



Paloalto-Networks

Exam Questions PCNSE

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

NEW QUESTION 1

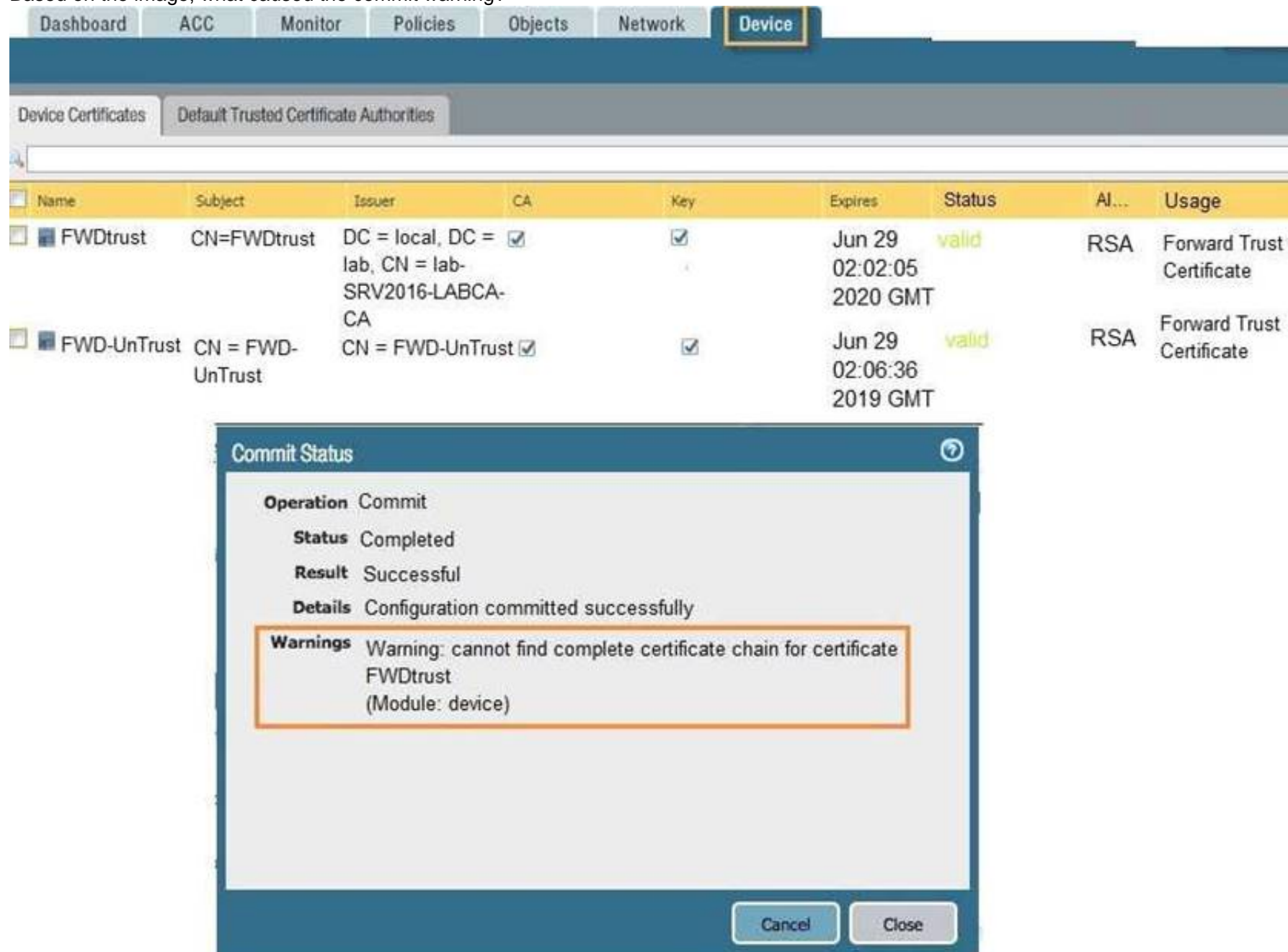
SAML SLO is supported for which two firewall features? (Choose two.)

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

Answer: AB

NEW QUESTION 2

Based on the image, what caused the commit warning?



The screenshot shows the Palo Alto Networks GUI with the 'Device' tab selected. Under 'Device Certificates', there are two certificates listed:

Name	Subject	Issuer	CA	Key	Expires	Status	AI...	Usage
FWDtrust	CN=FWDtrust	DC = local, DC = lab, CN = lab-SRV2016-LABCA-CA	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Jun 29 02:02:05 2020 GMT	valid	RSA	Forward Trust Certificate
FWD-UnTrust	CN = FWD-UnTrust	CN = FWD-UnTrust	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Jun 29 02:06:36 2019 GMT	valid	RSA	Forward Trust Certificate

A 'Commit Status' dialog box is open, showing the following details:

- Operation:** Commit
- Status:** Completed
- Result:** Successful
- Details:** Configuration committed successfully
- Warnings:** Warning: cannot find complete certificate chain for certificate FWDtrust (Module: device)

- 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.

Answer: D

NEW QUESTION 3

Which administrative authentication method supports authorization by an external service?

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

Answer: C

NEW QUESTION 4

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 5

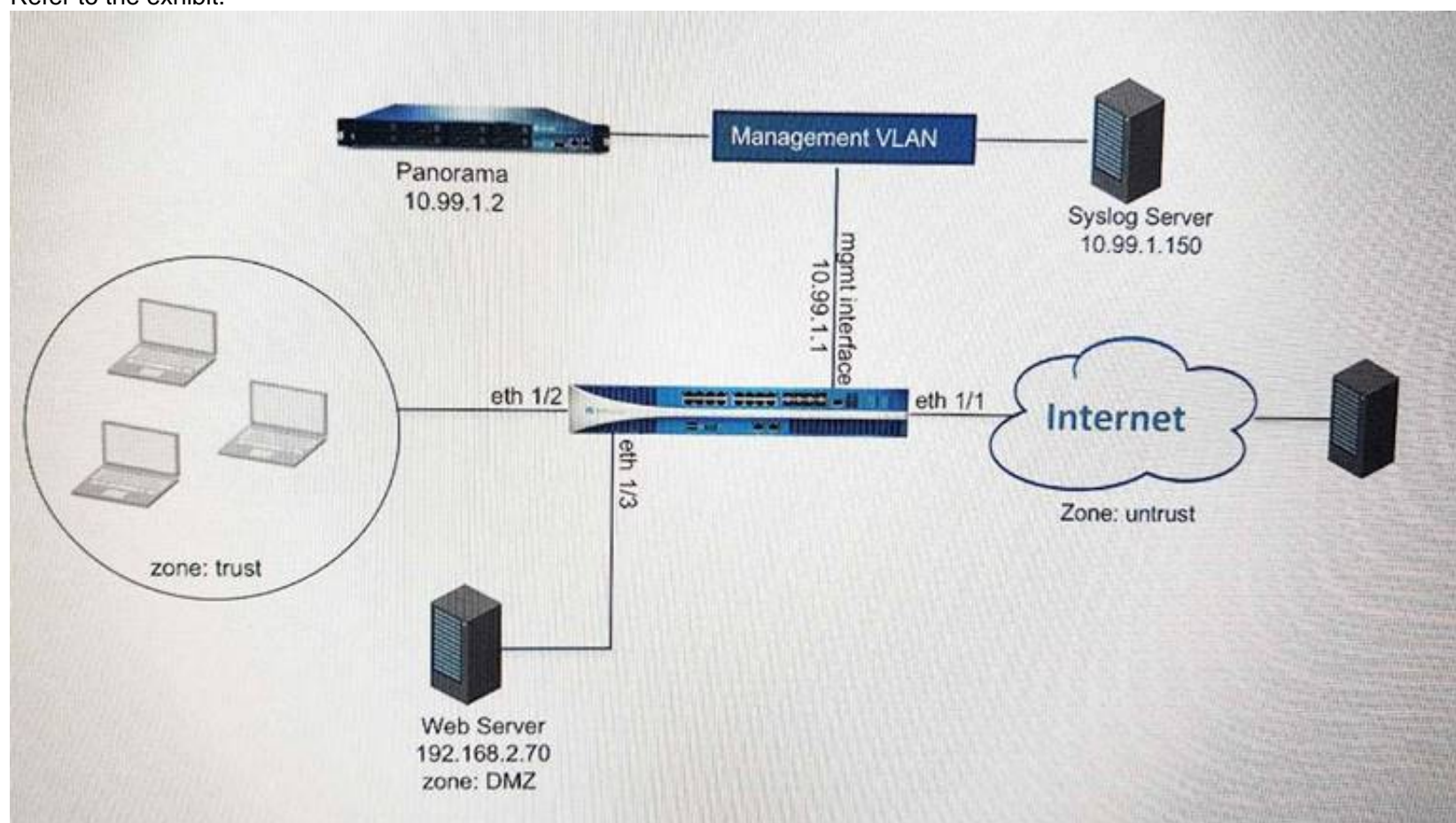
An administrator pushes a new configuration from Panorama to a pair of firewalls that are configured as an active/passive HA pair. Which NGFW receives the configuration from Panorama?

- 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

Answer: C

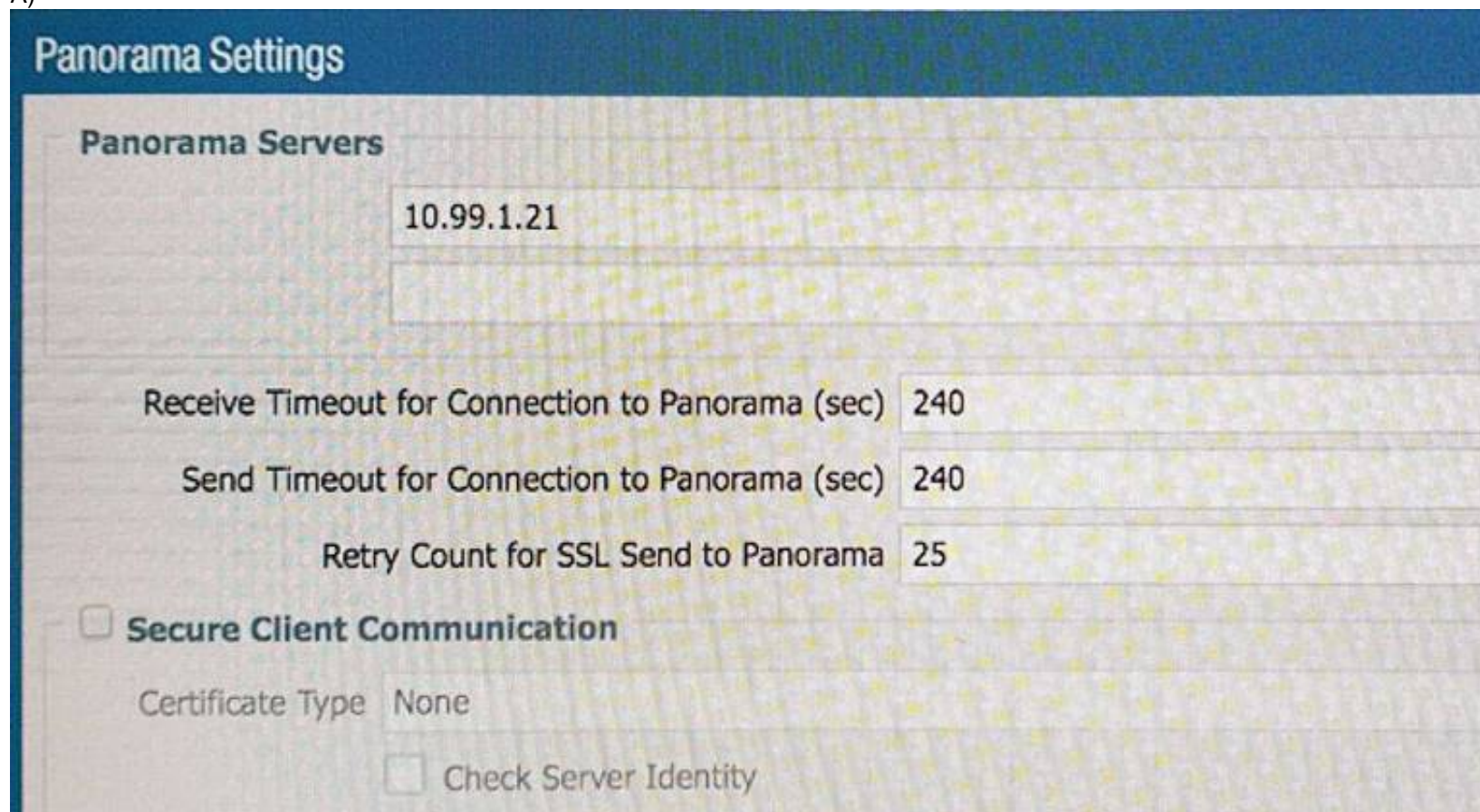
NEW QUESTION 6

Refer to the exhibit.



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

A)



B)

Security Policy Rule

General

Source

User

Destination

Application

Service/URL Category

Actions

Action Setting

Action

Allow

Send ICMP Unreachable

Log Setting

☒ Log at Session Start
 ☒ Log at Session End

Log Forwarding

None

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

Other Settings

Schedule

None

QoS Marking

None

☐ Disable Server Response Inspection

OK

Cancel

C)

Syslog Server Profile

Name

SyslogProfile1

Servers

Custom Log Format

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

Add

Delete

D)

Panorama Settings

Receive Timeout for Connection to Device (sec) 240

Send Timeout for Connection to Device (sec) 240

Retry Count for SSL Send to Device 25

☒ Share Unused Address and Service Objects with Devices

☐ Objects defined in ancestors will take higher precedence

Secure Server Communication

☐ Custom Certificate Only

SSL/TLS Service Profile None

Certificate Profile None

Authorization List

Identifier	Type	Value
0 items		

[Add](#) [Delete](#)

☐ Authorize Clients Based on Serial Number

☐ Check Authorization List

Connect Wait Time (min) [0 - 44640]

OK

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

Answer: D

NEW QUESTION 7

To connect the Palo Alto Networks firewall to AutoFocus, which setting must be enabled?

- A. Device>Setup>Services>AutoFocus
- B. Device> Setup>Management >AutoFocus
- C. AutoFocus is enabled by default on the Palo Alto Networks NGFW
- D. Device>Setup>WildFire>AutoFocus
- E. Device>Setup> Management> Logging and Reporting Settings

Answer: B

Explanation:

Reference: <https://www.paloaltoHYPERLINK>

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

NEW QUESTION 8

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 9

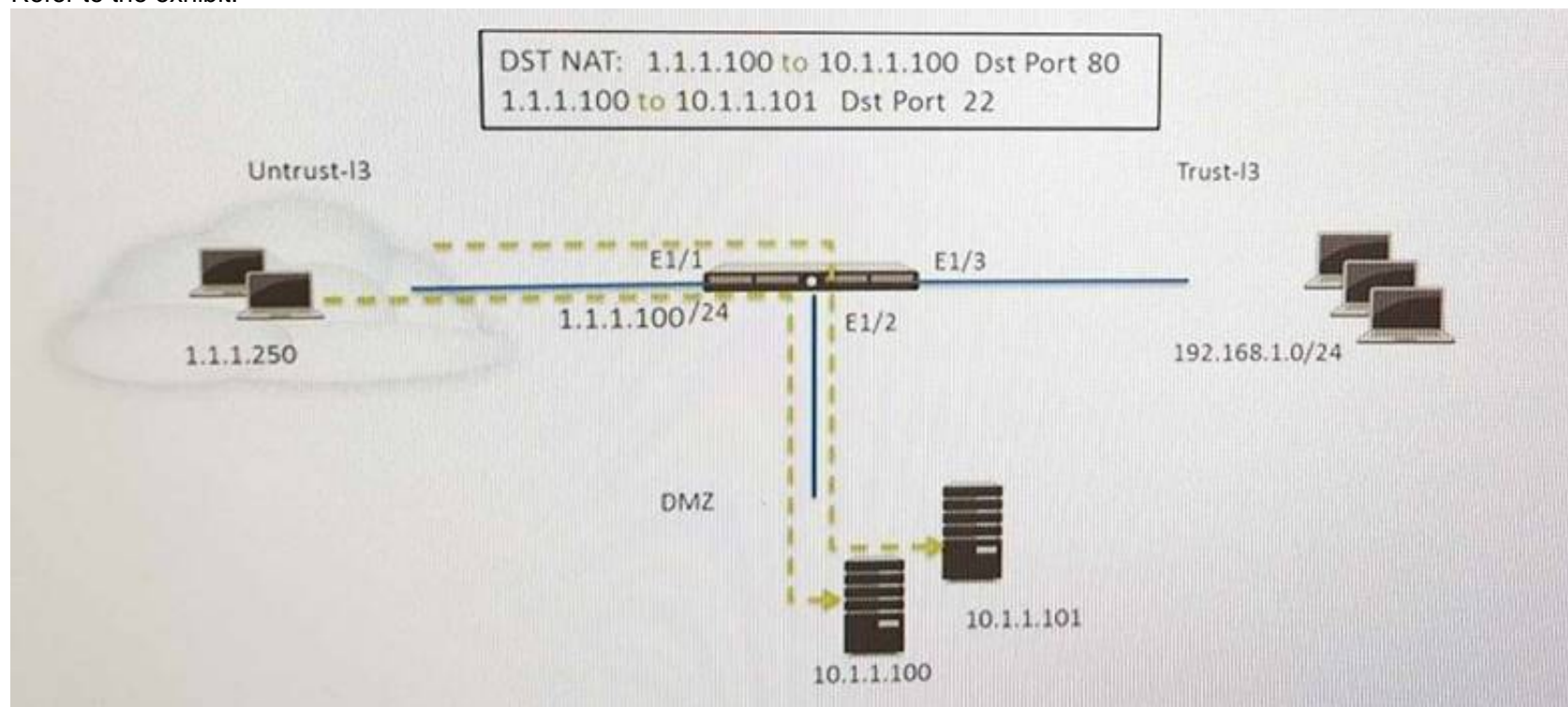
What are two benefits of nested device groups in Panorama? (Choose two.)

- A. Reuse of the existing Security policy rules and objects
- B. Requires configuring both function and location for every device
- C. All device groups inherit settings from the Shared group
- D. Overwrites local firewall configuration

Answer: BC

NEW QUESTION 10

Refer to the exhibit.



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

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

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

Answer: CD

NEW QUESTION 10

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

How quickly will the firewall receive back a verdict?

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

Answer: D

NEW QUESTION 12

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 15

An administrator creates a custom application containing Layer 7 signatures. The latest application and threat dynamic update is downloaded to the same NGFW.

The update contains an application that matches the same traffic signatures as the custom application. Which application should be used to identify traffic traversing the NGFW?

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

Answer: A

NEW QUESTION 20

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 23

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 27

Which option is part of the content inspection process?

- A. Packet forwarding process
- B. SSL Proxy re-encrypt
- C. IPsec tunnel encryption
- D. Packet egress process

Answer: A

NEW QUESTION 31

Which protection feature is available only in a Zone Protection Profile?

- A. SYN Flood Protection using SYN Flood Cookies
- B. ICMP Flood Protection
- C. Port Scan Protection
- D. UDP Flood Protections

Answer: A

NEW QUESTION 36

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 37

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

Which option would achieve this result?

- A. Create a custom App-ID and enable scanning on the advanced tab.
- B. Create an Application Override policy.

- C. Create a custom App-ID and use the “ordered conditions” check box.
- D. Create an Application Override policy and custom threat signature for the application.

Answer: A

NEW QUESTION 41

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 44

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
```

```
#####
```

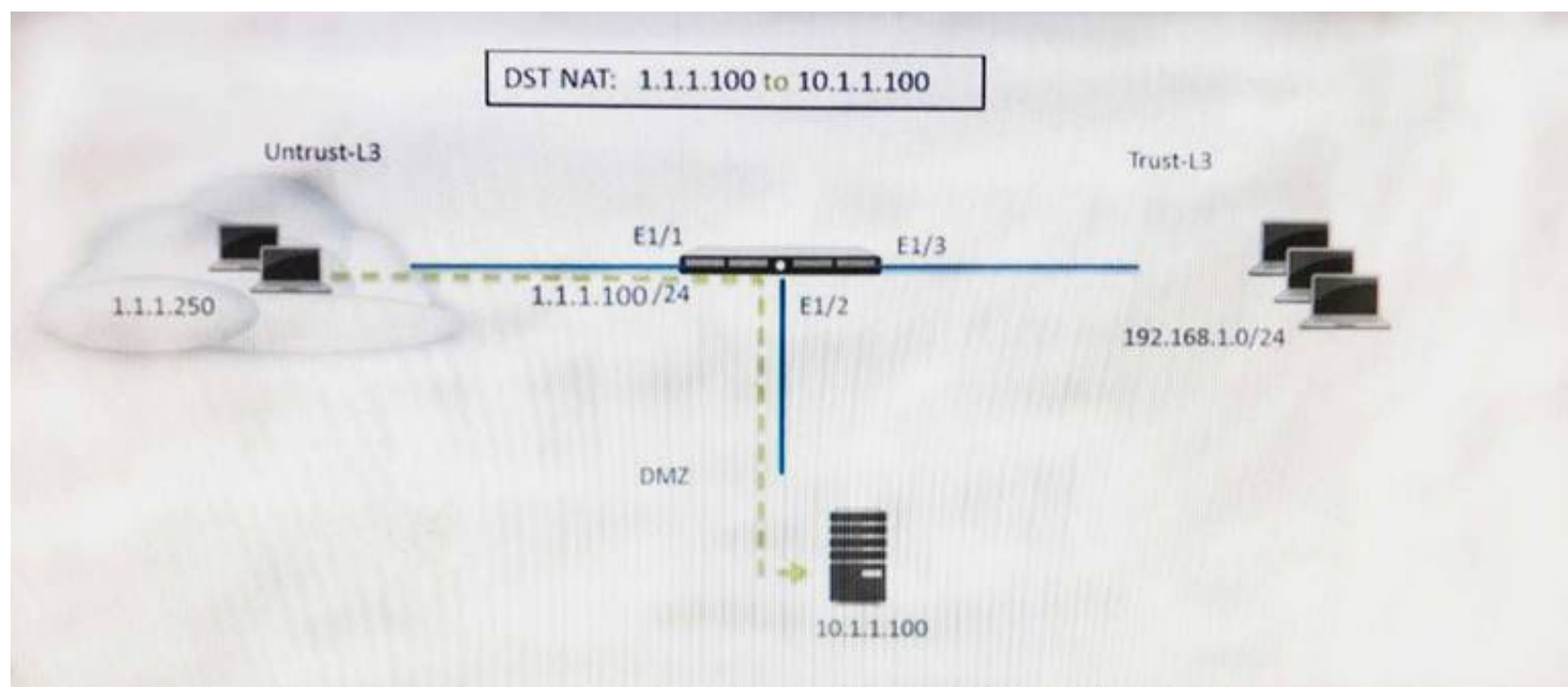
What will be the egress interface if the traffic's ingress interface is ethernet1/6 sourcing from 192.168.111.3 and to the destination 10.46.41.113 during the time shown in the image?

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

Answer: D

NEW QUESTION 48

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 50

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 53

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

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

Answer: A

NEW QUESTION 57

Which DoS protection mechanism detects and prevents session exhaustion attacks?

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

Answer: C

Explanation:

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

NEW QUESTION 60

Which two subscriptions are available when configuring panorama to push dynamic updates to connected devices? (Choose two.)

- A. Content-ID
- B. User-ID
- C. Applications and Threats
- D. Antivirus

Answer: CD

Explanation:

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

NEW QUESTION 65

What is exchanged through the HA2 link?

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

Answer: C

Explanation:

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

NEW QUESTION 66

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

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

Answer: AC

NEW QUESTION 68

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 73

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 77

Which operation will impact the performance of the management plane?

- A. WildFire Submissions
- B. DoS Protection
- C. decrypting SSL Sessions
- D. Generating a SaaS Application Report.

Answer: C

NEW QUESTION 78

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

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

Answer: D

NEW QUESTION 79

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

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

Answer: D

NEW QUESTION 83

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

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

Answer: B

NEW QUESTION 84

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

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

Answer: A

NEW QUESTION 89

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 94

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 99

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

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

Answer: B

NEW QUESTION 100

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 101

Which two statements are correct for the out-of-box configuration for Palo Alto Networks NGFWs? (Choose two)

- A. The devices are pre-configured with a virtual wire pair out the first two interfaces.
- B. The devices are licensed and ready for deployment.
- C. The management interface has an IP address of 192.168.1.1 and allows SSH and HTTPS connections.
- D. A default bidirectional rule is configured that allows Untrust zone traffic to go to the Trust zone.
- E. The interface are pingable.

Answer:

BC

NEW QUESTION 106

A company has a pair of Palo Alto Networks firewalls configured as an Active/Passive High Availability (HA) pair. What allows the firewall administrator to determine the last date a failover event occurred?

- A. From the CLI issue use the show System log
- B. Apply the filter subtype eq ha to the System log
- C. Apply the filter subtype eq ha to the configuration log
- D. Check the status of the High Availability widget on the Dashboard of the GUI

Answer: B

NEW QUESTION 108

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

less mp-log ikemgr.log:

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

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

What could be the cause of this problem?

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

Answer: B

NEW QUESTION 111

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

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

Answer: D

Explanation:

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

NEW QUESTION 112

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

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

Answer: A

Explanation:

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

NEW QUESTION 115

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 118

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

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

Answer: ABF

NEW QUESTION 120

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

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

Answer: BD

NEW QUESTION 125

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 129

Company.com has an in-house application that the Palo Alto Networks device doesn't identify correctly. A Threat Management Team member has mentioned that this in-house application is very sensitive and all traffic being identified needs to be inspected by the Content-ID engine.

Which method should company.com use to immediately address this traffic on a Palo Alto Networks device?

- A. Create a custom Application without signatures, then create an Application Override policy that includes the source, Destination, Destination Port/Protocol and Custom Application of the traffic.
- B. Wait until an official Application signature is provided from Palo Alto Networks.
- C. Modify the session timer settings on the closest referenced application to meet the needs of the in-house application
- D. Create a Custom Application with signatures matching unique identifiers of the in-house application traffic

Answer: D

NEW QUESTION 133

A network security engineer has been asked to analyze Wildfire activity. However, the Wildfire Submissions item is not visible from the Monitor tab. What could cause this condition?

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

Answer: B

NEW QUESTION 138

A network administrator uses Panorama to push security policies to managed firewalls at branch offices. Which policy type should be configured on Panorama if the administrators at the branch office sites to override these products?

- A. Pre Rules
- B. Post Rules
- C. Explicit Rules
- D. Implicit Rules

Answer: A

NEW QUESTION 143

A company has a policy that denies all applications it classifies as bad and permits only application it classifies as good. The firewall administrator created the following security policy on the company's firewall.

	Source				Destination				Action	Profile	Options
	Name	Zone	Address	User	Zone	Address	Application	Service			
1	rule1	Trust-L3	any	any	UnTrust-L3	any	Known Good	application-default	allow	none	
2	rule2	Trust-L3	any	any	UnTrust-L3	any	Known Bad	any	deny	none	
3	rule3	Trust-L3	any	any	UnTrust-L3	any	any	any	deny	none	

Which interface configuration will accept specific VLAN IDs?

Which two benefits are gained from having both rule 2 and rule 3 presents? (choose two)

- A. A report can be created that identifies unclassified traffic on the network.
- B. Different security profiles can be applied to traffic matching rules 2 and 3.
- C. Rule 2 and 3 apply to traffic on different ports.
- D. Separate Log Forwarding profiles can be applied to rules 2 and 3.

Answer: BD

NEW QUESTION 148

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 153

Which option is an IPv6 routing protocol?

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

Answer: B

NEW QUESTION 156

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 159

People are having intermittent quality issues during a live meeting via web application.

- A. Use QoS profile to define QoS Classes
- B. Use QoS Classes to define QoS Profile
- C. Use QoS Profile to define QoS Classes and a QoS Policy
- D. Use QoS Classes to define QoS Profile and a QoS Policy

Answer: C

NEW QUESTION 163

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 168

Which CLI command displays the current management plan memory utilization?

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

Answer: B

Explanation:

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

NEW QUESTION 172

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

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

Answer: ABC

Explanation:

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

NEW QUESTION 177

Which two logs on the firewall will contain authentication-related information useful for troubleshooting purpose (Choose two)

- A. ms.log
- B. traffic.log
- C. system.log
- D. dp-monitor.log
- E. authd.log

Answer: CE

NEW QUESTION 179

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

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

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

Answer: D

NEW QUESTION 182

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 186

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

PCNSE Practice Exam Features:

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

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