**

The firewall determines if a packet is the first packet of a new session or if a packet is part of an existing session using which kind of match?

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 70**

Which GlobalProtect Client connect method requires the distribution and use of machine certificates?

- A. At-boot
- B. Pre-logon
- C. User-logon (Always on)
- D. On-demand

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 71**

Which feature can provide NGFWs with User-ID mapping information?

- A. Web Captcha

- B. Native 802.1q authentication
- C. GlobalProtect
- D. Native 802.1x authentication

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 72

For which two reasons would a firewall discard a packet as part of the packet flow sequence? (Choose two.)

- A. ingress processing errors
- B. rule match with action "deny"
- C. rule match with action "allow"
- D. equal-cost multipath

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 73

An administrator needs to upgrade an NGFW to the most current version of PAN-OS® software. The following is occurring:

- Firewall has internet connectivity through e 1/1.
  - Default security rules and security rules allowing all SSL and web-browsing traffic to and from any zone.
  - Service route is configured, sourcing update traffic from e1/1.
  - A communication error appears in the System logs when updates are performed.
- Download does not complete.

What must be configured to enable the firewall to download the current version of PAN-OS software?

- A. Static route pointing application PaloAlto-updates to the update servers

- B. Security policy rule allowing PaloAlto-updates as the application
- C. Scheduler for timed downloads of PAN-OS software
- D. DNS settings for the firewall to use for resolution

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 74

A firewall administrator has been asked to configure a Palo Alto Networks NGFW to prevent against compromised hosts trying to phone-home or beacon out to external command-and-control (C2) servers.

Which Security Profile type will prevent these behaviors?

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



**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

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

#### QUESTION 75

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

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

**Correct Answer:** A

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Reference: <https://www.paloaltonetworks.com/documentation/81/pan-os/newfeaturesguide/upgrade-to-pan-os-81/upgradedowngrade-considerations>

#### **QUESTION 76**

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

**Correct Answer: AC**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Reference: <https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/certificate-management/set-up-verification-for-certificate-revocation-status>

#### **QUESTION 77**

Which administrative authentication method supports authorization by an external service?

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

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/firewall-administration/manage-firewall-administrators/administrative-authentication>



**QUESTION 78**

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. .fon
- D. .apk
- E. .pdf
- F. .jar

**Correct Answer:** DEF

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 79**

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.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/high-availability/floating-ip-address-and-virtual-mac-address>

**QUESTION 80**

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: [https://www.paloaltonetworks.com/documentation/41/globalprotect/globalprotect-app-new-features/new-features-released-in-gp-agent-4\\_1/split-tunnel-for-public-applications](https://www.paloaltonetworks.com/documentation/41/globalprotect/globalprotect-app-new-features/new-features-released-in-gp-agent-4_1/split-tunnel-for-public-applications)

#### **QUESTION 81**

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.)



Logs

Traffic

Threat

URL Filtering

WildFire Submissions

Data Filtering

HIP Match

User-ID

Tunnel Inspection

Configuration

System

Alarms

Authentication

Unified

Packet Capture

App Scope

Summary

Change Monitor

Threat Monitor

Threat Map

Receive Time	Type	Severity	Event	Object	Description
06/16 08:41:43	general	informational	general		User admin accessed Monitor ta
06/16 08:40:40	general	informational	general		User admin logged in via Web fr 192.168.55.1 using https. authenticated for user 'admin'. F 192.168.55.1.
06/16 08:40:40	auth	informational	auth-success		LOGIN ON tty1 BY admin.
06/16 08:40:06	general	informational	general		User admin logged in via CLI fro
06/16 08:39:43	general	informational	general		
06/16 08:39:42	auth	informational	auth-success		authenticated for user 'admin'. F
06/16 08:39:16	url-filtering	informational	upgrade-url-database- success		PAN-DB was upgraded to versio 20170615.40151.
06/16 08:34:15	url-filtering	informational	upgrade-url-database- success		PAN-DB was upgraded to versio 20170615.40150.
06/16 08:31:44	general	informational	general		Failed to connect to Panorama 192.168.55.5 Port: 3978 Retry:
06/16 08:31:40	ntpd	informational	restart		NTP restart synchronization per
06/16 08:31:33	general	informational	general		Commit job succeeded. Comple time=2017/06/16 05:31:33. Jobl User:admin

A.

## ▼ Logs

## Traffic

## Threat

## URL Filtering

## WildFire Submissions

## Data Filtering

## HIP Match

## User-ID

## Tunnel Inspection

## Configuration

## System

## Alarms

## Authentication

## Unified

## Packet Capture

## ▼ App Scope

## Summary

	Receive Time	Type	From Zone	To Zone	Source	Source User	Destination
	06/14 08:14:14	end	inside	outside	192.168.45.1		192.168.45.1
	06/14 08:13:44	drop	outside	outside	192.168.55.1		192.168.55.1
	06/14 08:04:14	end	inside	outside	192.168.45.1		192.168.45.1
	06/14 08:03:45	drop	outside	outside	192.168.55.1		192.168.55.1
	06/14 07:59:36	end	inside	outside	192.168.45.1		192.168.45.1
	06/14 07:59:06	drop	outside	outside	192.168.55.1		192.168.55.1
	06/14 07:40:27	end	inside	outside	192.168.45.1		192.168.45.1
	06/14 07:39:57	drop	outside	outside	192.168.55.1		192.168.55.1
	06/14 07:39:56	drop	outside	outside	192.168.55.1		192.168.55.1
	06/14 07:39:55	drop	outside	outside	192.168.55.1		192.168.55.1

B. 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
<u>05/23 20:47:24</u>	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



**Task Manager - All Tasks**

32 items

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		
<a href="#">Commit</a>	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	

Show All Tasks

Close

D.

Correct Answer: AD

**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### **QUESTION 82**

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.

**Correct Answer: AD**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Reference: <https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/objects/objects-decryption-profile>

#### **QUESTION 83**

SAML SLO is supported for which two firewall features? (Choose two.)

- A. GlobalProtect Portal
- B. CaptivePortal
- C. WebUI
- D. CLI

**Correct Answer: AB**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

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

**QUESTION 84**

What are the two behavior differences between Highlight Unused Rules and the Rule Usage Hit counter when a firewall is rebooted? (Choose two.)

- A. Rule Usage Hit counter will not be reset
- B. Highlight Unused Rules will highlight all rules.
- C. Highlight Unused Rules will highlight zero rules.
- D. Rule Usage Hit counter will reset.

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 85**

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



**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://www.paloaltonetworks.com/documentation/71/pan-os/newfeaturesguide/networking-features/ssl-ssh-session-end-reasons>

**QUESTION 86**

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.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://www.paloaltonetworks.com/documentation/81/pan-os/newfeaturesguide/panorama-features/device-monitoring-through-panorama>

#### QUESTION 87

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

**Correct Answer:** ABC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://www.paloaltonetworks.com/documentation/81/pan-os/newfeaturesguide/globalprotect-features/split-tunnel-for-public-applications>



<https://vcceplus.com/>



<https://vcceplus.com/>