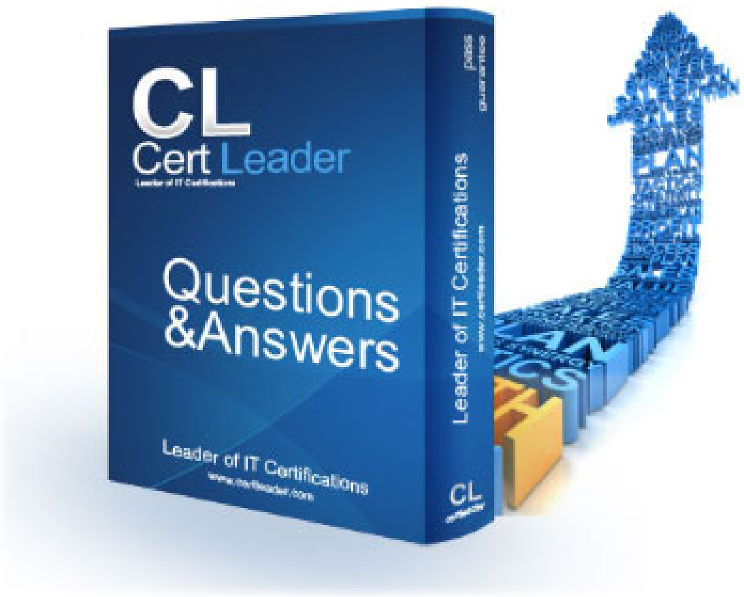
PCNSE Dumps

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

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



NEW QUESTION 1
Which three split tunnel methods are supported by a globalProtect gateway? (Choose three.)

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

Answer: ABC

NEW QUESTION 2
An administrator is defining protection settings on the Palo Alto Networks NGFW to guard against resource exhaustion. When platform utilization is considered, which steps must the administrator take to configure and apply packet buffer protection?

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

Answer: A

NEW QUESTION 3
Which feature can provide NGFWs with User-ID mapping information?

A. Web Captcha
B. Native 802.1q authentication
C. GlobalProtect
D. Native 802.1x authentication

Answer: C

NEW QUESTION 4
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.

Answer: AB

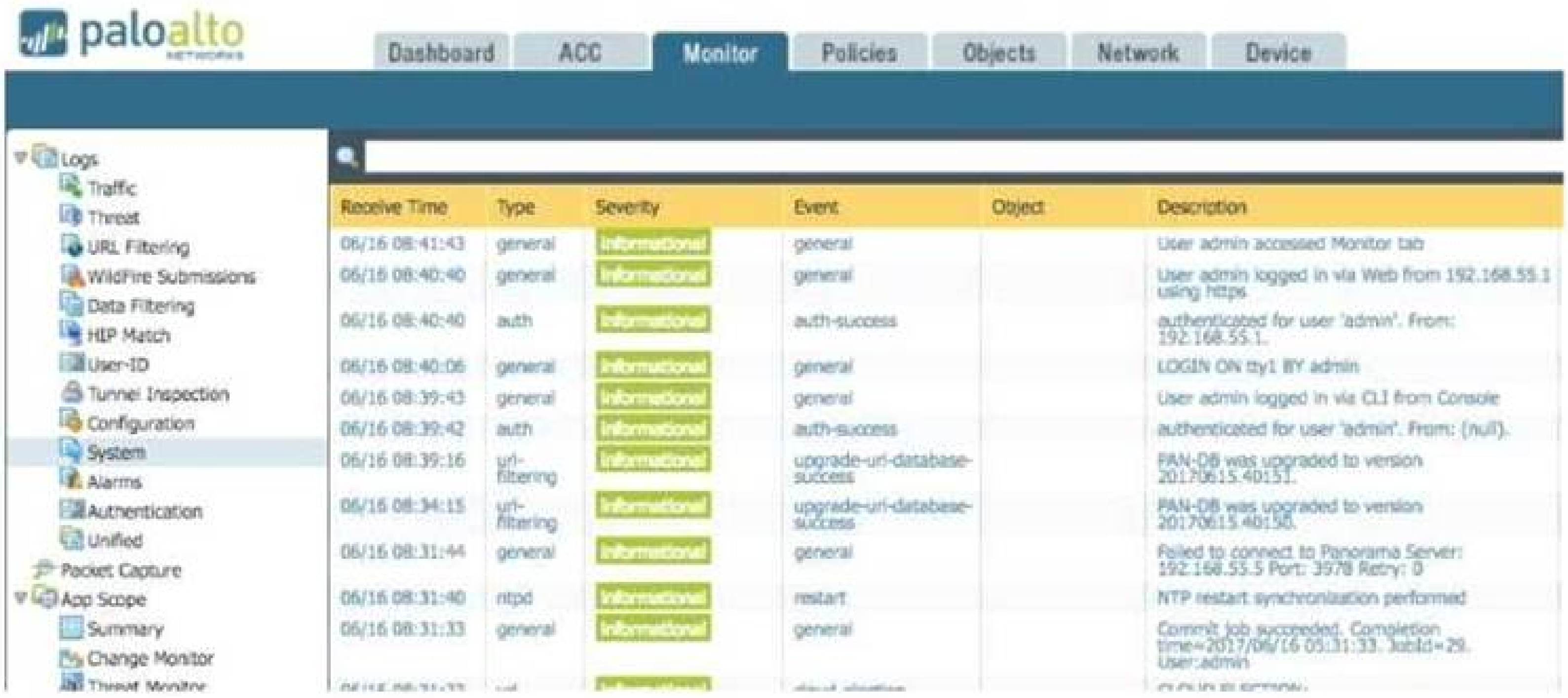
NEW QUESTION 5
Which version of GlobalProtect supports split tunneling based on destination domain, client process, and HTTP/HTTPS video streaming application?

A. GlobalProtect version 4.0 with PAN-OS 8.1
B. GlobalProtect version 4.1 with PAN-OS 8.1
C. GlobalProtect version 4.1 with PAN-OS 8.0
D. GlobalProtect version 4.0 with PAN-OS 8.0

Answer: B

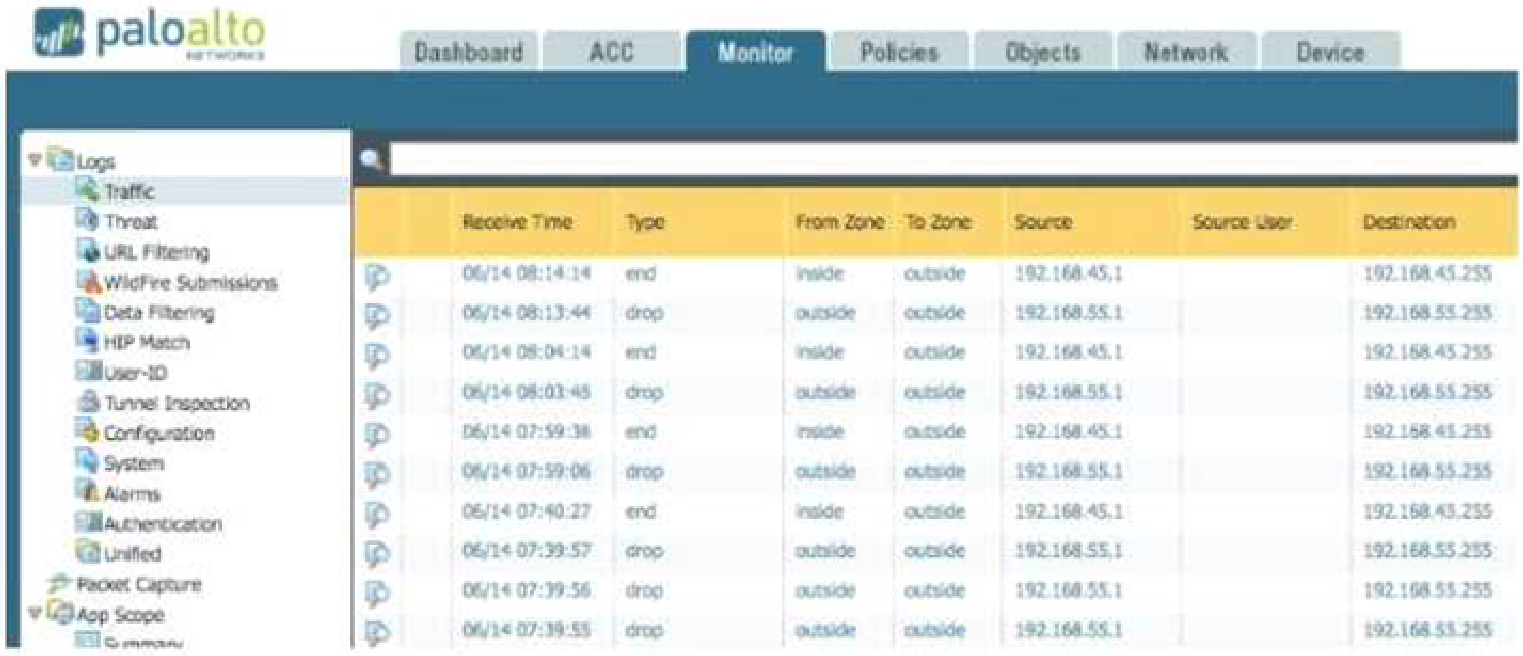
NEW QUESTION 6
An administrator accidentally closed the commit window/screen before the commit was finished. Which two options could the administrator use to verify the progress or success of that commit task? (Choose two.)

A



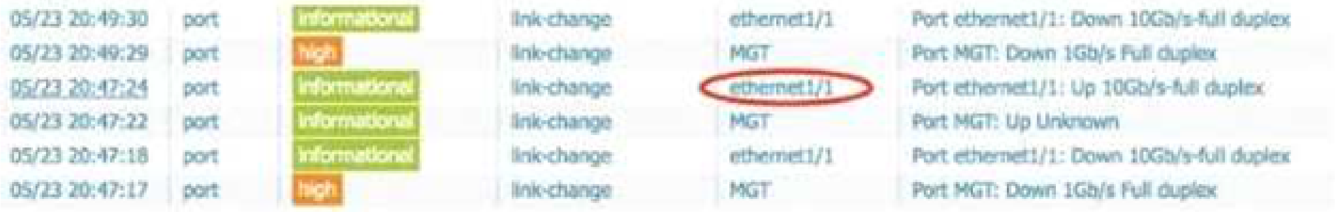
Receive Time	Type	Severity	Event	Object	Description
06/16 08:41:43	general	informational	general		User admin accessed Monitor tab
06/16 08:40:40	general	informational	general		User admin logged in via Web from 192.168.55.1 using https
06/16 08:40:40	auth	informational	auth-success		authenticated for user 'admin'. From: 192.168.55.1.
06/16 08:40:06	general	informational	general		LOGIN ON tty1 BY admin
06/16 08:39:43	general	informational	general		User admin logged in via CLI from Console
06/16 08:39:42	auth	informational	auth-success		authenticated for user 'admin'. From: (null).
06/16 08:39:16	url-filtering	informational	upgrade-url-database-success		PAN-DB was upgraded to version 20170615.40151.
06/16 08:34:15	url-filtering	informational	upgrade-url-database-success		PAN-DB was upgraded to version 20170615.40150.
06/16 08:31:44	general	informational	general		Failed to connect to Panorama Server: 192.168.55.5 Port: 3978 Retry: 0
06/16 08:31:40	ntpd	informational	restart		NTP restart synchronization performed
06/16 08:31:33	general	informational	general		Commit job succeeded. Completion time=2017/06/16 05:31:33. JobId=29. User:admin

B



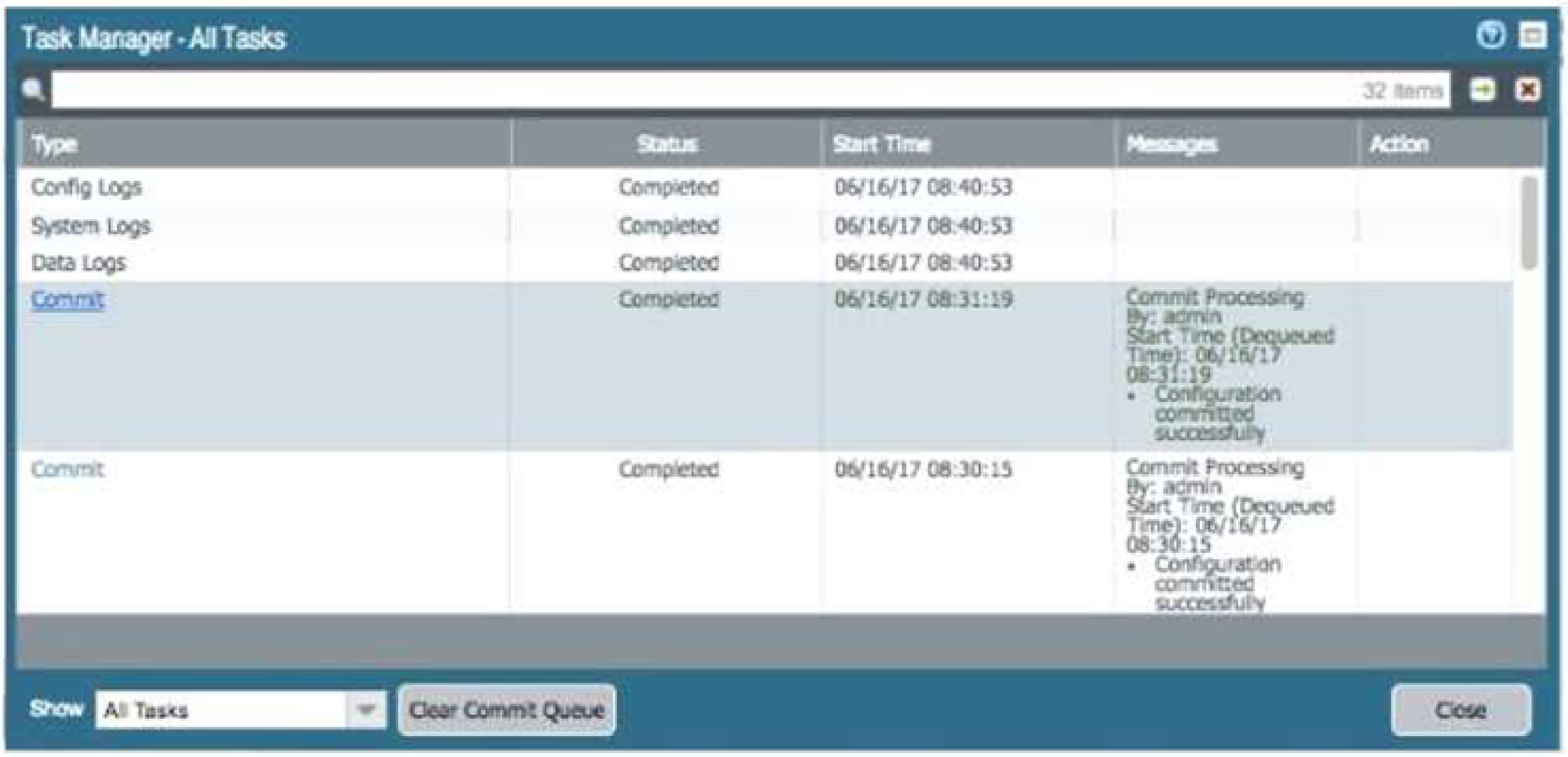
Receive Time	Type	From Zone	To Zone	Source	Source User	Destination
06/14 08:14:14	end	inside	outside	192.168.45.1		192.168.45.255
06/14 08:13:44	drop	outside	outside	192.168.55.1		192.168.55.255
06/14 08:04:14	end	inside	outside	192.168.45.1		192.168.45.255
06/14 08:03:45	drop	outside	outside	192.168.55.1		192.168.55.255
06/14 07:59:36	end	inside	outside	192.168.45.1		192.168.45.255
06/14 07:59:06	drop	outside	outside	192.168.55.1		192.168.55.255
06/14 07:40:27	end	inside	outside	192.168.45.1		192.168.45.255
06/14 07:39:57	drop	outside	outside	192.168.55.1		192.168.55.255
06/14 07:39:56	drop	outside	outside	192.168.55.1		192.168.55.255
06/14 07:39:55	drop	outside	outside	192.168.55.1		192.168.55.255

C



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

D



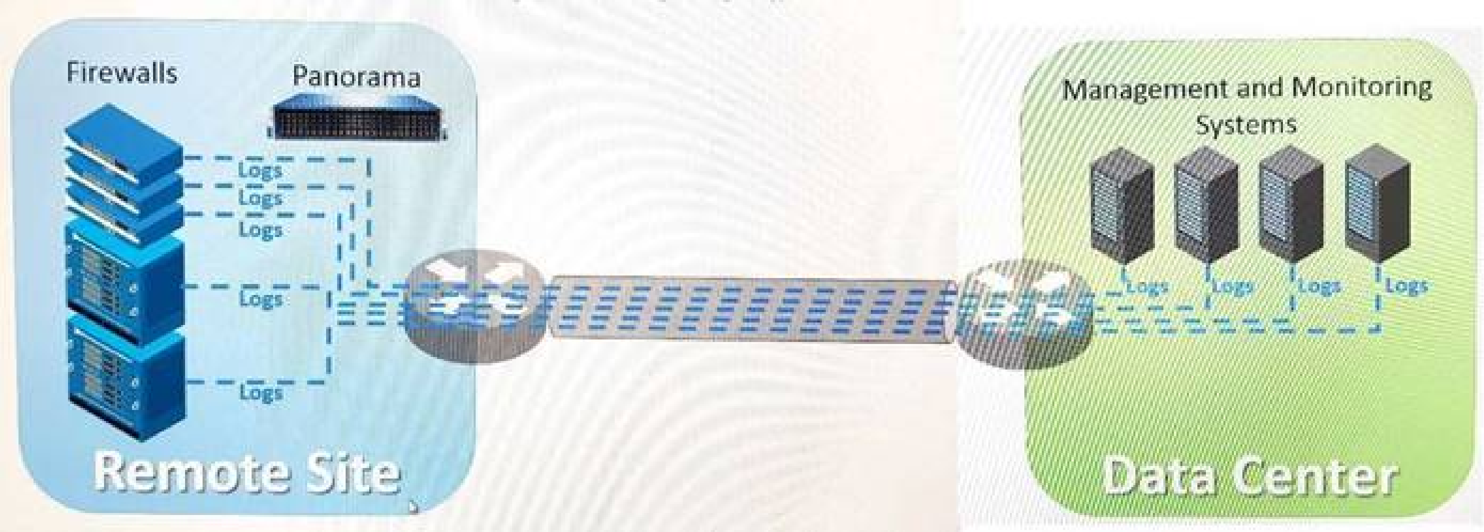
Task Manager - All Tasks

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

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

Answer: AD

NEW QUESTION 7
Refer to exhibit.



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

A. Forward logs from firewalls only to Panorama and have Panorama forward logs to other external services.
B. Forward logs from external sources to Panorama for correlation, and from Panorama send them to the NGFW.
C. Configure log compression and optimization features on all remote firewalls.
D. Any configuration on an M-500 would address the insufficient bandwidth concerns.

Answer: A

NEW QUESTION 8
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

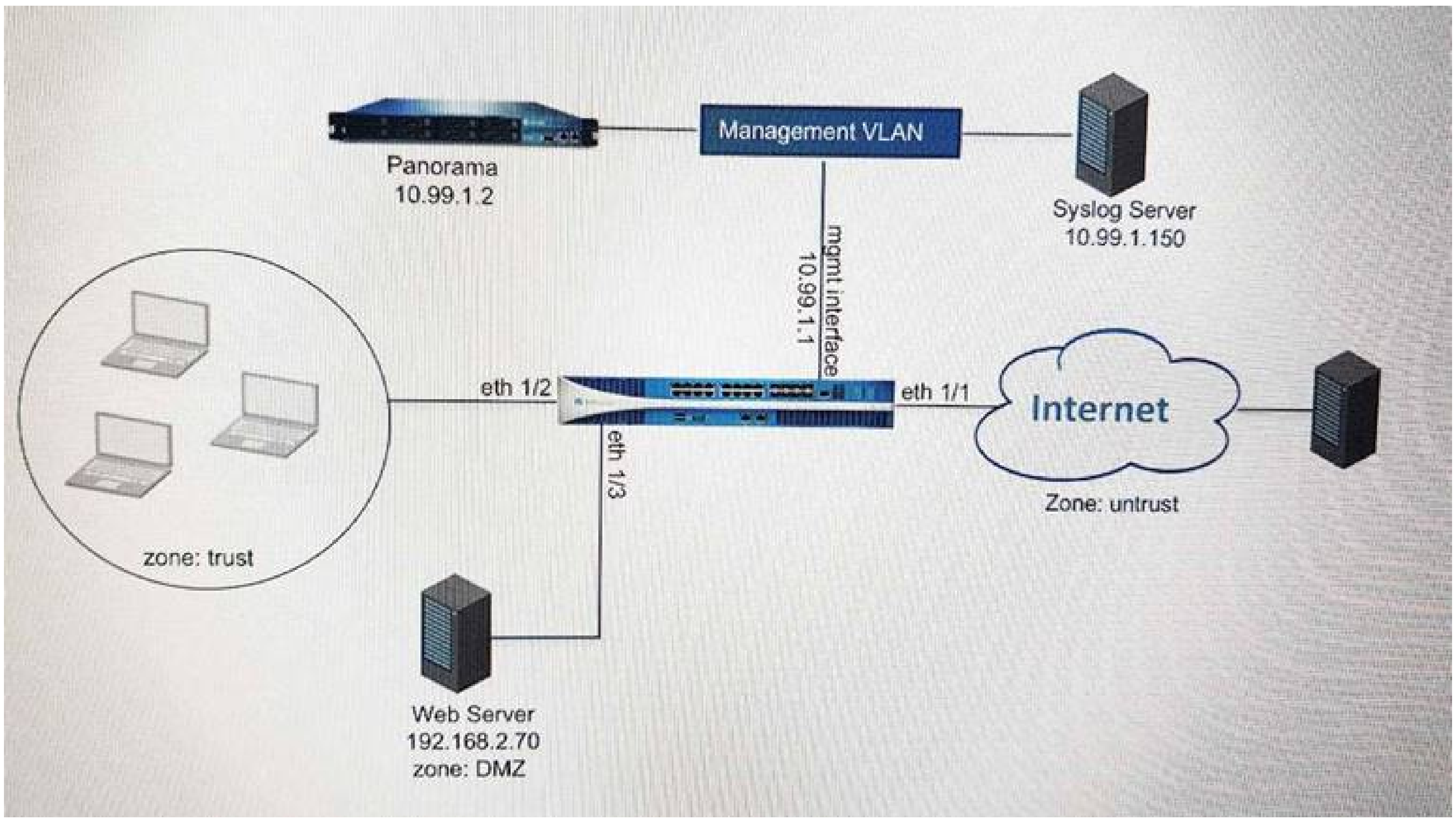
Answer: A

NEW QUESTION 9
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

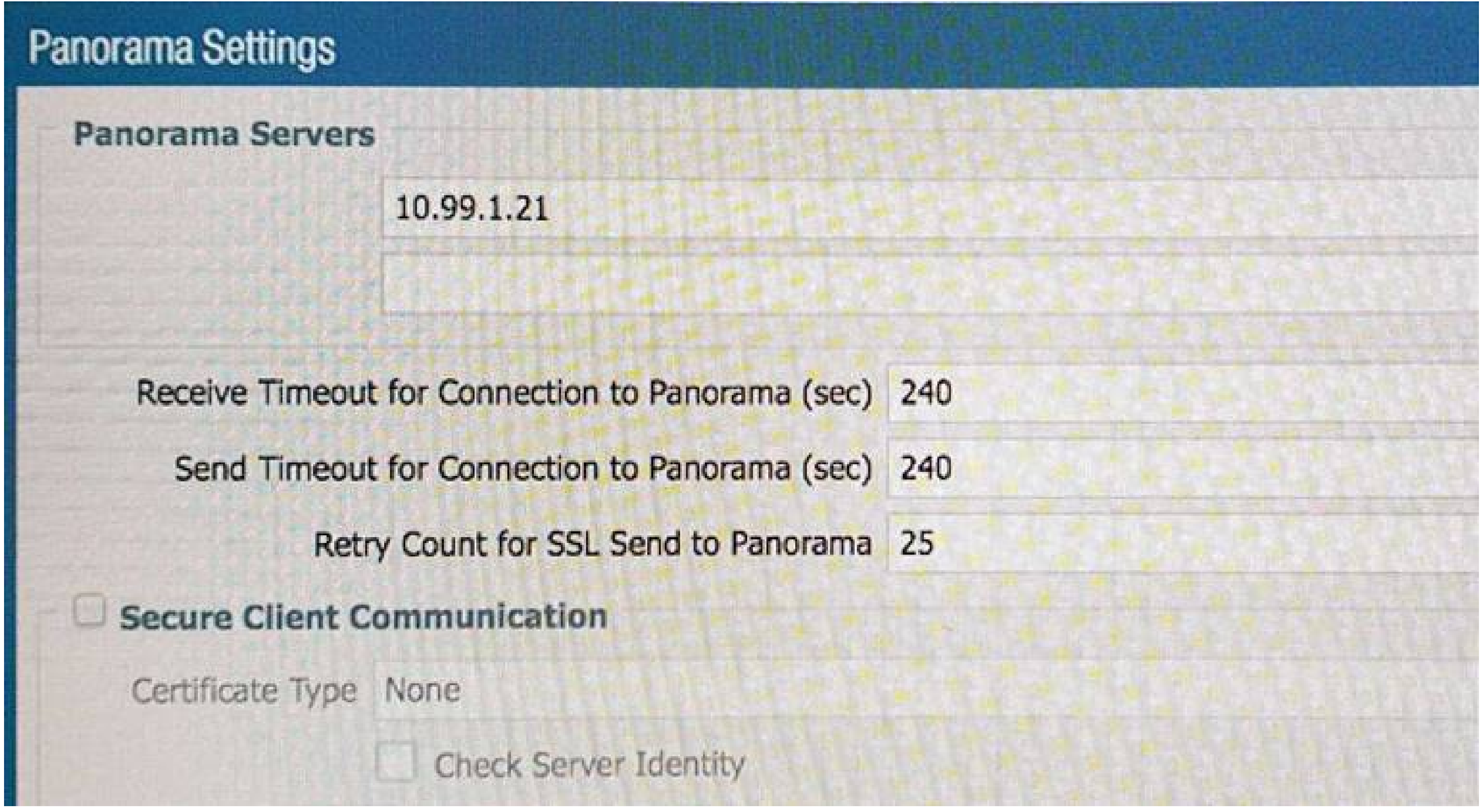
Answer: C

NEW QUESTION 10
Refer to the exhibit.



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

A)



Panorama Settings

Panorama Servers

10.99.1.21

Receive Timeout for Connection to Panorama (sec) 240

Send Timeout for Connection to Panorama (sec) 240

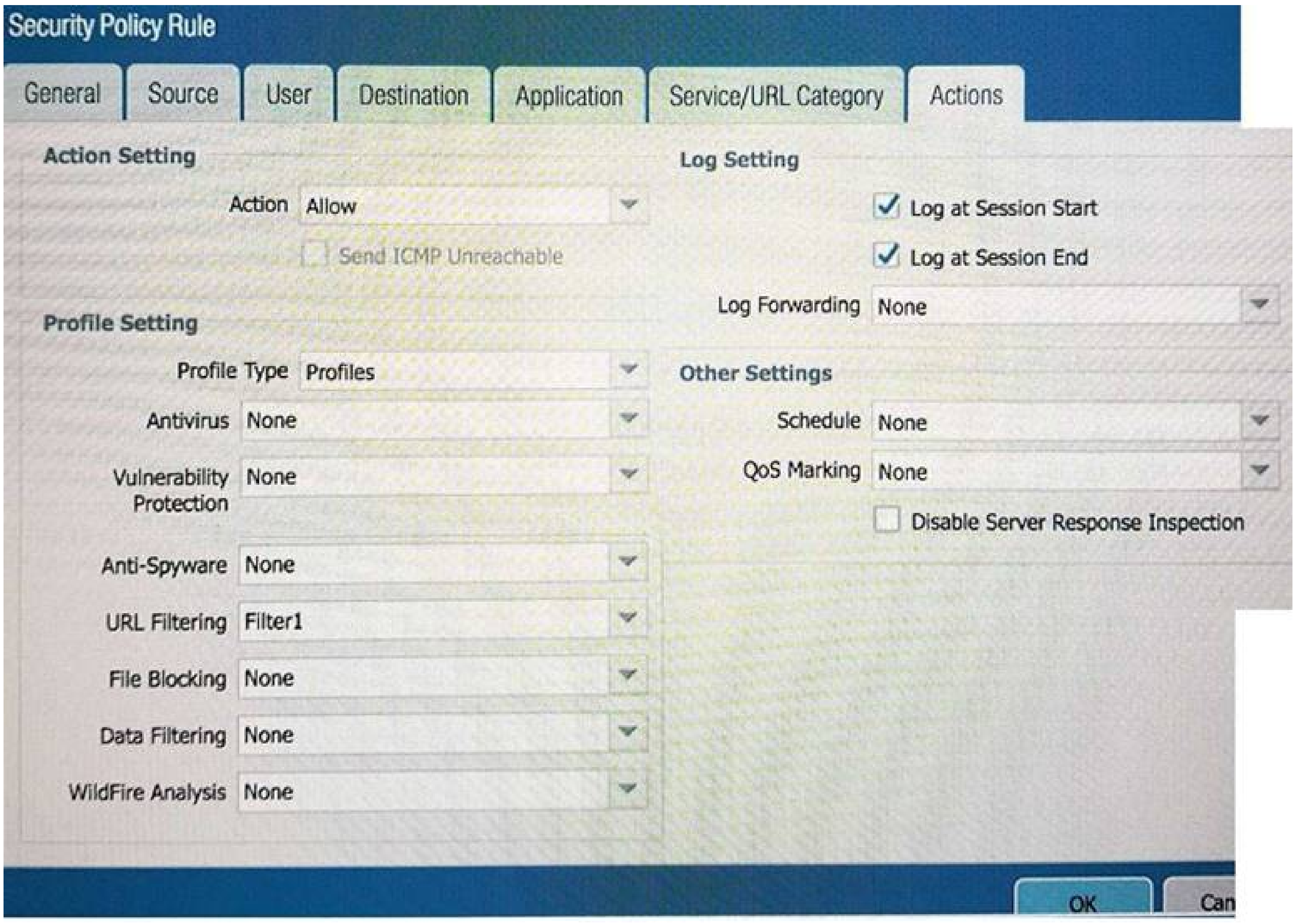
Retry Count for SSL Send to Panorama 25

□ Secure Client Communication

Certificate Type None

□ Check Server Identity

B)



Security Policy Rule

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

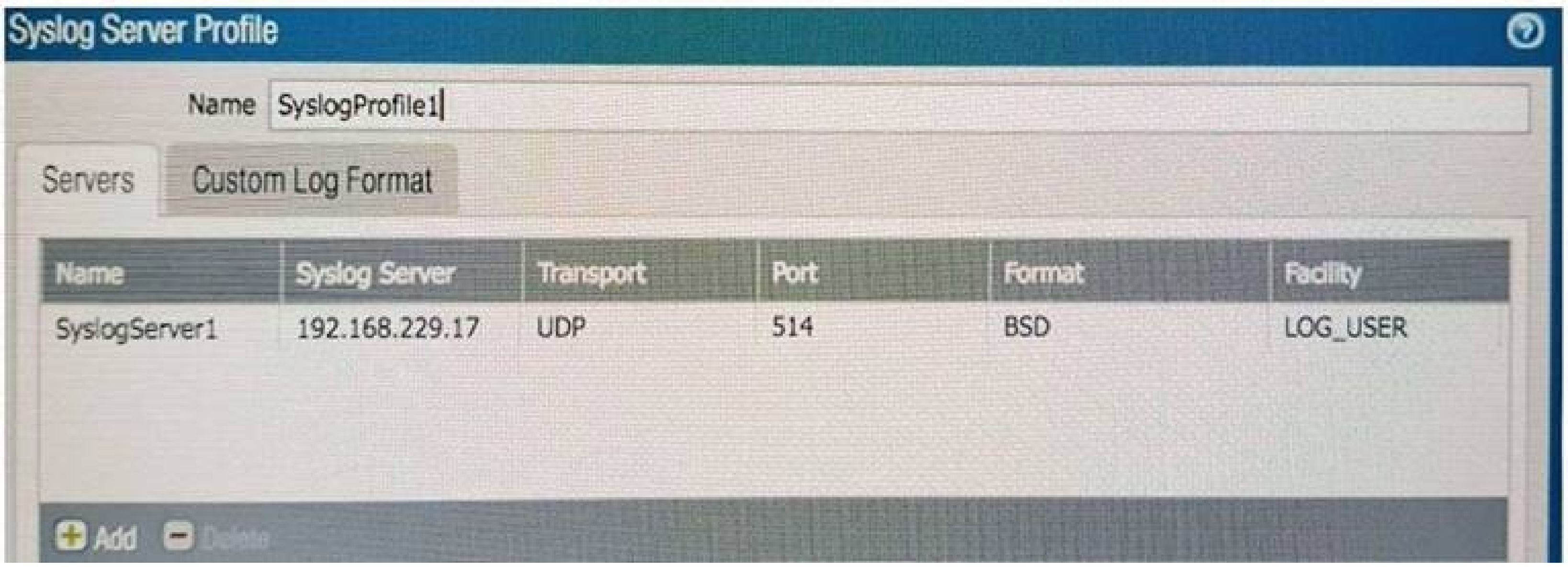
Other Settings

Schedule: None

QoS Marking: None

□ Disable Server Response Inspection

C)

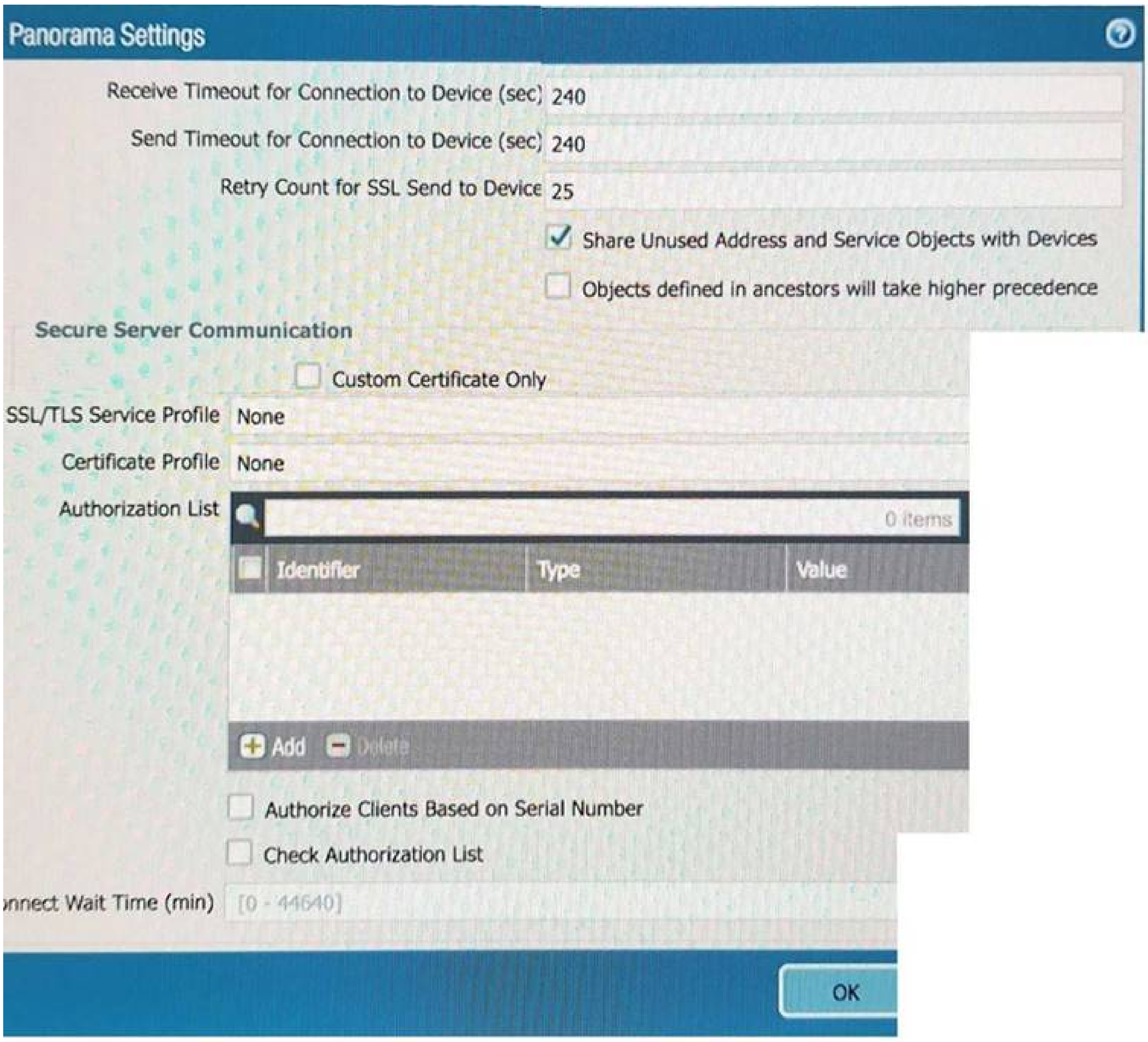


Syslog Server Profile

Name: SyslogProfile1

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

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 0 items

□ Identifier	Type	Value

□ Authorize Clients Based on Serial Number

□ Check Authorization List

nnect Wait Time (min) [0 - 44640]

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 13
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 14

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 19
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 invali
B. The Profile Settings section will be grayed out when the Action is set to "Deny".
C. The configuration will allow the matched session unless a vulnerability signature is detecte
D. The "Deny" action will supersede theper-severity defined actions defined in the associated Vulnerability Protection Profile.
E. The configuration is invali
F. It will cause the firewall to skip this Security policy rul
G. A warning will be displayed during a commit.
H. The configuration is vali
I. It will cause the firewall to deny the matched session
J. Any configured Security Profiles have no effect ifthe Security policy rule action is set to "Deny."

Answer: B

NEW QUESTION 20
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 22
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 form the Shared group
D. Overwrites local firewall configuration

Answer: BC

NEW QUESTION 27
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 EIGRPprotocols)
D. Layer 3 interfaces, but configuring EIGRP on the attached virtual router

Answer: C

NEW QUESTION 31
Which method does an administrator use to integrate all non-native MFA platforms in PAN-OS® software?

A. Okta
B. DUO
C. RADIUS
D. PingID

Answer: C

NEW QUESTION 34
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 39
An administrator logs in to the Palo Alto Networks NGFW and reports that the WebUI is missing the Policies tab. Which profile is the cause of the missing Policies tab?

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

Answer: A

NEW QUESTION 42
An administrator is using Panorama and multiple Palo Alto Networks NGFWs. After upgrading all
devices to the latest PAN-OS® software, the administrator enables log forwarding from the firewalls to Panorama. Pre-existing logs from the firewalls are not appearing in PanoramA.
Which action would enable the firewalls to send their pre-existing logs to Panorama?

A. Use the import option to pull logs into Panorama.
B. A CLI command will forward the pre-existing logs to Panorama.
C. Use the ACC to consolidate pre-existing logs.
D. The log database will need to exported form the firewalls and manually imported into Panorama.

Answer: B

NEW QUESTION 44
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

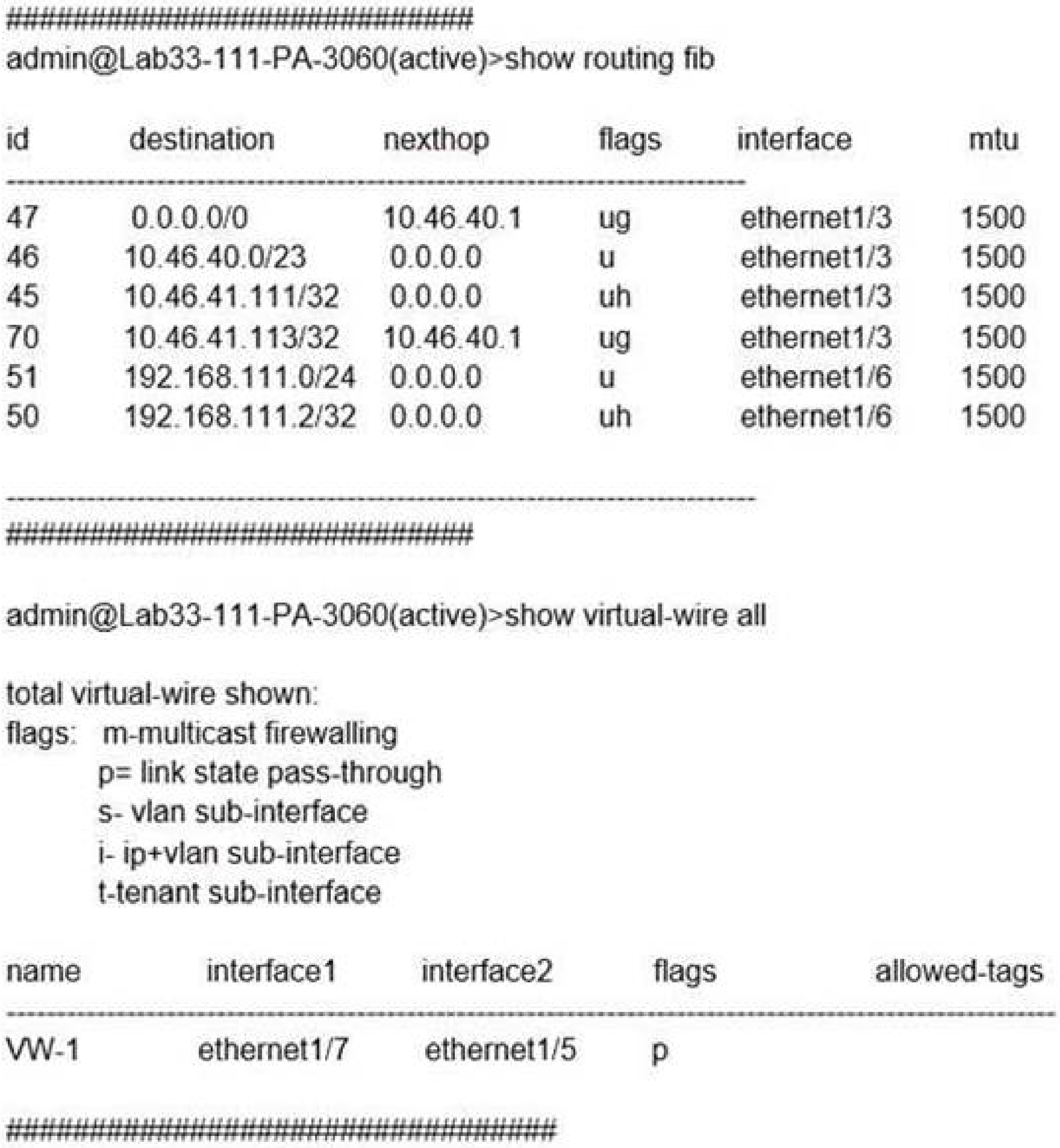
NEW QUESTION 46
Which Palo Alto Networks VM-Series firewall is valid?

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
Refer to the exhibit.



```
################################
admin@Lab33-111-PA-3060(active)>show routing fib

id      destination       nexthop      flags     interface      mtu
--------------------------------------------------------------------
47       0.0.0.0/0        10.46.40.1   ug        ethernet1/3    1500
46      10.46.40.0/23      0.0.0.0     u         ethernet1/3    1500
45      10.46.41.111/32    0.0.0.0     uh        ethernet1/3    1500
70      10.46.41.113/32   10.46.40.1   ug        ethernet1/3    1500
51      192.168.111.0/24   0.0.0.0     u         ethernet1/6    1500
50      192.168.111.2/32   0.0.0.0     uh        ethernet1/6    1500

--------------------------------------------------------------------
################################

admin@Lab33-111-PA-3060(active)>show virtual-wire all

total virtual-wire shown:
flags:   m-multicast firewalling
         p= link state pass-through
         s- vlan sub-interface
         i- ip+vlan sub-interface
         t-tenant sub-interface

name          interface1      interface2      flags         allowed-tags
--------------------------------------------------------------------------------
VW-1          ethernet1/7     ethernet1/5     p

######################################
```

Which will be the egress interface if the traffic's ingress interface is ethernet 1/7 sourcing from 192.168.111.3 and to the destination 10.46.41.113?

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

Answer: D

NEW QUESTION 54
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 57
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-amp-Tricks-How-to-Create-an-Application-Override/ta-p/65513

NEW QUESTION 59
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 60
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

Answer: D

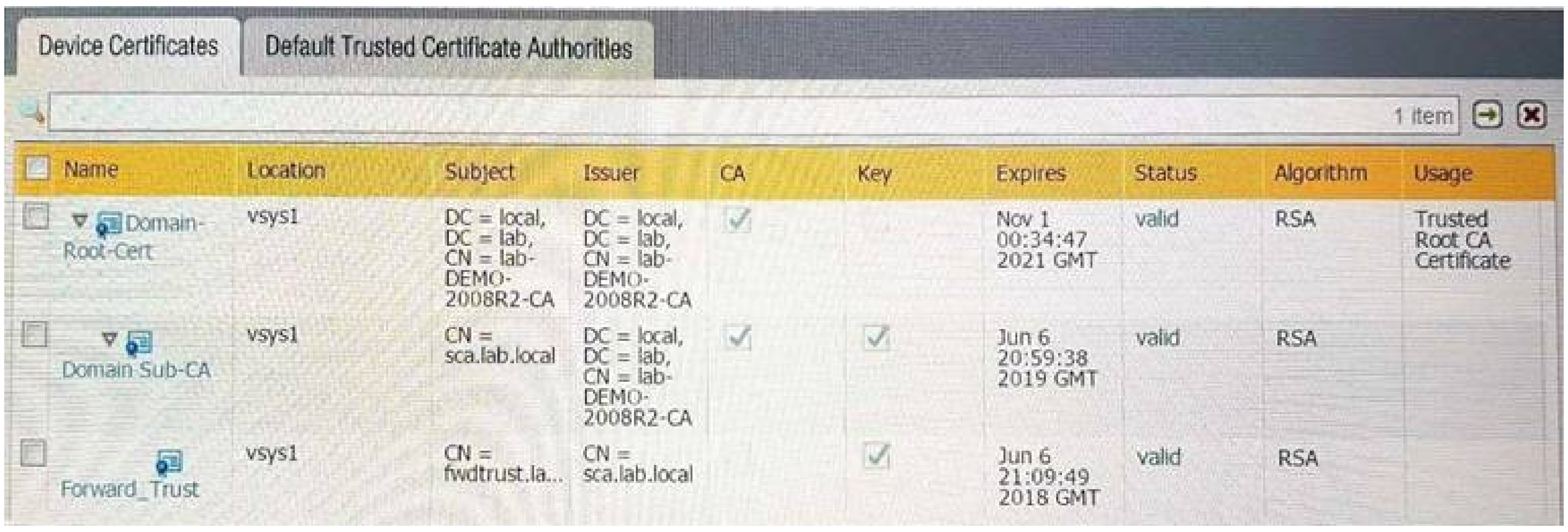
Explanation:
Reference: https://www.paloaltonetworks.com/cyberpedia/how-the-next-generation-security-platform-contributes-to-gdpr-compliance

NEW QUESTION 63
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 67
Refer to the exhibit.



□ 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	✓		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	✓	✓	Jun 6 20:59:38 2019 GMT	valid	RSA	
□ Forward_Trust	vsys1	CN = fwdtrust.la...	CN = sca.lab.local		✓	Jun 6 21:09:49 2018 GMT	valid	RSA	

Which certificates can be used as a Forwarded Trust certificate?

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

Answer: A

NEW QUESTION 70
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 73
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 76
An administrator has a requirement to export decrypted traffic from the Palo Alto Networks NGFW to a third-party, deep-level packet inspection appliance.
Which interface type and license feature are necessary to meet the requirement?

A. Decryption Mirror interface with the Threat Analysis license
B. Virtual Wire interface with the Decryption Port Export license
C. Tap interface with the Decryption Port Mirror license
D. Decryption Mirror interface with the associated Decryption Port Mirror license

Answer: D

Explanation:
Reference: https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/decryption/decryption-mirroring

NEW QUESTION 80
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

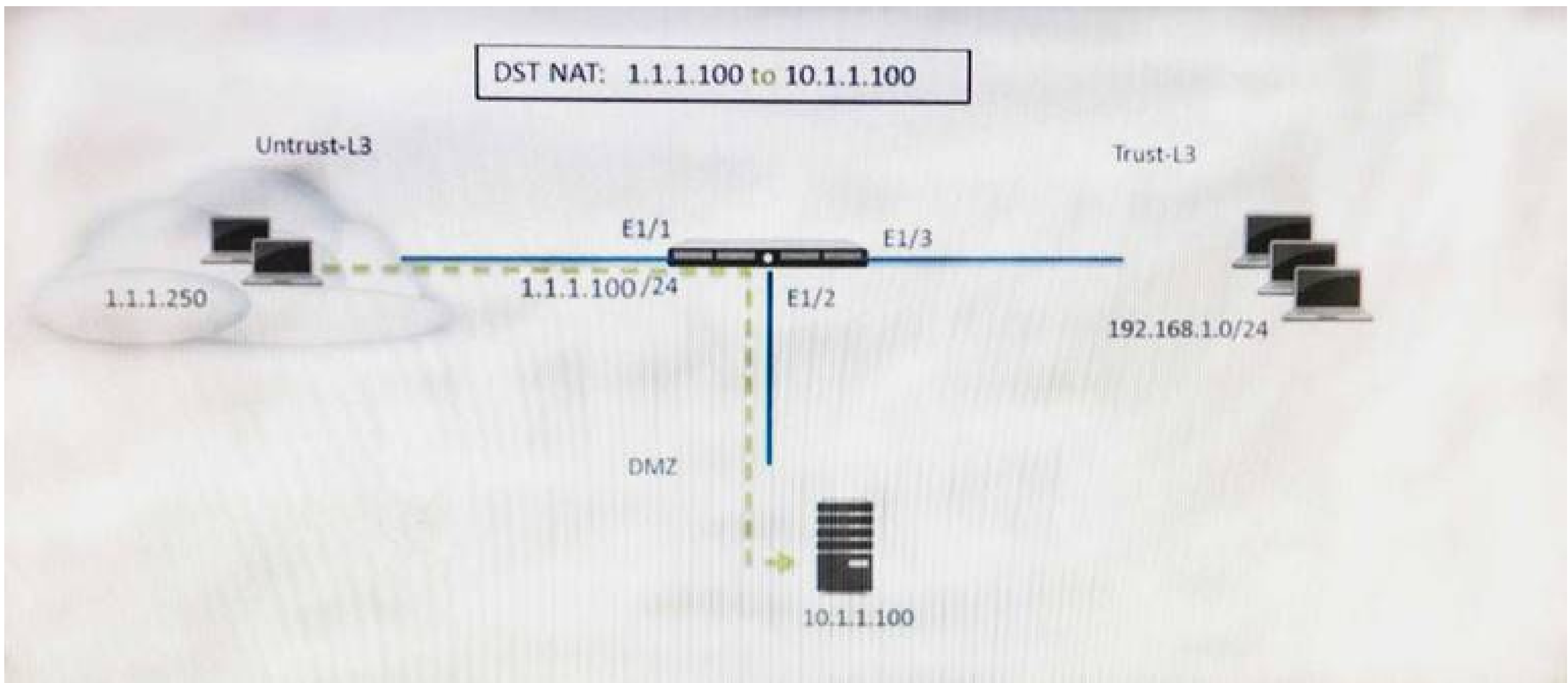
NEW QUESTION 84
Which processing order will be enabled when a Panorama administrator selects the setting “Objects defined in ancestors will take higher precedence?”

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 86
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 91
A web server is hosted in the DMZ and the server is configured to listen for incoming connections on TCP port 443. A Security policies rules allowing access from the Trust zone to the DMZ zone needs to be configured to allow web-browsing access. The web server hosts its contents over HTTP(S). Traffic from Trust to DMZ

is being decrypted with a Forward Proxy rule.
Which combination of service and application, and order of Security policy rules, needs to be configured to allow cleartext web- browsing traffic to this server on tcp/443.

A. Rule #1: application: web-browsing; service: application-default; action: allow Rule #2: application: ssl; service: application-default; action: allow
B. Rule #1: application: web-browsing; service: service-https; action: allow Rule #2: application: ssl; service: application-default; action: allow
C. Rule # 1: application: ssl; service: application-default; action: allowRule #2: application: web-browsing; service: application-default; action: allow
D. Rule #1: application: web-browsing; service: service-http; action: allow Rule #2: application: ssl; service: application-default; action: allow

Answer: A

NEW QUESTION 92
Which feature can be configured on VM-Series firewalls?

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

Answer: D

NEW QUESTION 97
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 98
The firewall identifies a popular application as an unknown-tcp.
Which two options are available to identify the application? (Choose two.)

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

Answer: AB

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

NEW QUESTION 102
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 106
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 107

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
An administrator deploys PA-500 NGFWs as an active/passive high availability pair. The devices are not participating in dynamic routing and preemption is disabled.
What must be verified to upgrade the firewalls to the most recent version of PAN-OS software?

A. Mastered
B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 112
A customer wants to set up a site-to-site VPN using tunnel interfaces? Which two formats are correct for naming tunnel interfaces? (Choose two.)

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

Answer: CD

NEW QUESTION 117
The firewall determines if a packet is the first packet of a new session or if a packet is part of an existing session using which kind of match?

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

Answer: A

NEW QUESTION 119
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 121
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 124
Which log file can be used to identify SSL decryption failures?

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

Answer:

C

NEW QUESTION 126
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 e1/1.
•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. DNS settings for the firewall to use for resolution
B. scheduler for timed downloads of PAN-OS software
C. static route pointing application PaloAlto-updates to the update servers
D. Security policy rule allowing PaloAlto-updates as the application

Answer: D

NEW QUESTION 128
Which three firewall states are valid? (Choose three)

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

Answer: ABC

NEW QUESTION 132
Which is the maximum number of samples that can be submitted to WildFire per day, based on wildfire subscription?

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

Answer: B

NEW QUESTION 133
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 135
Where can an administrator see both the management plane and data plane CPU utilization in the WebUI?

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

Answer: C

NEW QUESTION 137
Which option enables a Palo Alto Networks NGFW administrator to schedule Application and Threat updates while applying only new content-IDs to traffic?

A. Select download-and-install.
B. Select download-and-install, with "Disable new apps in content update" selected.
C. Select download-only.
D. Select disable application updates and select "Install only Threat updates"

Answer: C

NEW QUESTION 139
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 141
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 142
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 146
A logging infrastructure may need to handle more than 10,000 logs per second. Which two options support a dedicated log collector function? (Choose two)

A. Panorama virtual appliance on ESX(i) only
B. M-500
C. M-100 with Panorama installed
D. M-100

Answer: BC

Explanation:
(httpHYPERLINK "https://live.paloaltonetworks.com/t5/Management-Articles/Panorama-Sizing-and- Design-Guide/ta-p/72181"s://live.paloaltonetworks.com/t5/Management-Articles/Panorama-Sizing- and-Design-Guide/ta-p/72181)

NEW QUESTION 148
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 152
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 153
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 accesss https://www.youtube.com in a web browser, they get an error indecating 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 155
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 159
A Palo Alto Networks firewall is being targeted by an NTP Amplification attack and is being flooded with tens thousands of bogus UDP connections per second to a single destination IP address and post.
Which option when enabled with the correction threshold would mitigate this attack without dropping legitirnate traffic to other hosts insides the network?

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

Answer: D

NEW QUESTION 162
A network security engineer is asked to perform a Return Merchandise Authorization (RMA) on a firewall
Which part of files needs to be imported back into the replacement firewall that is using Panorama?

A. Device state and license files
B. Configuration and serial number files
C. Configuration and statistics files
D. Configuration and Large Scale VPN (LSVPN) setups file

Answer: A

NEW QUESTION 163
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 referanced 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 167
A network security engineer has been asked to analyze Wildfire activity. However, the Wildfire Submissions item is not visible form the Monitor tab.
What could cause this condition?

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

Answer: B

NEW QUESTION 170
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 173
A host attached to ethernet1/3 cannot access the internet. The default gateway is attached to ethernet1/4. After troubleshooting. It is determined that traffic cannot pass from the ethernet1/3 to ethernet1/4. What can be the cause of the problem?

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

Answer: B

NEW QUESTION 175
Which two interface types can be used when configuring GlobalProtect Portal?(Choose two)

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

Answer: BC

NEW QUESTION 180
Which three options does the WF-500 appliance support for local analysis? (Choose three)

A. E-mail links
B. APK files
C. jar files
D. PNG files
E. Portable Executable (PE) files

Answer: ACE

NEW QUESTION 182
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 187
A Network Administrator wants to deploy a Large Scale VPN solution. The Network Administrator has chosen a GlobalProtect Satellite solution. This configuration needs to be deployed to multiple remote offices and the Network Administrator decides to use Panorama to deploy the configurations.
How should this be accomplished?

A. Create a Template with the appropriate IKE Gateway settings
B. Create a Template with the appropriate IPSec tunnel settings
C. Create a Device Group with the appropriate IKE Gateway settings
D. Create a Device Group with the appropriate IPSec tunnel settings

Answer: B

NEW QUESTION 191
Firewall administrators cannot authenticate to a firewall GUI.
Which two logs on that firewall will contain authentication-related information useful in troubleshooting this issue? (Choose two.)

A. ms log
B. authd log
C. System log
D. Traffic log
E. dp-monitor .log

Answer: BC

NEW QUESTION 194
Which authentication source requires the installation of Palo Alto Networks software, other than PAN-OS 7x, to obtain a username-to-IP-address mapping?

A. Microsoft Active Directory
B. Microsoft Terminal Services
C. Aerohive Wireless Access Point
D. Palo Alto Networks Captive Portal

Answer: B

NEW QUESTION 198
Which Panorama feature allows for logs generated by Panorama to be forwarded to an external Security Information and Event Management(SIEM) system?

A. Panorama Log Settings
B. Panorama Log Templates
C. Panorama Device Group Log Forwarding

D. Collector Log Forwarding for Collector Groups

Answer: A

Explanation:
https://www.paloaltonetworks.com/documentation/61/panorama/panorama_admiHYPERLINK "https://www.paloaltonetworks.com/documentation/61/panorama/panorama_adminguide/manag e-log-collection/enable-log-forwarding-from-panorama-to-external-destinations"nguidHYPERLINK "https://www.paloaltonetworks.com/documentation/61/panorama/panorama_adminguide/manag e-log-collection/enable-log-forwarding-from-panorama-to-external-destinations"e/manage-log- collection/enable-log-forwarding-from-panorama-to-external-destinaHYPERLINK "https://www.paloaltonetworks.com/documentation/61/panorama/panorama_adminguide/manag e-log-collection/enable-log-forwarding-from-panorama-to-external-destinations"tions

NEW QUESTION 200
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.comHYPERLINK "https://live.paloaltonetworks.com/t5/Management- Articles/Show-System-Resource-Command-Displays-CPU-Utilization-of-9999/ta-p/58149"/t5/Management-Articles/Show-System-Resource-Command-Displays-CPU-Utilization-of- 9999/ta-p/58149

NEW QUESTION 203
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.paloaltonetwoHYPERLINK "https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/panorama- web-interface/defining-policies-on-panorama"rks.com/documentation/71/pan-os/web-interHYPERLINK "https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface- help/panorama-web-interface/defining-policies-on-panorama"face-help/panorama-web- interface/defining-policies-on-panorama

NEW QUESTION 204
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 207
A network security engineer needs to configure a virtual router using IPv6 addresses. Which two routing options support these addresses? (Choose two)

A. BGP not sure
B. OSPFv3
C. RIP
D. Static Route

Answer: BD

Explanation:
https://live.paloaltonetworks.com/t5/Management-Articles/Does-PAN-OS-Support-Dynamic-Routing-Protocols-OSPF-or-BGP-with/ta-p/62773

NEW QUESTION 211
When a malware-infected host attempts to resolve a known command-and-control server, the traffic matches a security policy with DNS sinhole enabled, generating a traffic log.
What will be the destination IP Address in that log entry?

A. The IP Address of sinkhole.paloaltonetworks.com
B. The IP Address of the command-and-control server
C. The IP Address specified in the sinkhole configuration
D. The IP Address of one of the external DNS servers identified in the anti-spyware database

Answer: C

Explanation:
https://live.paloaltonetworks.com/t5/MaHYPERLINK "https://live.paloaltonetworks.com/t5/Management-Articles/How-to-Verify-DNS-Sinkhole-Function- is-Working/ta-p/65864"naHYPERLINK "https://live.paloaltonetworks.com/t5/Management- Articles/How-to-Verify-DNS-Sinkhole-Function-is-Working/ta-p/65864"gement-Articles/How-to- Verify-DNS-Sinkhole-Function-is-Working/ta-p/65864

NEW QUESTION 214
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 219
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 221
How can a Palo Alto Networks firewall be configured to send syslog messages in a format compatible with non-standard syslog servers?

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

Answer: D

NEW QUESTION 223
Refer to Exhibit:

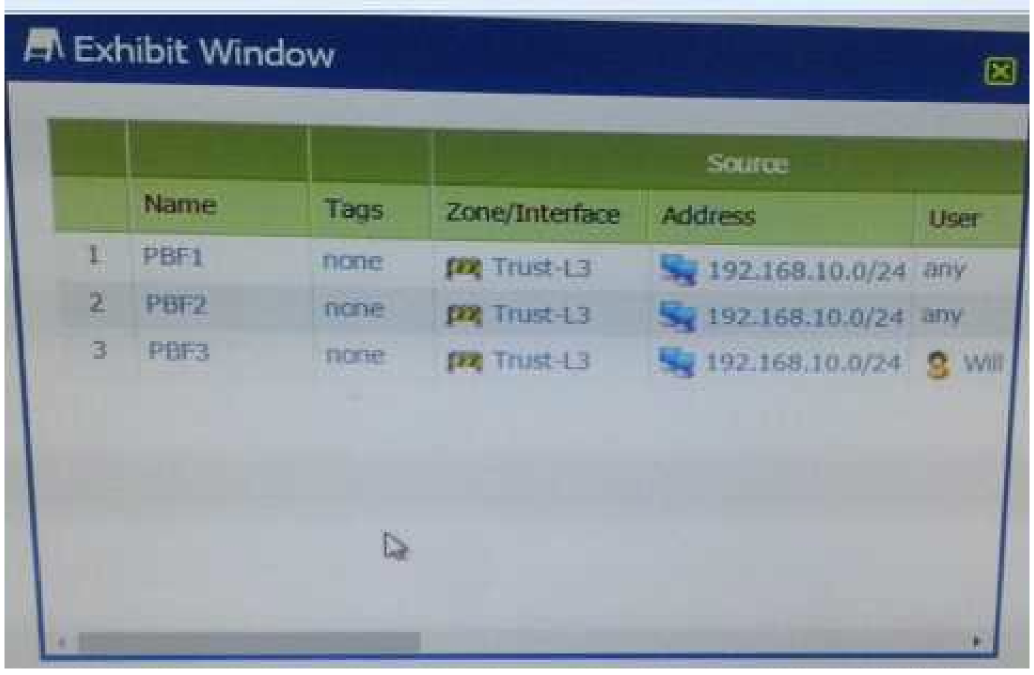


Exhibit Window

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

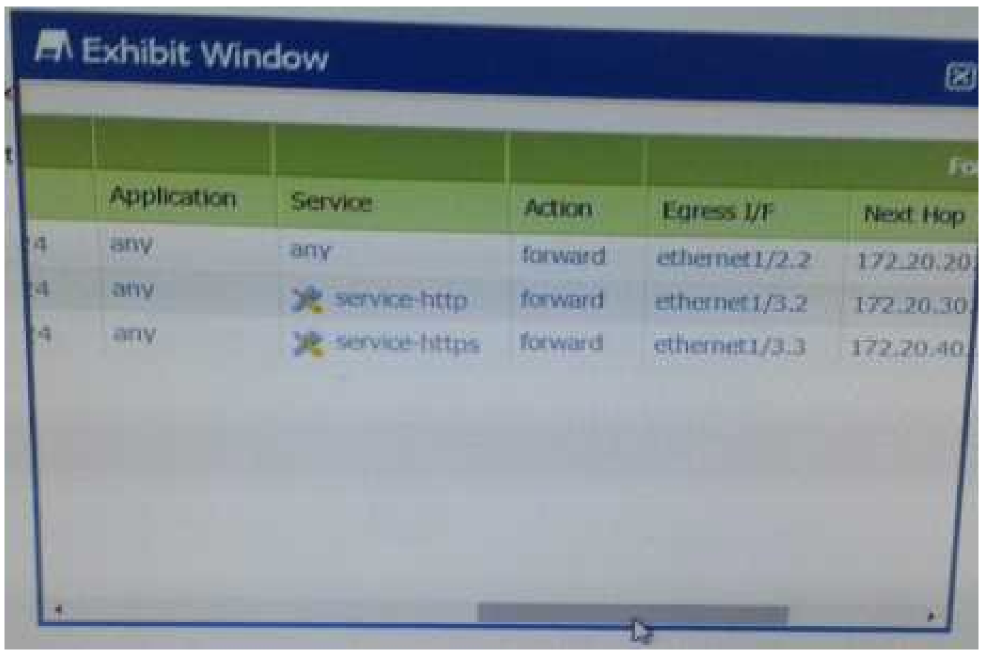


Exhibit Window

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

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

He makes an HTTPS connection to 172.16.10.29.
What is the next hop IP address for the HTTPS traffic from Wills PC.

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

Answer: B

NEW QUESTION 225
Which Device Group option is assigned by default in Panorama whenever a new device group is created to manage a Firewall?

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

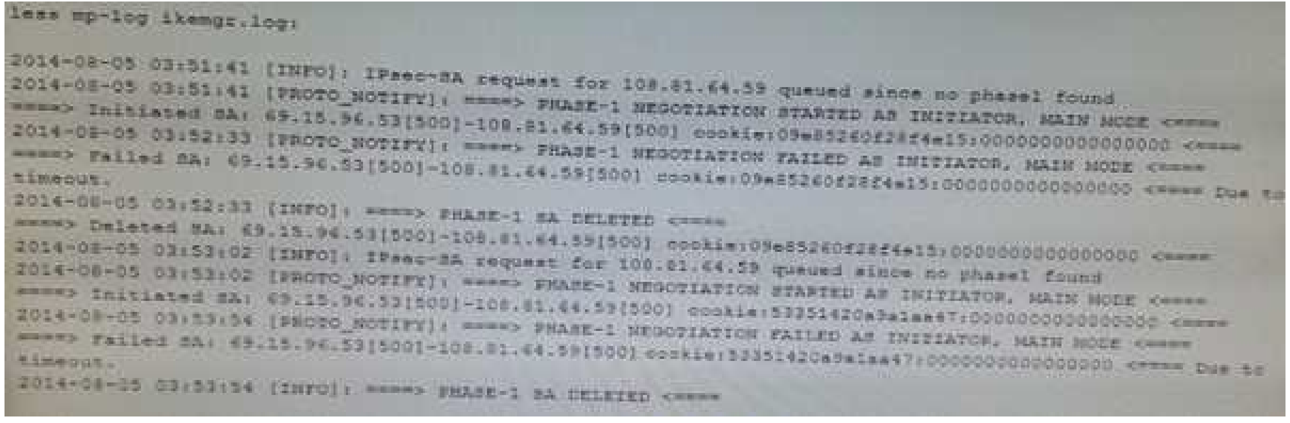
Answer: C

NEW QUESTION 226
A distributed log collection deployment has dedicated log Collectors. A developer needs a device to send logs to Panorama instead of sending logs to the Collector Group.
What should be done first?

A. Remove the cable from the management interface, reload the log Collector and then re-connect that cable
B. Contact Palo Alto Networks Support team to enter kernel mode commands to allow adjustments
C. remove the device from the Collector Group
D. Revert to a previous configuration

Answer: C

NEW QUESTION 227
An administrator is configuring an IPSec VPN to a Cisco ASA at the administrator's home and experiencing issues completing the connection. the following is the output from the command:



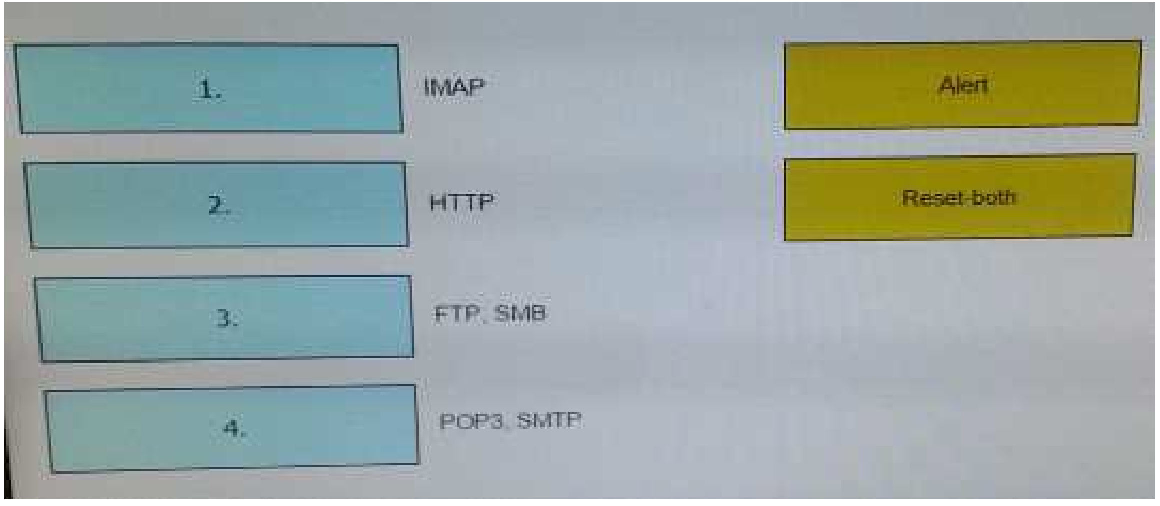
```
less mp-log ikemgr.log:

2014-08-05 03:51:41 [INFO]: IPsec-SA request for 108.81.64.59 queued since no phase1 found
2014-08-05 03:51:41 [PROTO_NOTIFY]: ====> PHASE-1 NEGOTIATION STARTED AS INITIATOR, MAIN MODE <====
====> Initiated SA: 69.15.96.53[500]-108.81.64.59[500] cookie: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 dead peer detection settings do not match between the Palo Alto Networks Firewall and the ASA.
B. The Proxy IDs on the Palo Alto Networks Firewall do not match the setting on the ASA.
C. The public IP addresses do not match for both the Palo Alto Networks Firewall and the ASA.
D. The shared secrets do not match between the Palo Alto Networks Firewall and the ASA.

Answer: C

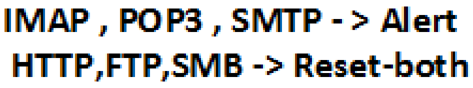
NEW QUESTION 232
DRAG DROP
When using the predefined default profile, the policy will inspect for viruses on the decoders. Match each decoder with its default action.
Answer options may be used more than once or not at all.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



IMAP , POP3 , SMTP - > Alert
HTTP,FTP,SMB -> Reset-both

NEW QUESTION 233

......