

# 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

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-vsyz Session Threshold alerts and triggers for Packet Buffer Limits.Enable Zone Buffer Protection per zone.

**Answer:** A

### NEW QUESTION 3

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

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

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

**Answer:** C

### NEW QUESTION 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

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 6

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 7**

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

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

**Answer: A**

**NEW QUESTION 8**

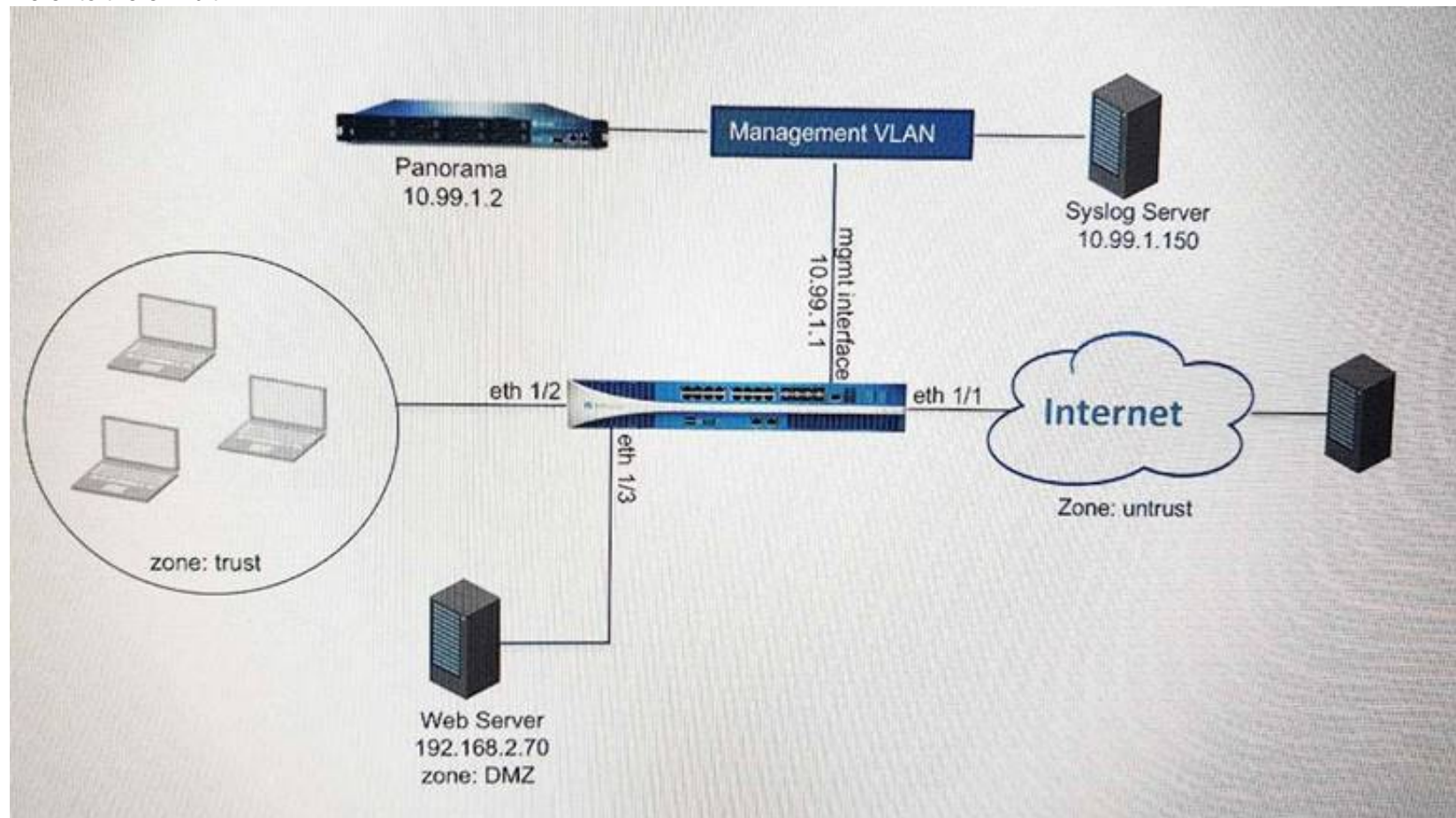
An administrator pushes a new configuration from Panorama to a pair of firewalls that are configured as an active/passive HA pair. Which NGFW receives the configuration from Panorama?

- 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 9**

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

**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		

☐ 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 10

When configuring a GlobalProtect Portal, what is the purpose of specifying an Authentication Profile?

- A. To enable Gateway authentication to the Portal
- B. To enable Portal authentication to the Gateway
- C. To enable user authentication to the Portal
- D. To enable client machine authentication to the Portal

**Answer: C**

#### Explanation:

The additional options of Browser and Satellite enable you to specify the authentication profile to use for specific scenarios. Select Browser to specify the authentication profile to use to authenticate a user accessing the portal from a web browser with the intent of downloading the GlobalProtect agent (Windows and Mac). Select Satellite to specify the authentication profile to use to authenticate the satellite.

Reference <https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/globalprotect/network-globalprotect-portals>

#### NEW QUESTION 10

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 15

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.

**Answer:** A

#### NEW QUESTION 17

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

#### NEW QUESTION 21

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

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

**Answer:** BD

#### Explanation:

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

#### NEW QUESTION 26

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 29

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 30

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 31

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 36

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.

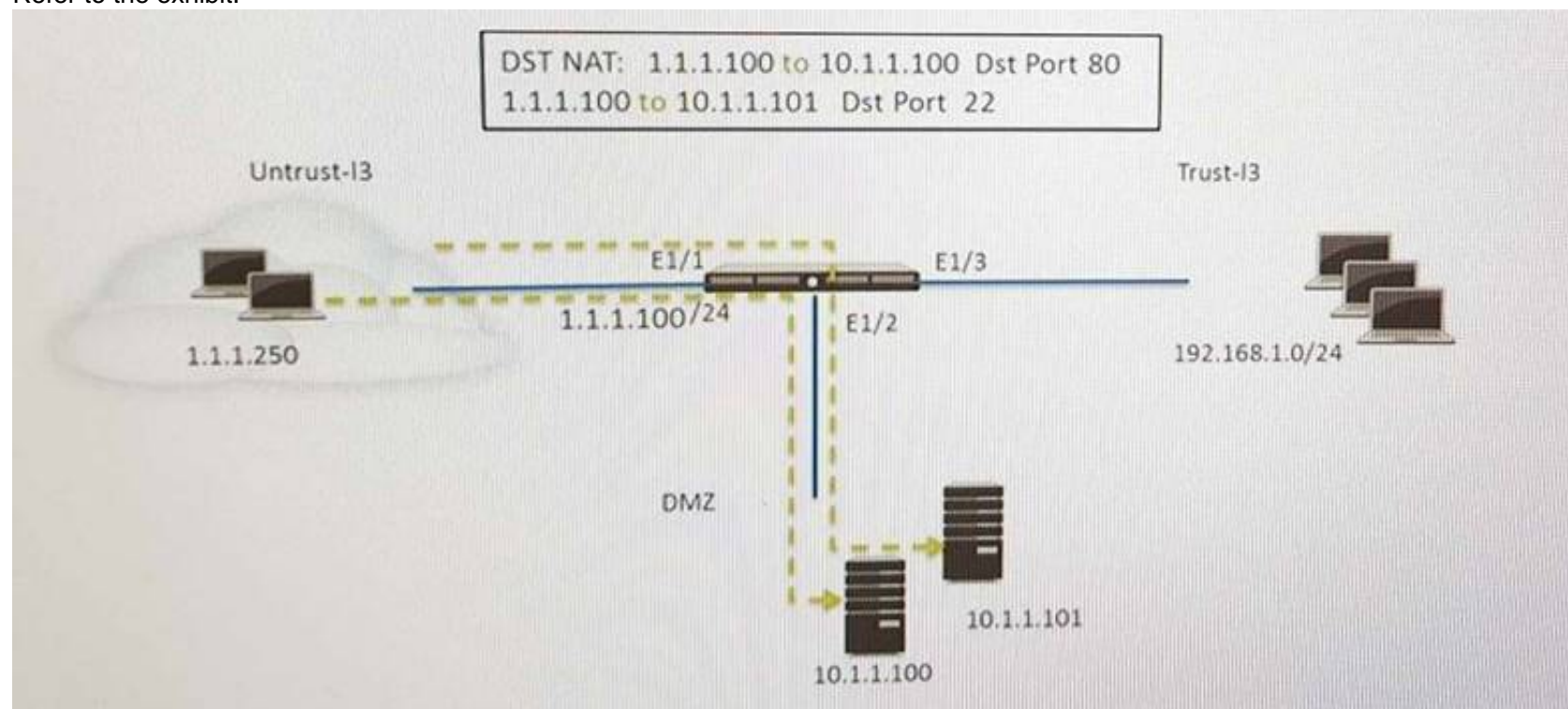
**Answer: D**

#### Explanation:

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

#### NEW QUESTION 38

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

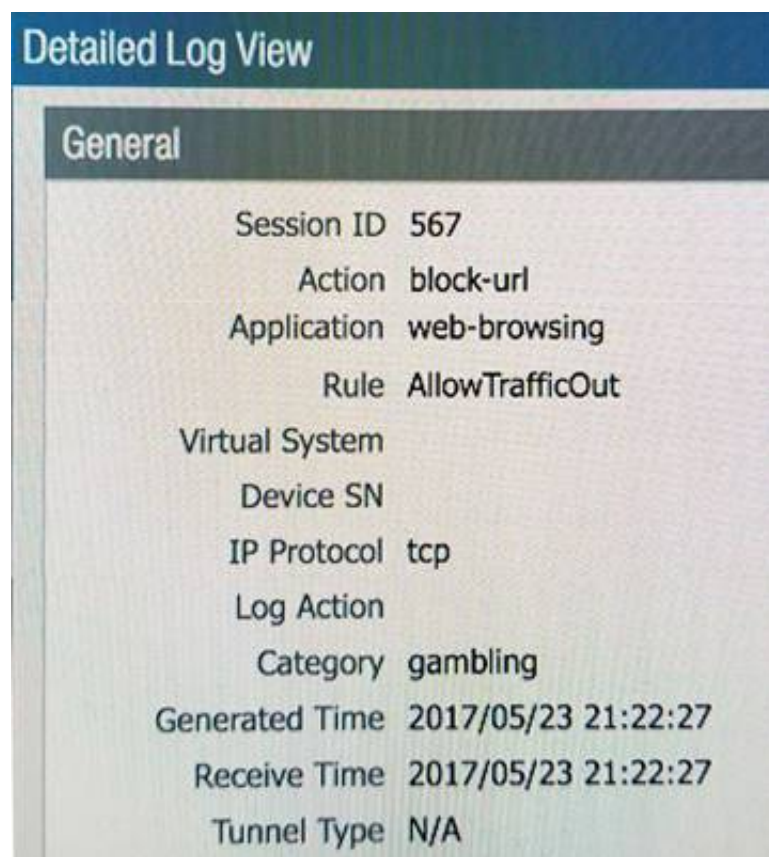
**Answer: CD**

#### NEW QUESTION 40

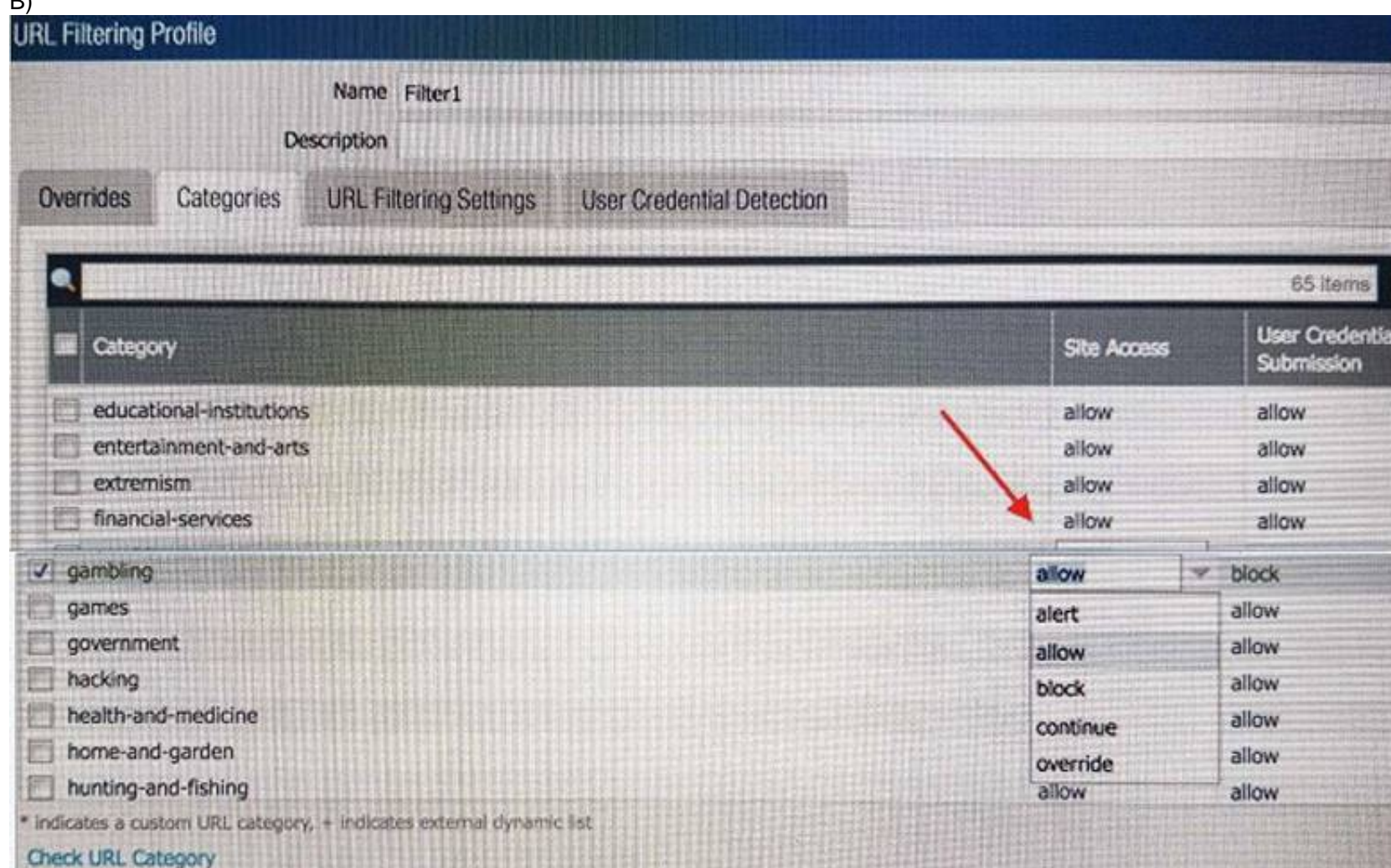
An administrator needs to determine why users on the trust zone cannot reach certain websites. The only information available is shown on the following image. Which configuration change should the administrator make?

A)

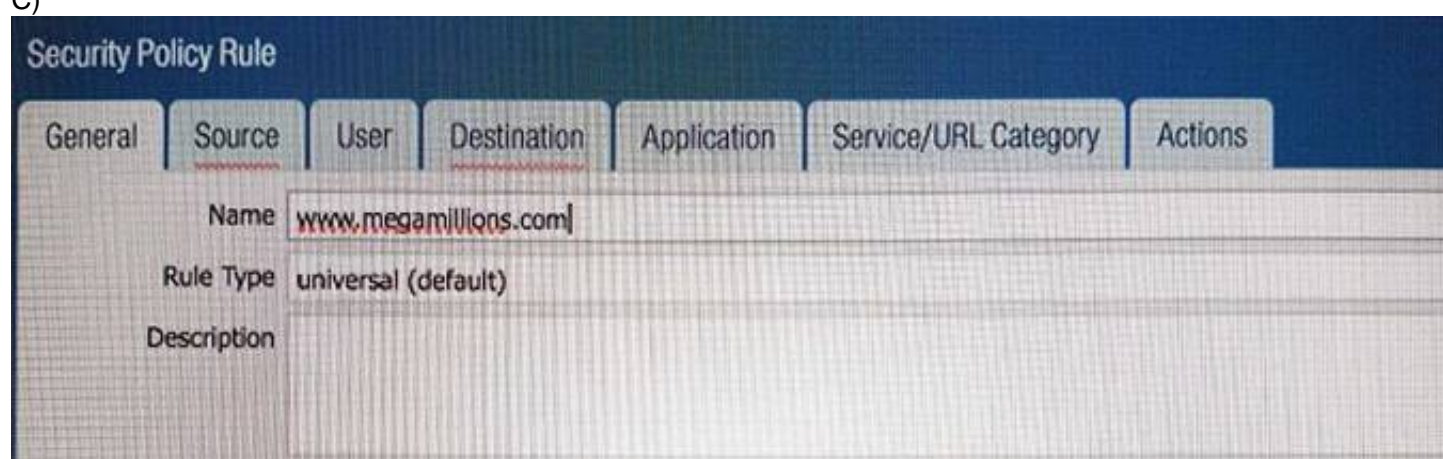




B)



C)



D)



**URL Filtering Profile**

Name: Filter1

Description:

Overrides: Categories URL Filtering Settings User Credential Detection

Allow List: www.megamillions.com

Block List:

Action: continue

For the block list and allow list enter one entry per row, separating the rows with a newline. Each entry should be in the form of "www.example.com" without quotes or an IP address (http:// or https:// should not be included). Use separators to specify match criteria - for example, "www.example.com/test" will match "www.example.com/test" but not match "www.example.com.hk"

OK

E)

**URL Filtering Profile**

Name: Filter1

Description:

Overrides: Categories URL Filtering Settings User Credential Detection

Allow List: www.megamillions.com

Block List:

Action: block

- 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 45**

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 46**

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 48

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 51

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 55

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 56

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 59

An administrator has users accessing network resources through Citrix XenApp 7 x. Which User-ID mapping solution will map multiple users who are using Citrix to connect to the network and access resources?

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

**Answer:** B

#### NEW QUESTION 61

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

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

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

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

**Answer:** D

#### NEW QUESTION 65

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 68

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 70

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

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

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

**Answer:** D

#### Explanation:

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

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

#### NEW QUESTION 71

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.

**Answer:** BD

#### NEW QUESTION 73

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

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 77

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 78

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

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

E. Suspended

**Answer:** ADE

**Explanation:**

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

#### NEW QUESTION 82

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 87

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

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

**Answer:** A

**Explanation:**

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

#### NEW QUESTION 89

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 93

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 97

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 102

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 106**

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 108**

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 109**

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 111**

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 112**

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 117**

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 118**

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 119**

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

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

**Answer:** BCEF

**NEW QUESTION 120**

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

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

**Answer:** C

**NEW QUESTION 124**

Which three firewall states are valid? (Choose three)

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

**Answer:** ABC

**NEW QUESTION 129**

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 133**

An administrator has configured a QoS policy rule and a QoS profile that limits the maximum allowable bandwidth for the YouTube application. However , YouTube is consuming more than the maximum bandwidth allotment configured.

Which configuration step needs to be configured to enable QoS?

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

**Answer:** C

**NEW QUESTION 136**

Which 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 137**

Which User-ID method maps IP address to usernames for users connecting through a web proxy that has already authenticated the user?

- A. Client Probing
- B. Port mapping
- C. Server monitoring
- D. Syslog listening

**Answer:** D

**NEW QUESTION 139**

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 142**

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 145**

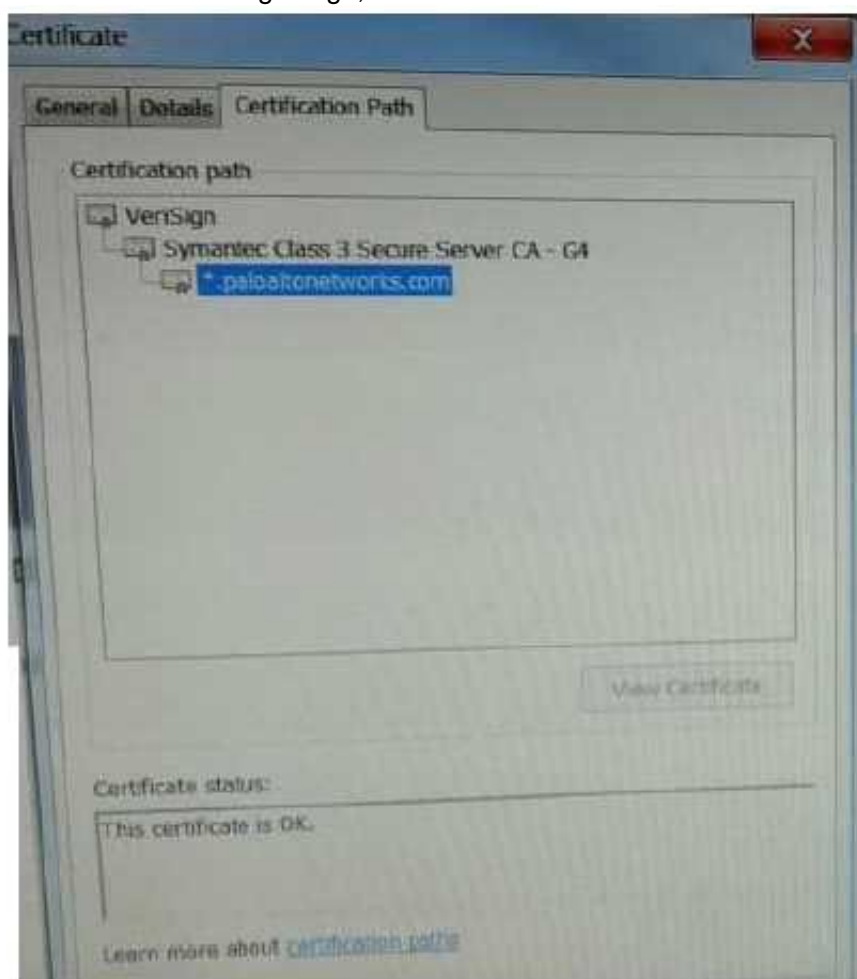
Which Panorama administrator types require the configuration of at least one access domain? (Choose two)

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

**Answer:** DE

**NEW QUESTION 149**

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 154

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 156

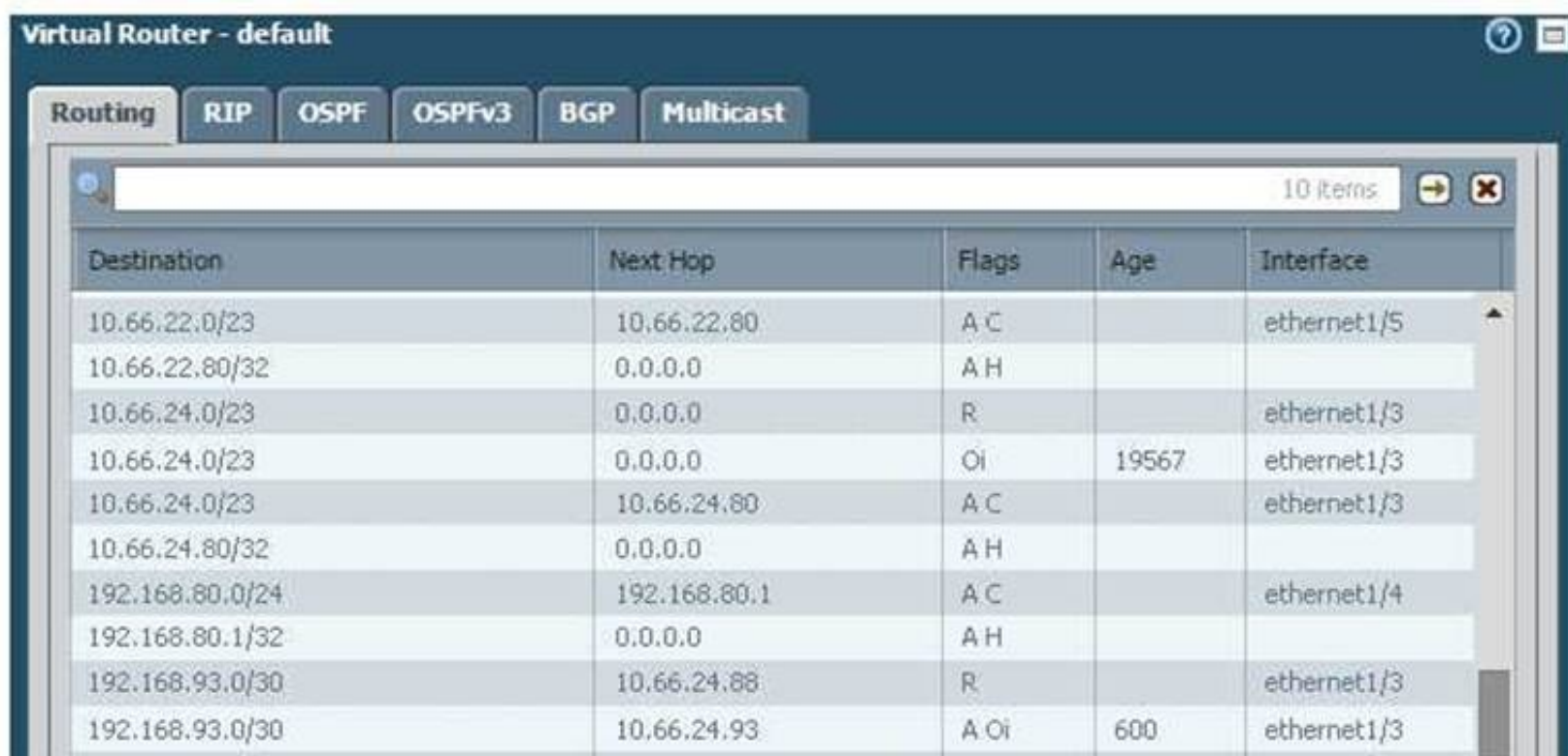
A host attached to Ethernet 1/4 cannot ping the default gateway. The widget on the dashboard shows Ethernet 1/1 and Ethernet 1/4 to be green. The IP address of Ethernet 1/1 is 192.168.1.7 and the IP address of Ethernet 1/4 is 10.1.1.7. The default gateway is attached to Ethernet 1/1. A default route 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 159

Given the following table.



Destination	Next Hop	Flags	Age	Interface
10.66.22.0/23	10.66.22.80	A C		ethernet1/5
10.66.22.80/32	0.0.0.0	A H		
10.66.24.0/23	0.0.0.0	R		ethernet1/3
10.66.24.0/23	0.0.0.0	Oi	19567	ethernet1/3
10.66.24.0/23	10.66.24.80	A C		ethernet1/3
10.66.24.80/32	0.0.0.0	A H		
192.168.80.0/24	192.168.80.1	A C		ethernet1/4
192.168.80.1/32	0.0.0.0	A H		
192.168.93.0/30	10.66.24.88	R		ethernet1/3
192.168.93.0/30	10.66.24.93	A Oi	600	ethernet1/3

Which configuration change on the firewall would cause it to use 10.66.24.88 as the next hop for the 192.168.93.0/30 network?

- A. Configuring the administrative Distance for RIP to be lower than that of OSPF Int.  
B. Configuring the metric for RIP to be higher than that of OSPF Int.  
C. Configuring the administrative Distance for RIP to be higher than that of OSPF Ext.  
D. Configuring the metric for RIP to be lower than that OSPF Ext.

**Answer: A**

#### NEW QUESTION 164

A company is upgrading its existing Palo Alto Networks firewall from version 7.0.1 to 7.0.4.

Which three methods can the firewall administrator use to install PAN-OS 8.0.4 across the enterprise?( Choose three)

- A. Download PAN-OS 8.0.4 files from the support site and install them on each firewall after manually uploading.  
B. Download PAN-OS 8.0.4 to a USB drive and the firewall will automatically update after the USB drive is inserted in the firewall.  
C. Push the PAN-OS 8.0.4 updates from the support site to install on each firewall.  
D. Push the PAN-OS 8.0.4 update from one firewall to all of the other remaining after updating one firewall.  
E. Download and install PAN-OS 8.0.4 directly on each firewall.  
F. Download and push PAN-OS 8.0.4 from Panorama to each firewall.

**Answer: ACF**

#### NEW QUESTION 169

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 170**

A company hosts a publically accessible web server behind a Palo Alto Networks next generation firewall with the following configuration information. Users outside the company are in the "Untrust-L3" zone The web server physically resides in the "Trust-L3" zone. Web server public IP address: 23.54.6.10 Web server private IP address: 192.168.1.10 Which two items must be NAT policy contain to allow users in the untrust-L3 zone to access the web server? (Choose two)

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

**Answer:** CD

**NEW QUESTION 174**

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 176**

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

- A. Configure the management interface as HA3 Backup
- B. Configure Ethernet 1/1 as HA1 Backup
- C. Configure Ethernet 1/1 as HA2 Backup
- D. Configure the management interface as HA2 Backup
- E. Configure the management interface as HA1 Backup
- F. Configure ethernet1/1 as HA3 Backup

**Answer:** BE

**NEW QUESTION 181**

What are three valid actions in a File Blocking Profile? (Choose three)

- A. Forward
- B. Block
- C. Alert
- D. Upload
- E. Reset-both
- F. Continue

**Answer:** ABC

**Explanation:**

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

**NEW QUESTION 182**

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

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

**Answer:** C

**NEW QUESTION 184**

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 189

Which Public Key infrastructure component is used to authenticate users for GlobalProtect when the Connect Method is set to pre-logon?

- A. Certificate revocation list
- B. Trusted root certificate
- C. Machine certificate
- D. Online Certificate Status Protocol

**Answer: C**

#### NEW QUESTION 190

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

less mp-log ikemgr.log:

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

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

What could be the cause of this problem?

- A. The public IP 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 191

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 193

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 198

A network security engineer is asked to provide a report on bandwidth usage. Which tab in the ACC provides the information needed to create the report?



- A. Blocked Activity
- B. Bandwidth Activity
- C. Threat Activity
- D. Network Activity

**Answer:** D

**NEW QUESTION 202**

Click the Exhibit button below,

Exhibit Window							
				Source		Destination	
	Name	Tags	Zone/Interface	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 204**

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 205**

What are three valid method of user mapping? (Choose three)

- A. Syslog
- B. XML API
- C. 802.1X
- D. WildFire
- E. Server Monitoring

**Answer:** ABE

**NEW QUESTION 206**

Which interface configuration will accept specific VLAN IDs?

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

**Answer:** B

#### NEW QUESTION 211

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.

	Name	Source			Destination			Application	Service	Action	Profile	Options
		Zone	Address	User	Zone	Address	User					
1	rule1	Trust-L3	any	any	UnTrust-L3	any	any	Known Good	application-default	allow	none	
2	rule2	Trust-L3	any	any	UnTrust-L3	any	any	Known Bad	any	deny	none	
3	rule3	Trust-L3	any	any	UnTrust-L3	any	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 215

After pushing a security policy from Panorama to a PA-3020 firwall, the firewall administrator notices that traffic logs from the PA-3020 are not appearing in Panorama's traffic logs. What could be the problem?

- A. A Server Profile has not been configured for logging to this Panorama device.
- B. Panorama is not licensed to receive logs from this particular firewall.
- C. The firewall is not licensed for logging to this Panorama device.
- D. None of the firwwall's policies have been assigned a Log Forwarding profile

**Answer: D**

#### NEW QUESTION 216

A company.com wants to enable Application Override. Given the following screenshot:

Which two statements are true if Source and Destination traffic match the Application Override policy? (Choose two)

- A. Traffic that matches "rtp-base" will bypass the App-ID and Content-ID engines.
- B. Traffic will be forced to operate over UDP Port 16384.
- C. Traffic utilizing UDP Port 16384 will now be identified as "rtp-base".
- D. Traffic utilizing UDP Port 16384 will bypass the App-ID and Content-ID engines.

**Answer: AC**

#### NEW QUESTION 217

A network design calls for a "router on a stick" implementation with a PA-5060 performing inter- VLAN routing All VLAN-tagged traffic will be forwarded to the PA-5060 through a single dot1q trunk interface

Which interface type and configuration setting will support this design?

- A. Trunk interface type with specified tag
- B. Layer 3 interface type with specified tag
- C. Layer 2 interface type with a VLAN assigned
- D. Layer 3 subinterface type with specified tag

**Answer: D**

#### NEW QUESTION 220

Which option is an IPv6 routing protocol?

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

**Answer:** B

**NEW QUESTION 222**

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 225**

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

Which configuration setting needs to be modified?

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

**Answer:** A

**NEW QUESTION 227**

A file sharing application is being permitted and no one knows what this application is used for. How should this application be blocked?

- A. Block all unauthorized applications using a security policy
- B. Block all known internal custom applications
- C. Create a WildFire Analysis Profile that blocks Layer 4 and Layer 7 attacks
- D. Create a File blocking profile that blocks Layer 4 and Layer 7 attacks

**Answer:** D

**NEW QUESTION 229**

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://HYPERLINK "https://live.paloaltonetworks.com/t5/Learning-Articles/How-to-Interpret-show-system-resources/ta-p/59364"](https://live.paloaltonetworks.com/t5/Learning-Articles/How-to-Interpret-show-system-resources/ta-p/59364)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.HYPERLINK "https://live.paloaltonetworks.com/t5/Learning-Articles/How-to-Interpret- show-system-resources/ta-p/59364"](https://live.paloaltonetworks.com/t5/Learning-Articles/How-to-Interpret-show-system-resources/ta-p/59364)paloHYPERLINK

"[https://live.paloaltonetworks.com/t5/Learning-Articles/How-to-Interpret-show-system- resources/ta-p/59364"](https://live.paloaltonetworks.com/t5/Learning-Articles/How-to-Interpret-show-system-resources/ta-p/59364)altonetworHYPERLINK

"[https://live.paloaltonetworks.com/t5/Learning- Articles/How-to-Interpret-show-system-resources/ta-p/59364"](https://live.paloaltonetworks.com/t5/Learning-Articles/How-to-Interpret-show-system-resources/ta-p/59364)ks.com/t5/Learning-Articles/How-to- Interpret-show-system-resources/ta-p/59364

**NEW QUESTION 233**

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 237**

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

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

**Answer:** D



#### NEW QUESTION 242

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 244

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

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

**Answer: AB**

#### NEW QUESTION 247

YouTube videos are consuming too much bandwidth on the network, causing delays in mission-critical traffic. The administrator wants to throttle YouTube traffic. The following interfaces and zones are in use on the firewall:

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

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

Which setting for class 6 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

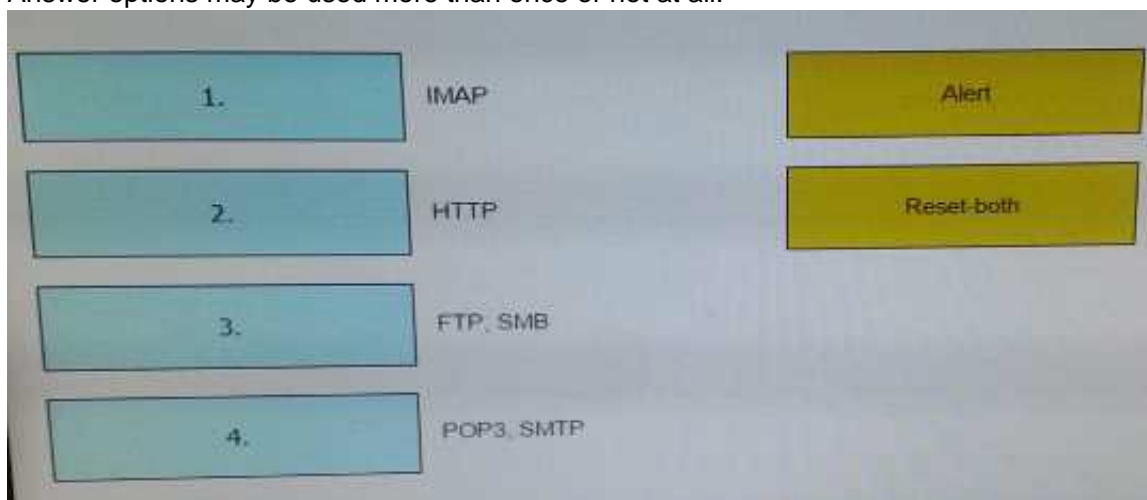
**Answer: D**

#### NEW QUESTION 251

DRAG DROP

When using the predefined default profile, the policy will inspect for viruses on the decoders. Match each decoder with its default action.

Answer options may be used more than once or not at all.



- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

**IMAP, POP3, SMTP -> Alert**

**HTTP, FTP, SMB -> Reset-both**

#### NEW QUESTION 254

.....

## Thank You for Trying Our Product

### We offer two products:

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

2nd - Questons 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](#)**