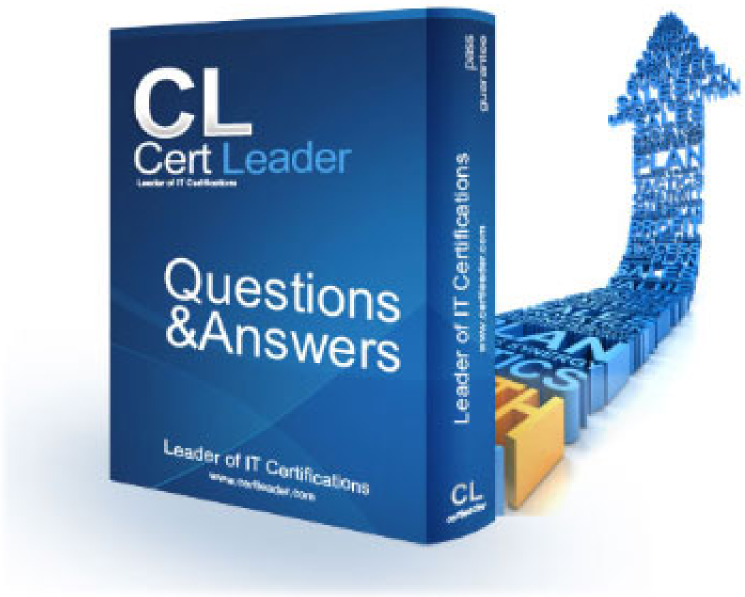
PCNSE Dumps

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

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

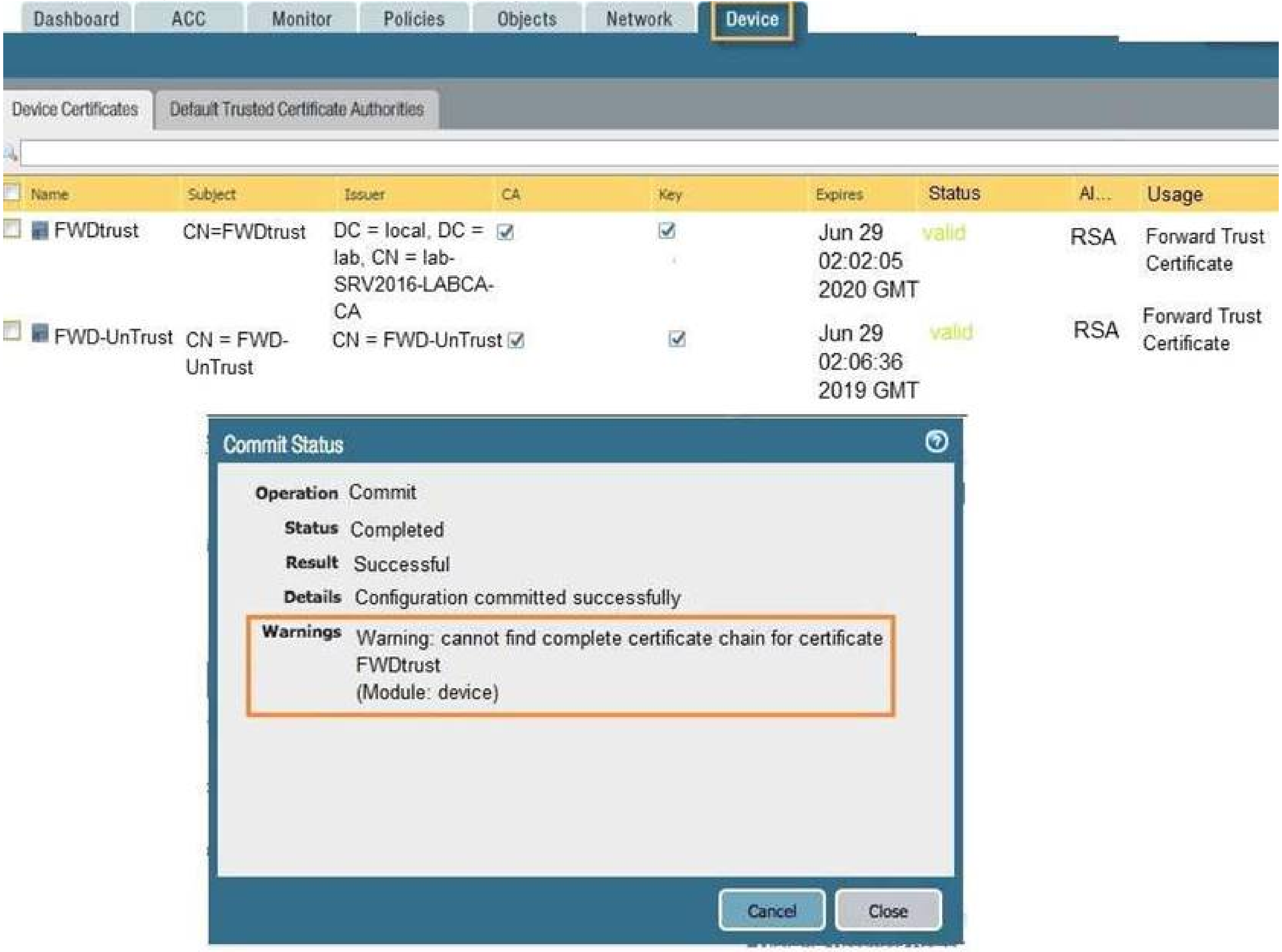


NEW QUESTION 1
Which three split tunnel methods are supported by a globalProtect gateway? (Choose three.)

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
Based on the image, what caused the commit warning?



☐	Name	Subject	Issuer	CA	Key	Expires	Status	Al...	Usage
☐	FWDtrust	CN=FWDtrust	DC = local, DC = lab, CN = lab-SRV2016-LABCA-CA	☑	☑	Jun 29 02:02:05 2020 GMT	valid	RSA	Forward Trust Certificate
☐	FWD-UnTrust	CN = FWD-UnTrust	CN = FWD-UnTrust	☑	☑	Jun 29 02:06:36 2019 GMT	valid	RSA	Forward Trust Certificate

Commit Status

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

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

Answer: D

NEW QUESTION 3
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

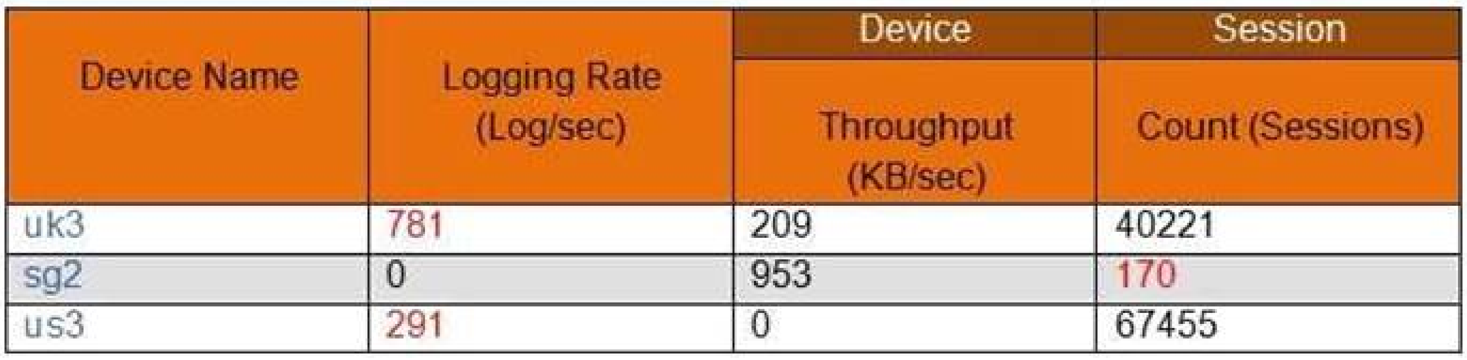
NEW QUESTION 4
Which feature can provide NGFWs with User-ID mapping information?

A. Web Captcha

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

Answer: C

NEW QUESTION 5
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

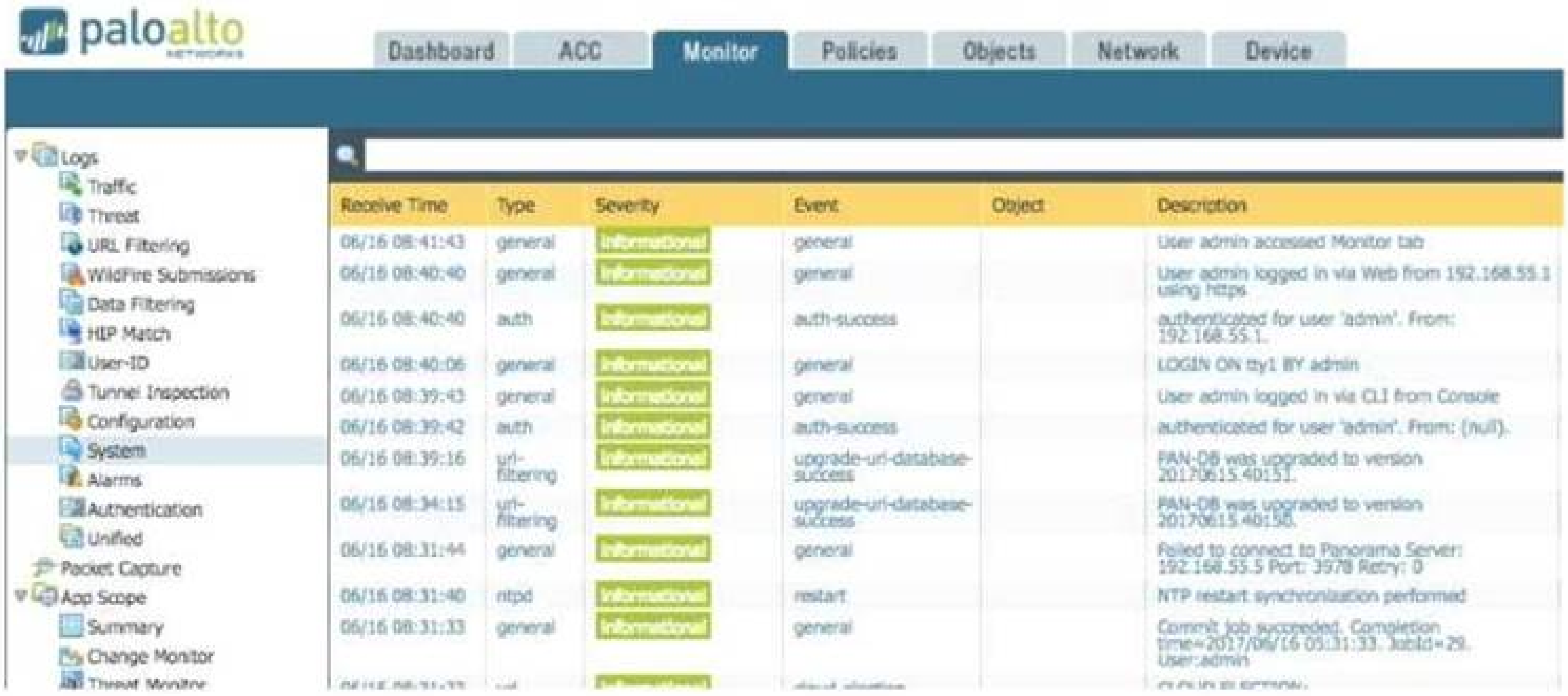
NEW QUESTION 6
An administrator has been asked to configure active/active HA for a pair of Palo Alto Networks NGFWs. The firewall use Layer 3 interfaces to send traffic to a single gateway IP for the pair.
Which configuration will enable this HA scenario?

A. The two firewalls will share a single floating IP and will use gratuitous ARP to share the floating IP.
B. Each firewall will have a separate floating IP, and priority will determine which firewall has the primary IP.
C. The firewalls do not use floating IPs in active/active HA.
D. The firewalls will share the same interface IP address, and device 1 will use the floating IP if device 0 fails.

Answer: A

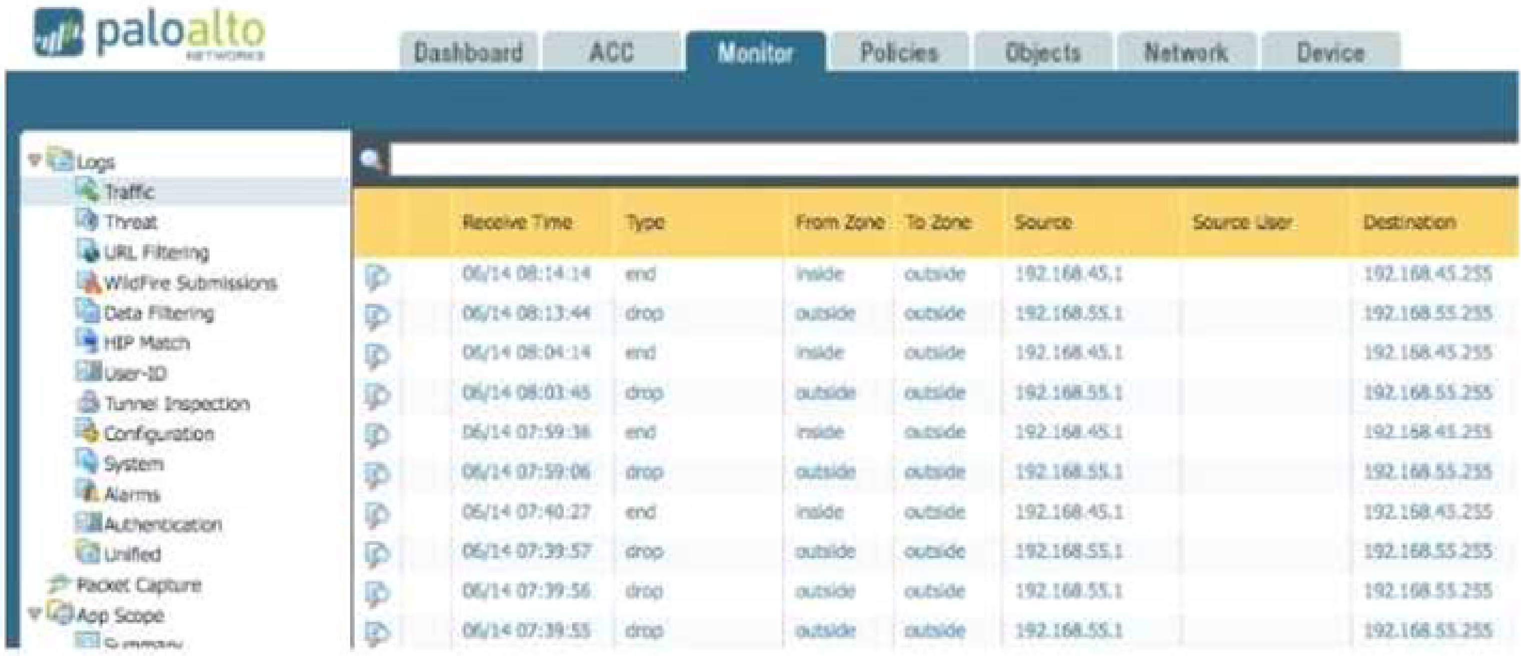
NEW QUESTION 7
An administrator accidentally closed the commit window/screen before the commit was finished. Which two options could the administrator use to verify the progress or success of that commit task? (Choose two.)

A



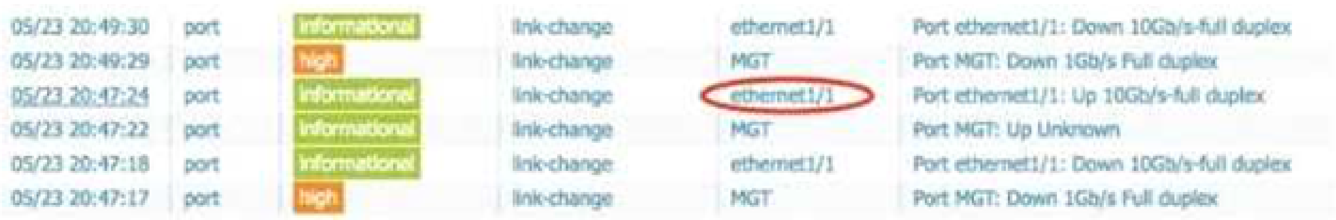
Receive Time	Type	Severity	Event	Object	Description
06/16 08:41:43	general	Informational	general		User admin accessed Monitor tab
06/16 08:40:40	general	Informational	general		User admin logged in via Web from 192.168.55.1 using https
06/16 08:40:40	auth	Informational	auth-success		authenticated for user 'admin'. From: 192.168.55.1.
06/16 08:40:06	general	Informational	general		LOGIN ON tty1 BY admin
06/16 08:39:43	general	Informational	general		User admin logged in via CLI from Console
06/16 08:39:42	auth	Informational	auth-success		authenticated for user 'admin'. From: (null).
06/16 08:39:16	url-filtering	Informational	upgrade-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
06/16 08:31:33	url	Informational	cloud-election		CLOUD ELECTION:

B



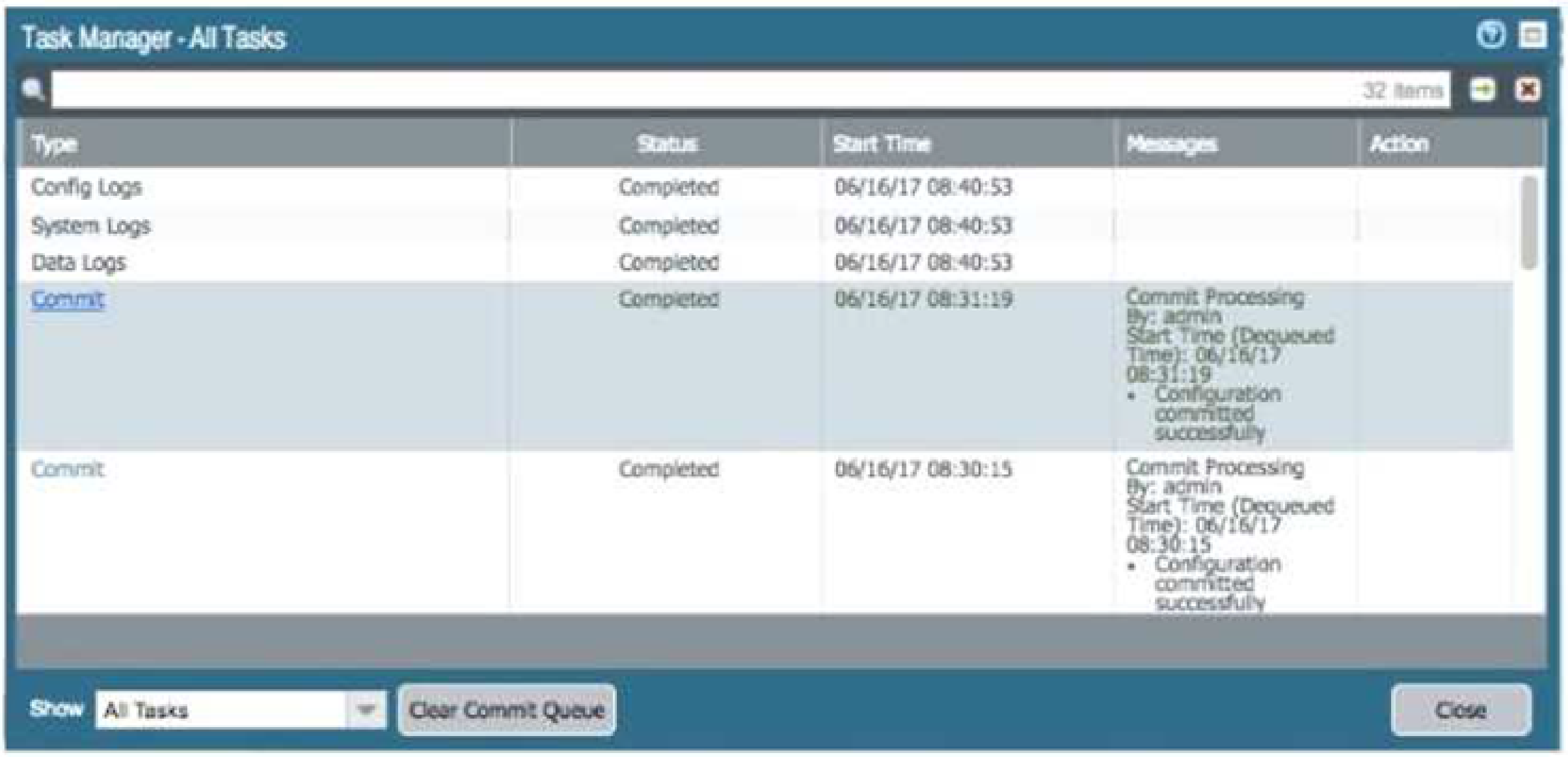
Receive Time	Type	From Zone	To Zone	Source	Source User	Destination
06/14 08:14:14	end	inside	outside	192.168.45.1		192.168.45.255
06/14 08:13:44	drop	outside	outside	192.168.55.1		192.168.55.255
06/14 08:04:14	end	inside	outside	192.168.45.1		192.168.45.255
06/14 08:03:45	drop	outside	outside	192.168.55.1		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



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

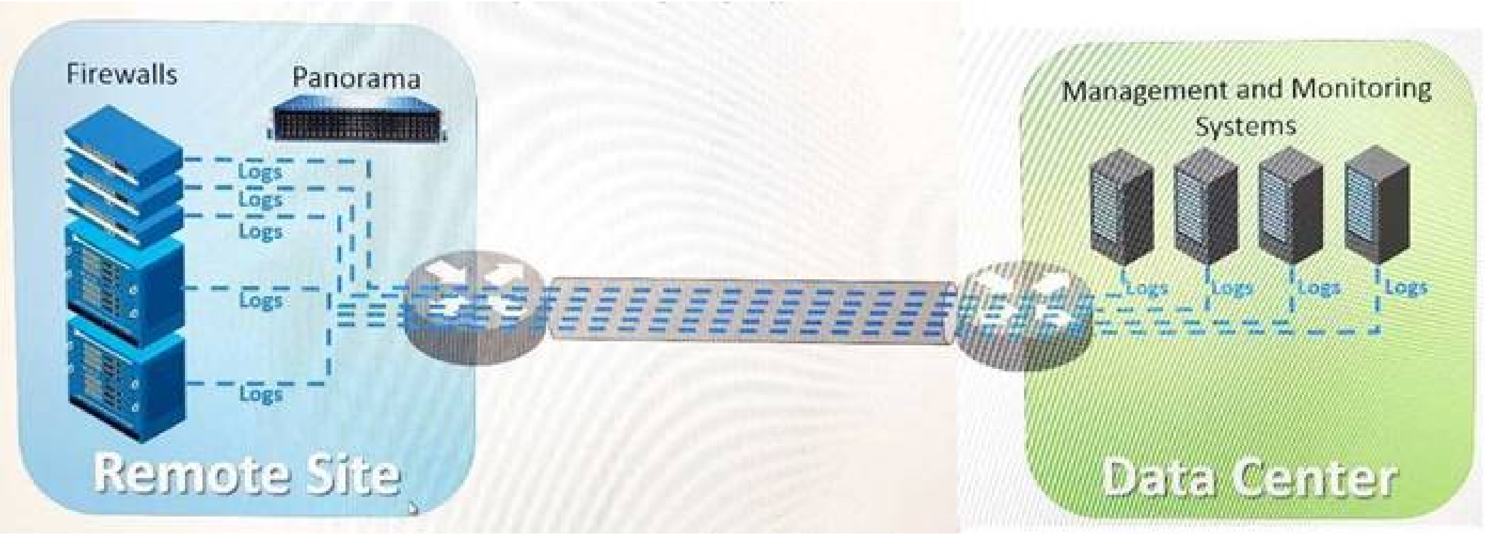
Answer: AD

NEW QUESTION 8
Which two actions would be part of an automatic solution that would block sites with untrusted certificates without enabling SSL Forward Proxy? (Choose two.)

A. Create a no-decrypt Decryption Policy rule.
B. Configure an EDL to pull IP addresses of known sites resolved from a CRL.
C. Create a Dynamic Address Group for untrusted sites
D. Create a Security Policy rule with vulnerability Security Profile attached.
E. Enable the “Block sessions with untrusted issuers” setting.

Answer: AD

NEW QUESTION 9
Refer to exhibit.



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

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

Answer: A

NEW QUESTION 10
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 10
An administrator has been asked to configure active/passive HA for a pair of Palo Alto Networks NGFWs. The administrator assigns priority 100 to the active firewall.
Which priority is correct for the passive firewall?

A. 99
B. 1
C. 255

Answer:

Explanation: Reference:
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/framemaker/71/pan-os/pan-os/section_5.pdf (page 9)

NEW QUESTION 12
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 14
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 16

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

NEW QUESTION 20
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 21
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 23
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 25
A speed/duplex negotiation mismatch is between the Palo Alto Networks management port and the switch port which it connects. How would an administrator configure the interface to 1Gbps?

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

Answer: B

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

NEW QUESTION 28
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

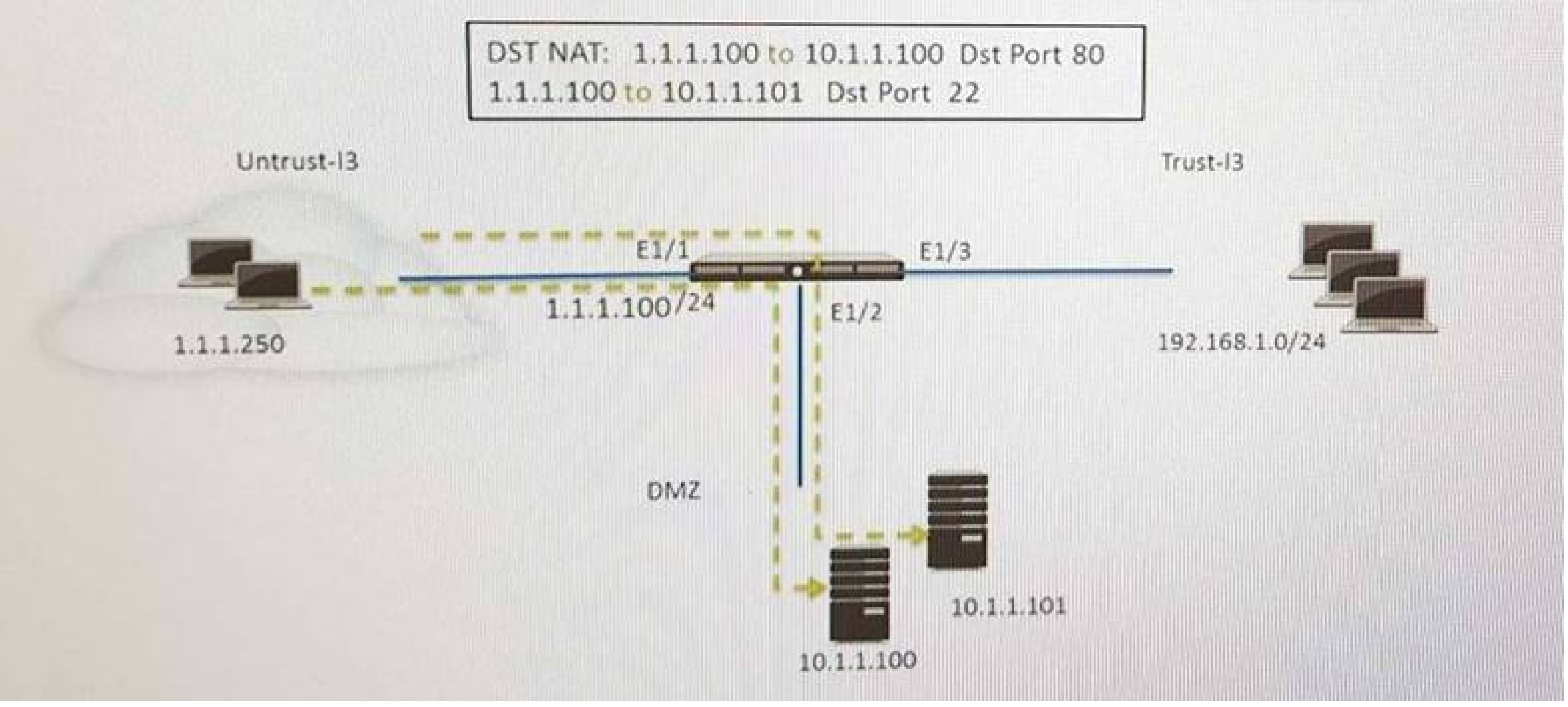
NEW QUESTION 32
How would an administrator monitor/capture traffic on the management interface of the Palo Alto Networks NGFW?

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 37
Refer to the exhibit.

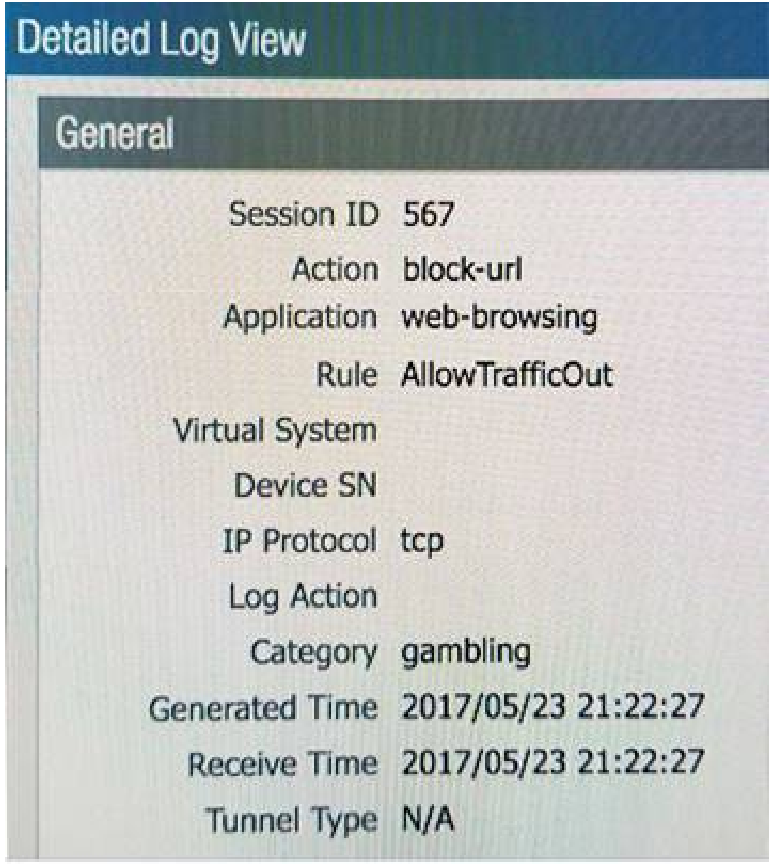


An administrator is using DNAT to map two servers to a single public IP address. Traffic will be steered to the specific server based on the application, where Host A (10.1.1.100) receives HTTP traffic and HOST B (10.1.1.101) receives SSH traffic.)
Which two security policy rules will accomplish this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

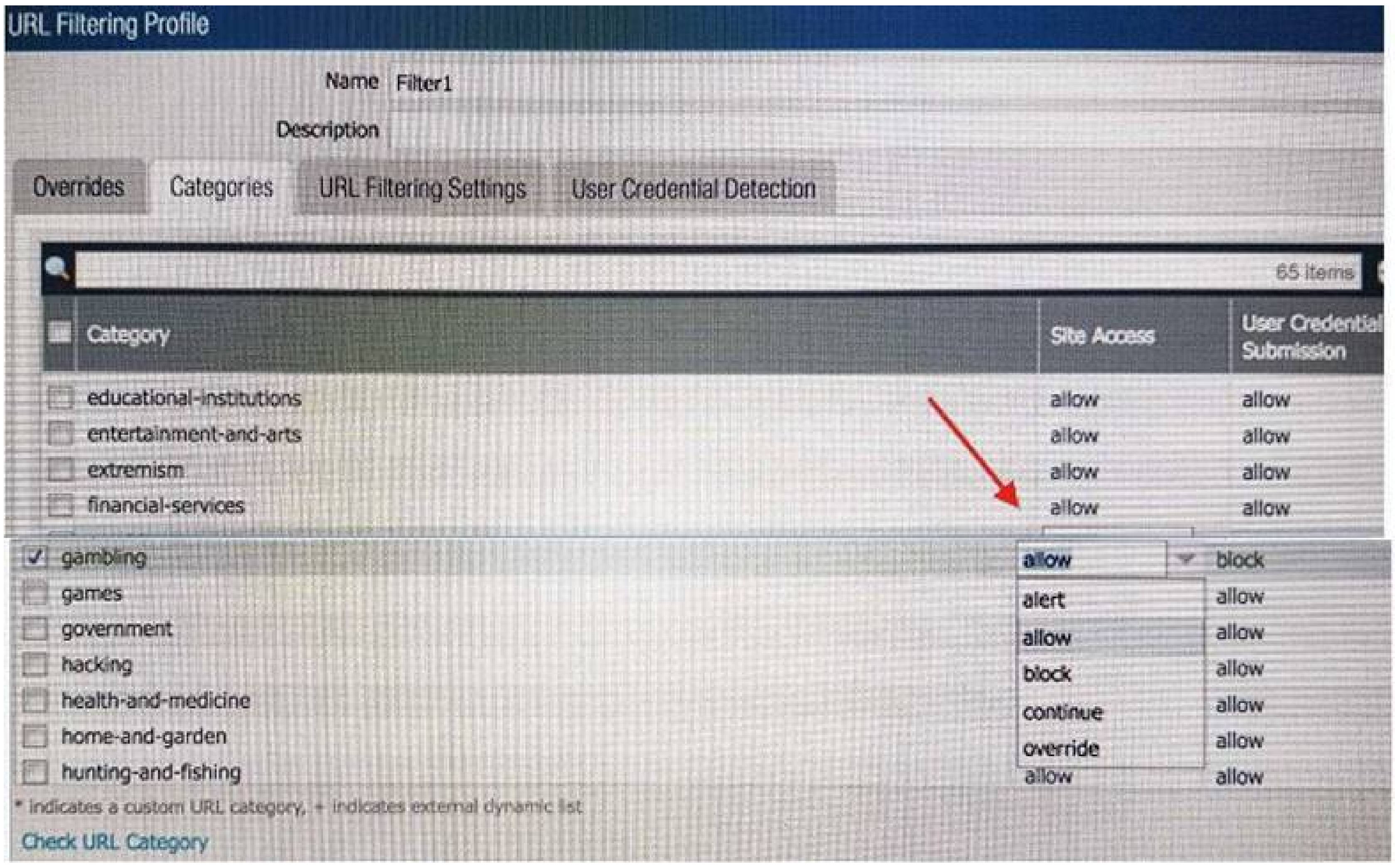
NEW QUESTION 41
An administrator needs to determine why users on the trust zone cannot reach certain websites. The only information available is shown on the following image. Which configuration change should the administrator make?
A)


Detailed Log View

General

Session ID 567
Action block-url
Application web-browsing
Rule AllowTrafficOut
Virtual System
Device SN
IP Protocol tcp
Log Action
Category gambling
Generated Time 2017/05/23 21:22:27
Receive Time 2017/05/23 21:22:27
Tunnel Type N/A

B)



URL Filtering Profile

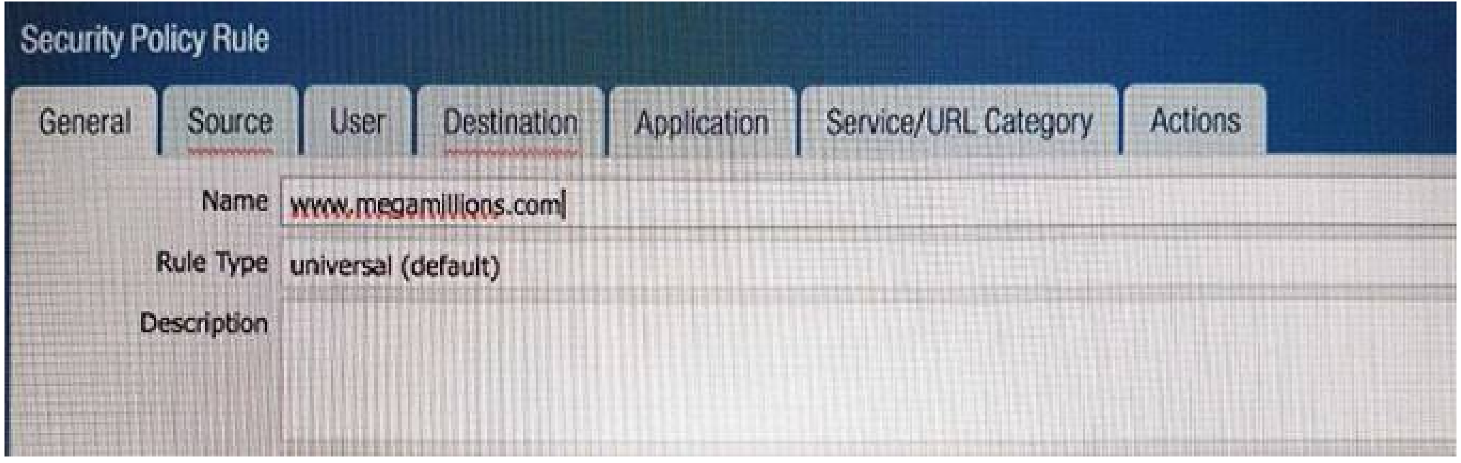
Name Filter1

Description

☐ Category	Site Access	User Credential Submission
☐ educational-institutions	allow	allow
☐ entertainment-and-arts	allow	allow
☐ extremism	allow	allow
☐ financial-services	allow	allow
☑ gambling	allow	block
☐ games	alert	allow
☐ government	allow	allow
☐ hacking	block	allow
☐ health-and-medicine	continue	allow
☐ home-and-garden	override	allow
☐ hunting-and-fishing	allow	allow

* indicates a custom URL category, + indicates external dynamic list

C)



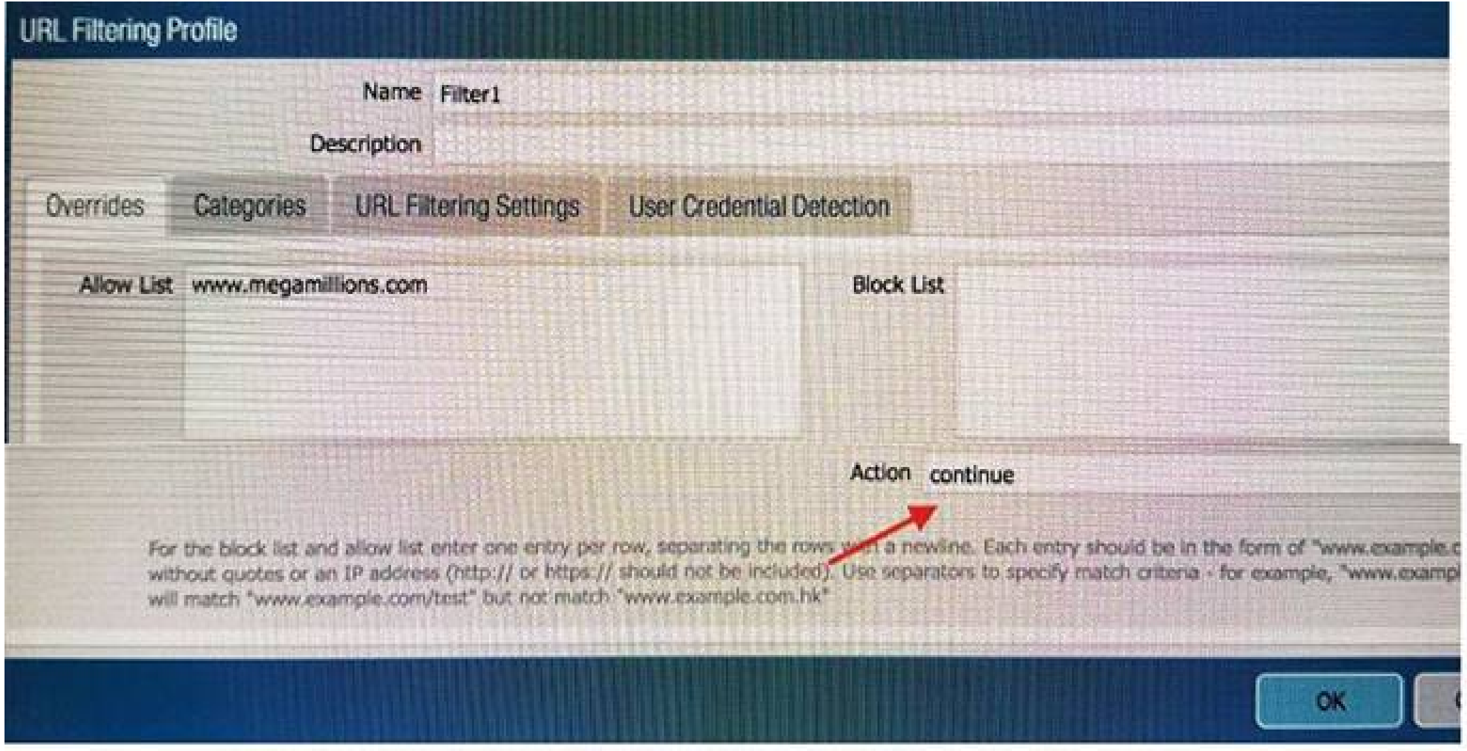
Security Policy Rule

Name www.megamillions.com

Rule Type universal (default)

Description

D)



URL Filtering Profile

Name Filter1

Description

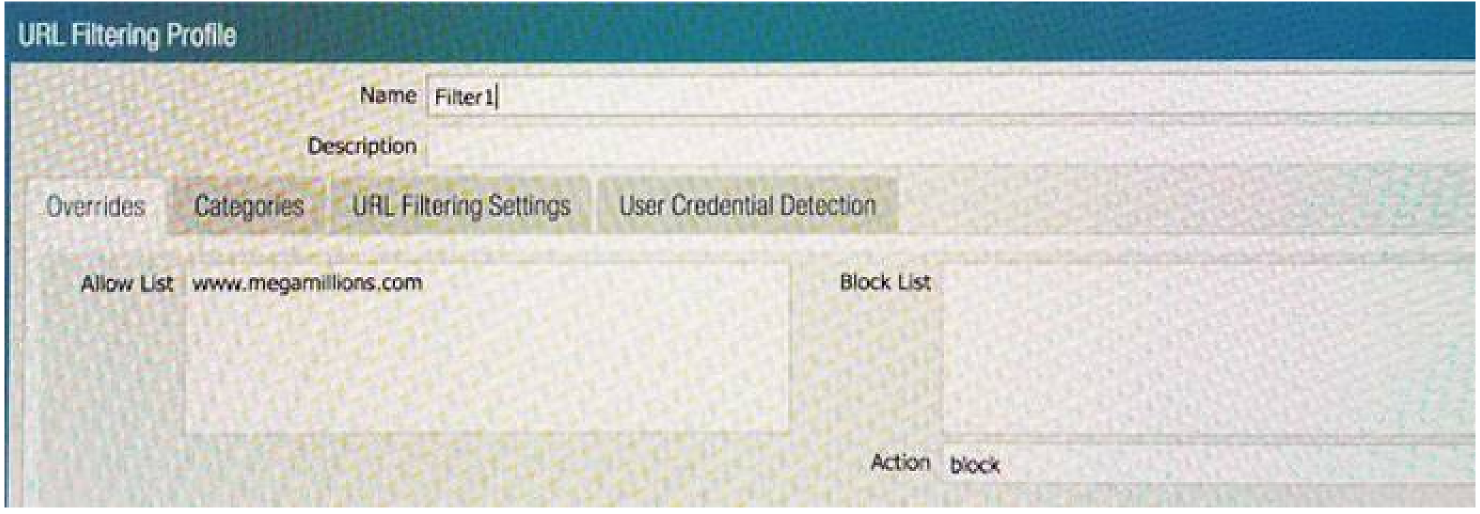
Allow List www.megamillions.com

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.c without quotes or an IP address (http:// or https:// should not be included). Use separators to specify match criteria - for example, "www.exampl will match "www.example.com/test" but not match "www.example.com.hk"

E)



URL Filtering Profile

Name Filter1

Description

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 45
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 47
An administrator has left a firewall to use the default port for all management services. Which three functions are performed by the dataplane? (Choose three.)

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

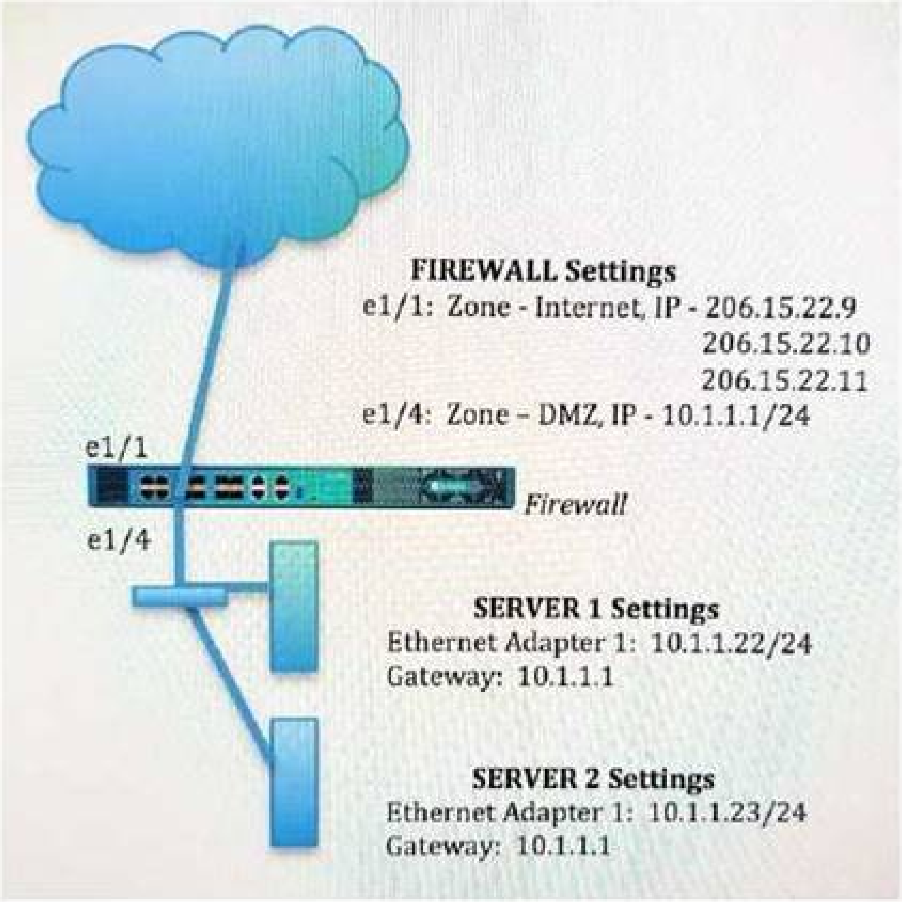
Answer: ABC

NEW QUESTION 50
An administrator is using Panorama and multiple Palo Alto Networks NGFWs. After upgrading all devices to the latest PAN-OS® software, the administrator enables log forwarding from the firewalls to Panorama. Pre-existing logs from the firewalls are not appearing in PanoramA.
Which action would enable the firewalls to send their pre-existing logs to Panorama?

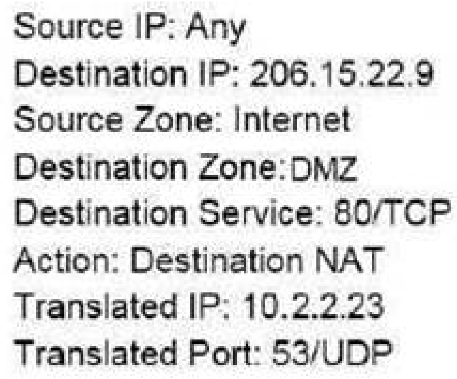
A. Use the import option to pull logs into Panorama.
B. A CLI command will forward the pre-existing logs to Panorama.
C. Use the ACC to consolidate pre-existing logs.
D. The log database will need to exported form the firewalls and manually imported into Panorama.

Answer: B

NEW QUESTION 54
An administrator wants multiple web servers in the DMZ to receive connections initiated from the internet. Traffic destined for 206.15.22.9 port 80/TCP needs to be forwarded to the server at 10.1.1.22

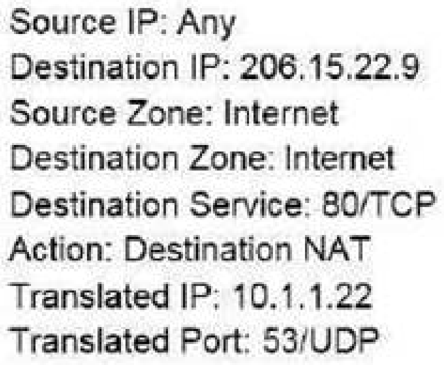

FIREWALL Settings
e1/1: Zone - Internet, IP - 206.15.22.9
206.15.22.10
206.15.22.11
e1/4: Zone - DMZ, IP - 10.1.1.1/24
e1/1
Firewall
e1/4
SERVER 1 Settings
Ethernet Adapter 1: 10.1.1.22/24
Gateway: 10.1.1.1
SERVER 2 Settings
Ethernet Adapter 1: 10.1.1.23/24
Gateway: 10.1.1.1

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



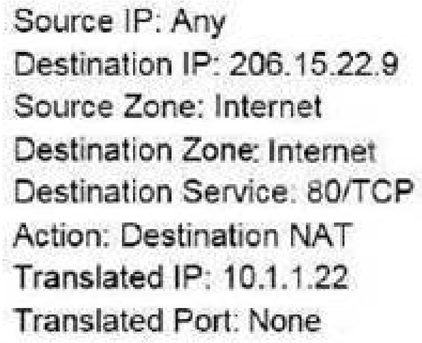
Source IP: Any
Destination IP: 206.15.22.9
Source Zone: Internet
Destination Zone: DMZ
Destination Service: 80/TCP
Action: Destination NAT
Translated IP: 10.2.2.23
Translated Port: 53/UDP

B)



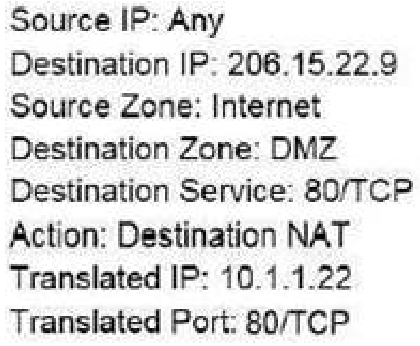
Source IP: Any
Destination IP: 206.15.22.9
Source Zone: Internet
Destination Zone: Internet
Destination Service: 80/TCP
Action: Destination NAT
Translated IP: 10.1.1.22
Translated Port: 53/UDP

C)



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

D)



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

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

Answer: D

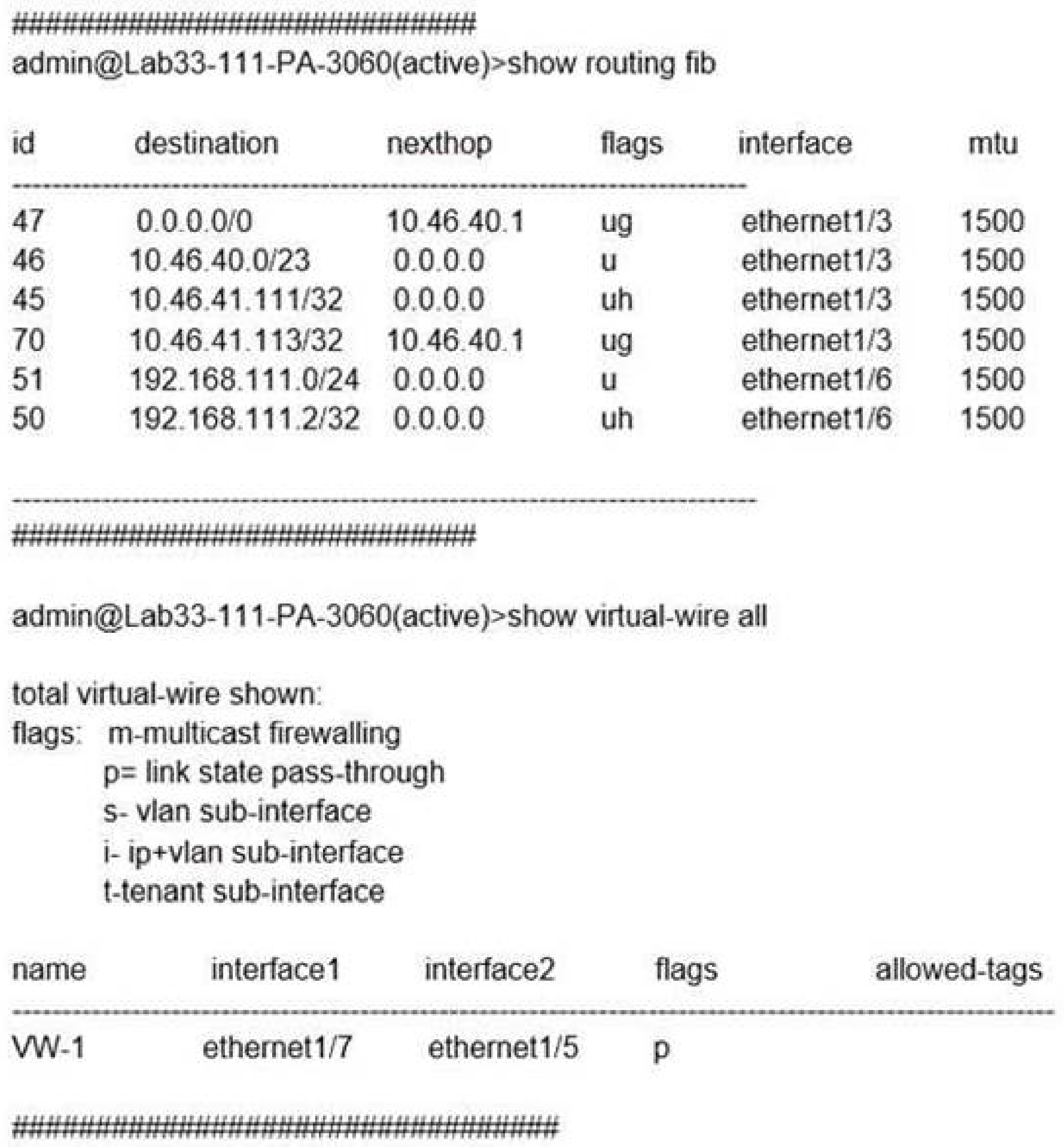
NEW QUESTION 55
Which three file types can be forwarded to WildFire for analysis as a part of the basic WildFire service? (Choose three.)

A. dll
B. exe
C. src
D. apk
E. pdf
F. jar

Answer: DEF

Explanation: Reference: https://www.paloaltonetworks.com/documentation/80/wildfire/wf_admin/wildfire-overview/wildfire-file-type-support

NEW QUESTION 59
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 64
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: D

NEW QUESTION 65
Which event will happen if an administrator uses an Application Override Policy?

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

Answer: B

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

NEW QUESTION 67
If the firewall is configured for credential phishing prevention using the “Domain Credential Filter” method, which login will be detected as credential theft?

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

Answer: A

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

NEW QUESTION 72
Which option is part of the content inspection process?

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

Answer: A

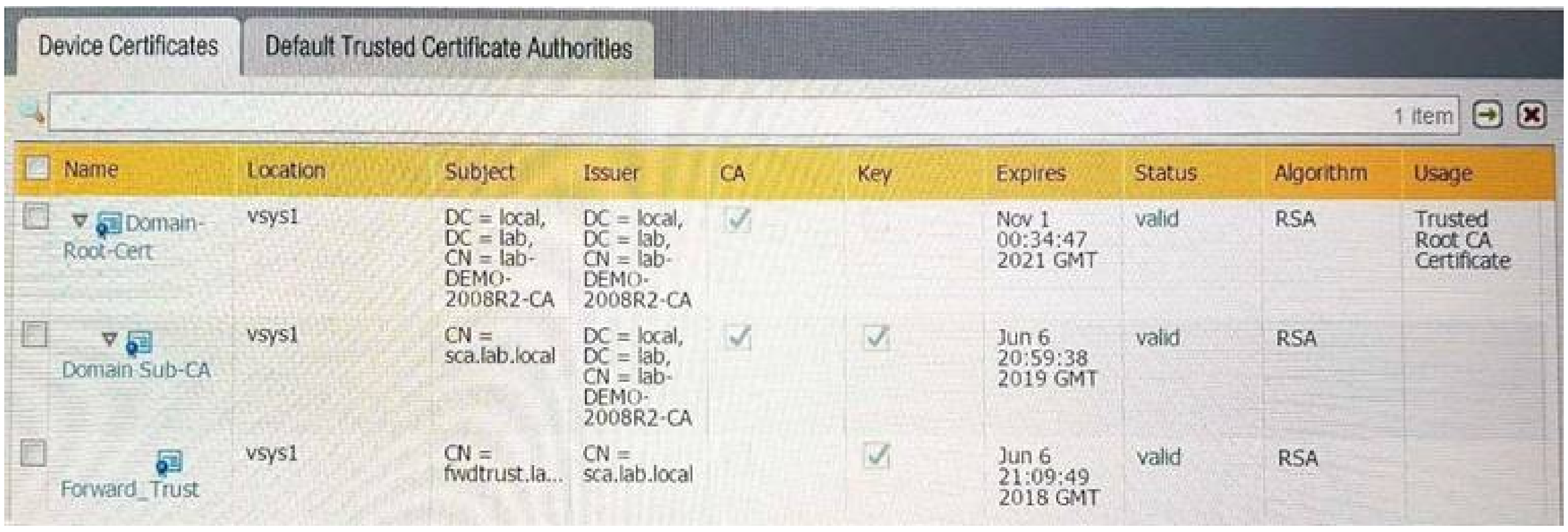
NEW QUESTION 76
In a virtual router, which object contains all potential routes?

A. MIB
B. RIB
C. SIP
D. FIB

Answer: B

Explanation: Reference: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=10&ved=0ahUKEwiOkbfYzPzXAhVnEJoKHcwVCg4QFghiMAk&url=https%3A%2F%2Flive.paloaltonetworks.com%2Ftwzvq79624%2Fattachments%2Ftwzvq79624%2Fdocumentation_tkb%2F487%2F1%2FRoute%2520Redistribution%2520and%2520Filtering%2520TechNote%2520-%2520Rev% 2520B. pdf&usg=AOvVaw0H9qgaJK0oI2xjIJBNo1Km

NEW QUESTION 77
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 80
Which option would an administrator choose to define the certificate and protocol that Panorama and its managed devices use for SSL/TLS services?

A. Configure a Decryption Profile and select SSL/TLS services.
B. Set up SSL/TLS under Polices > Service/URL Category>Service.
C. Set up Security policy rule to allow SSL communication.
D. Configure an SSL/TLS Profile.

Answer: D

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

NEW QUESTION 82
Which item enables a firewall administrator to see details about traffic that is currently active through the NGFW?

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

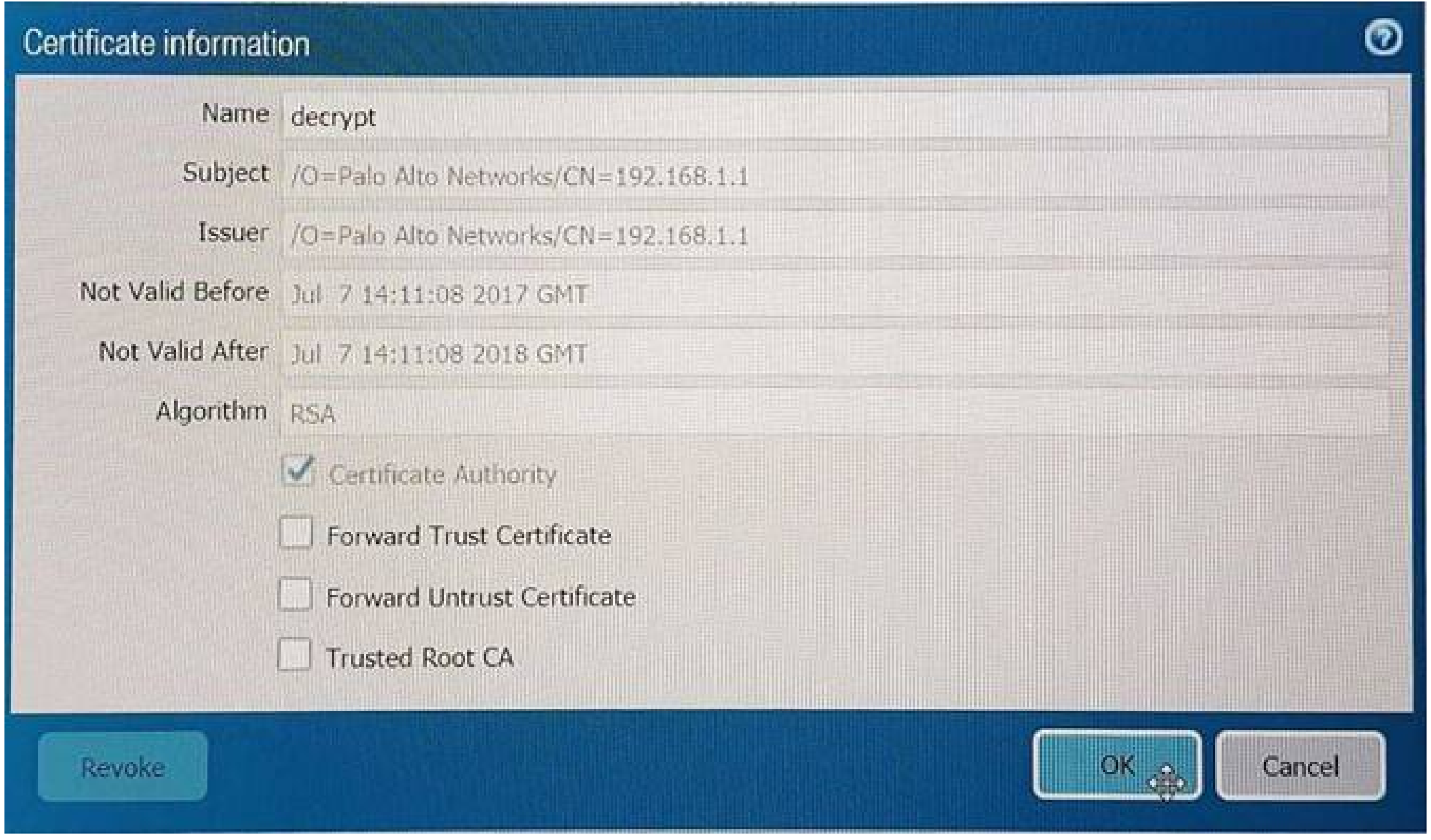
Answer: D

NEW QUESTION 87
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 92
The certificate information displayed in the following image is for which type of certificate? Exhibit:



Certificate information

Name decrypt
Subject /O=Palo Alto Networks/CN=192.168.1.1
Issuer /O=Palo Alto Networks/CN=192.168.1.1
Not Valid Before Jul 7 14:11:08 2017 GMT
Not Valid After Jul 7 14:11:08 2018 GMT
Algorithm RSA

☑ Certificate Authority
□ Forward Trust Certificate
□ Forward Untrust Certificate
□ Trusted Root CA

A. Forward Trust certificate
B. Self-Signed Root CA certificate
C. Web Server certificate
D. Public CA signed certificate

Answer: D

NEW QUESTION 95
Which three steps will reduce the CPU utilization on the management plane? (Choose three.)

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

Answer: CD

NEW QUESTION 96
Which feature must you configure to prevent users form accidentally submitting their corporate credentials to a phishing website?

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

Answer: A

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

NEW QUESTION 97
The administrator has enabled BGP on a virtual router on the Palo Alto Networks NGFW, but new routes do not seem to be populating the virtual router. Which two options would help the administrator troubleshoot this issue? (Choose two.)

A. View the System logs and look for the error messages about BGP.
B. Perform a traffic pcap on the NGFW to see any BGP problems.
C. View the Runtime Stats and look for problems with BGP configuration.

D. View the ACC tab to isolate routing issues.

Answer: CD

NEW QUESTION 102
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 103
Which virtual router feature determines if a specific destination IP address is reachable?

A. Heartbeat Monitoring
B. Failover
C. Path Monitoring
D. Ping-Path

Answer: C

Explanation: Reference: https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/policy/pbf

NEW QUESTION 105
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 110
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 112
An administrator has created an SSL Decryption policy rule that decrypts SSL sessions on any port. Which log entry can the administrator use to verify that sessions are being decrypted?

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

Answer: A

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

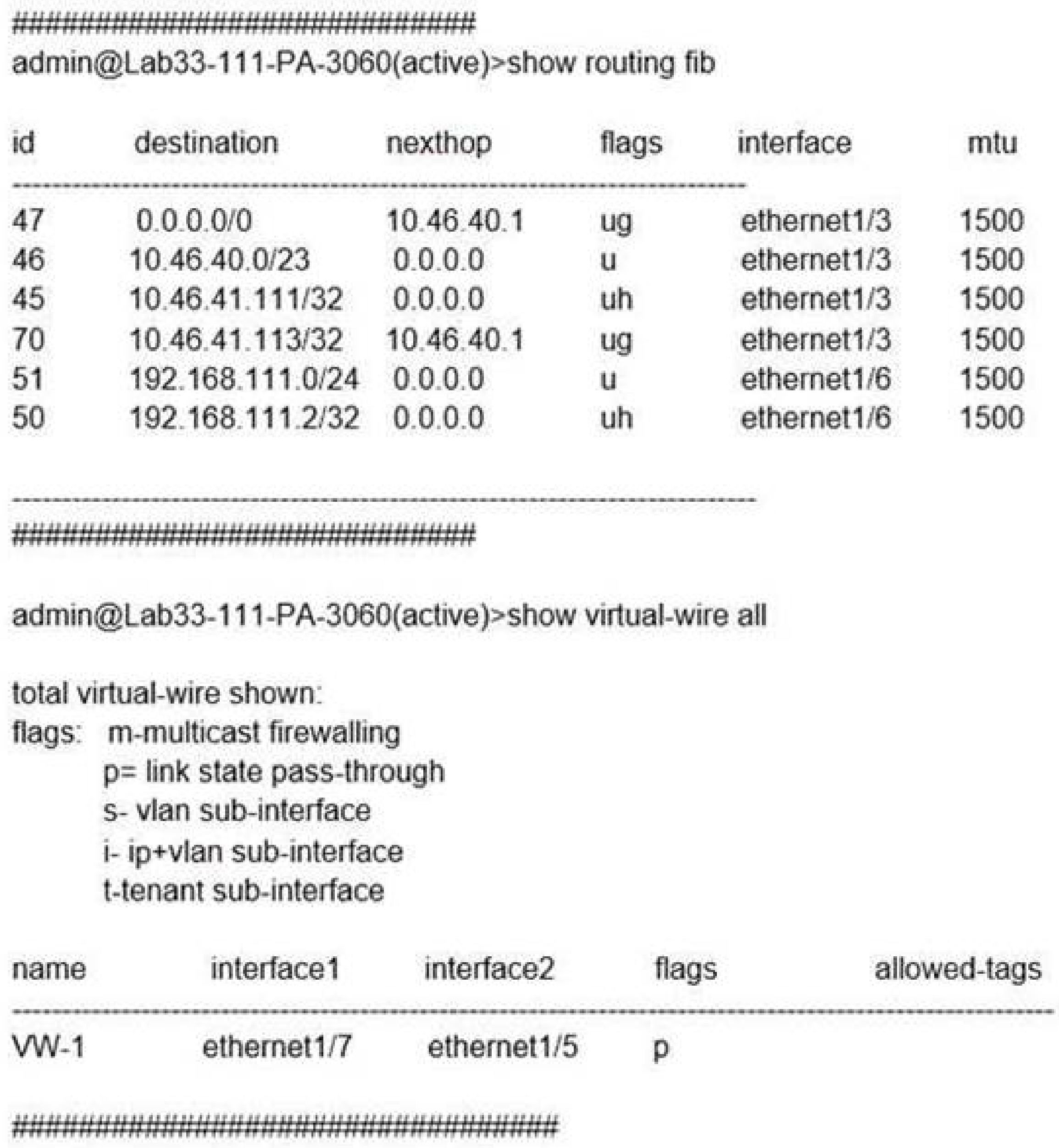
NEW QUESTION 116
Which processing order will be enabled when a Panorama administrator selects the setting “Objects defined in ancestors will take higher precedence?”

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 117
Exhibit:



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

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

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

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

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

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

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

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

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

Answer: D

NEW QUESTION 119
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 121
Which two options prevent the firewall from capturing traffic passing through it? (Choose two.)

A. The firewall is in multi-vsys mode.
B. The traffic is offloaded.
C. The traffic does not match the packet capture filter.

D. The firewall's DP CPU is higher than 50%.

Answer: BC

Explanation: Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/monitoring/take-packet-captures/disable-hardware-offload

NEW QUESTION 125
An administrator has been asked to create 100 virtual firewalls in a local, on-premise lab environment (not in "the cloud"). Bootstrapping is the most expedient way to perform this task. Which option describes deployment of a bootstrap package in an on-premise virtual environment?

A. Use config-drive on a USB stick.
B. Use an S3 bucket with an ISO.
C. Create and attach a virtual hard disk (VHD).
D. Use a virtual CD-ROM with an ISO.

Answer: D

Explanation: Reference: https://www.paloaltonetworks.com/documentation/71/pan-os/newfeaturesguide/management-features/bootstrapping-firewalls-for-rapid-deployment.html

NEW QUESTION 128
Which two benefits come from assigning a Decryption Profile to a Decryption policy rule with a "No Decrypt" action? (Choose two.)

A. Block sessions with expired certificates
B. Block sessions with client authentication
C. Block sessions with unsupported cipher suites
D. Block sessions with untrusted issuers
E. Block credential phishing

Answer: ABC

Explanation: Reference: https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/decryption/create-a-decryption-profile

NEW QUESTION 131
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

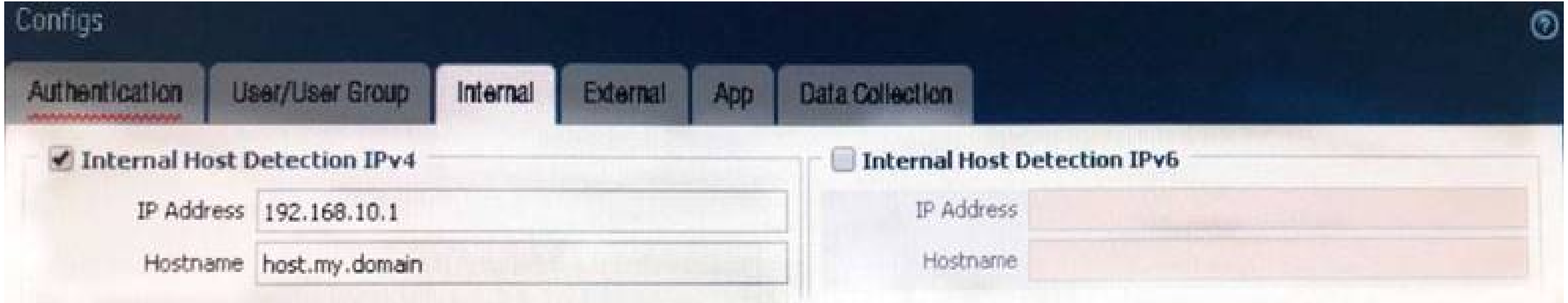
NEW QUESTION 132
If an administrator wants to decrypt SMTP traffic and possesses the server's certificate, which SSL decryption mode will allow the Palo Alto Networks NGFW to inspect traffic to the server?

A. TLS Bidirectional Inspection
B. SSL Inbound Inspection
C. SSH Forward Proxy
D. SMTP Inbound DecryptionExplanation:

Answer: B

Explanation: Reference: https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/decryption/configure-ssl-inbound-inspection

NEW QUESTION 134
View the GlobalProtect configuration screen capture.



☑ Internal Host Detection IPv4
IP Address 192.168.10.1
Hostname host.my.domain

□ Internal Host Detection IPv6
IP Address
Hostname

What is the purpose of this configuration?

A. It configures the tunnel address of all internal clients to an IP address range starting at 192.168.10.1.
B. It forces an internal client to connect to an internal gateway at IP address 192.168.10.1.
C. It enables a client to perform a reverse DNS lookup on 192.168.10.1 to detect that it is an internal client.
D. It forces the firewall to perform a dynamic DNS update, which adds the internal gateway’s hostname and IP address to the DNS server.

Answer: C

Explanation: Reference: https://www.paloaltonetworks.com/documentation/80/globalprotect/globalprotect-admin-guide/globalprotect-portals/define-the-globalprotect-client-authentication-configurations/define-the-globalprotect-agent-configurations

NEW QUESTION 136
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 141
Which prerequisite must be satisfied before creating an SSH proxy Decryption policy?

A. Both SSH keys and SSL certificates must be generated.
B. No prerequisites are required.
C. SSH keys must be manually generated.
D. SSL certificates must be generated.

Answer: B

Explanation: Reference: https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/decryption/configure-ssh-proxy

NEW QUESTION 146
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 151
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 154
Which logs enable a firewall administrator to determine whether a session was decrypted?

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

Answer: B

NEW QUESTION 157
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 162
An administrator wants a new Palo Alto Networks NGFW to obtain automatic application updates daily, so it is configured to use a scheduler for the application database. Unfortunately, they required the management network to be isolated so that it cannot reach the internet. Which configuration will enable the firewall to download and install application updates automatically?

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

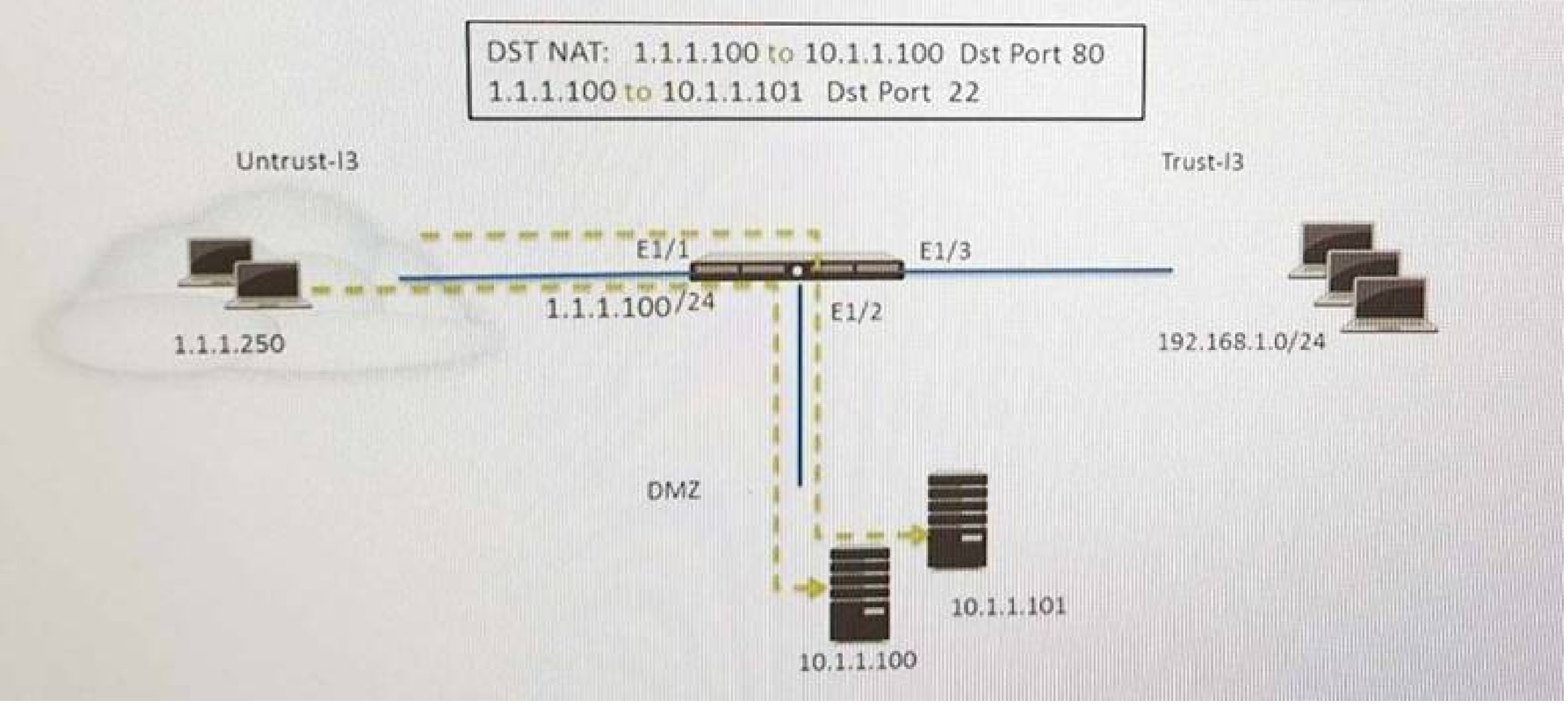
Answer: B

NEW QUESTION 163
Which three firewall states are valid? (Choose three)

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

Answer: ABC

NEW QUESTION 165
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) received 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) Ssh-Allow
B. Untrust (Any) to DMZ (1.1.1.100) Ssh-Allow
C. Untrust (Any) to DMZ (1.1.1.100) Web-browsing -Allow
D. Untrust (Any) to Untrust (10.1.1.1) Web-browsing -Allow

Answer: CD

NEW QUESTION 169
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 171
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 172
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 175
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 180
What are the differences between using a service versus using an application for Security Policy match?

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

Answer: B

NEW QUESTION 184
When backing up and saving configuration files, what is achieved using only the firewall and is not available in Panorama?

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

Answer: A

NEW QUESTION 189
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: D

NEW QUESTION 194
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 197
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 201
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 203
How is the Forward Untrust Certificate used?

A. It issues certificates encountered on the Untrust security zone when clients attempt to connect to a site that has be decrypted/
B. It is used when web servers request a client certificate.
C. It is presented to clients when the server they are connecting to is signed by a certificate authority that is not trusted by firewall.
D. It is used for Captive Portal to identify unknown users.

Answer: C

NEW QUESTION 206
What are three valid actions in a File Blocking Profile? (Choose three)

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

Answer: ABC

Explanation: https://live.paloaltonetworksHYPERLINK "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 207
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 208
Which three log-forwarding destinations require a server profile to be configured? (Choose three)

A. SNMP Trap
B. Email
C. RADIUS
D. Kerberos
E. Panorama
F. Syslog

Answer: ABF

NEW QUESTION 211
A critical US-CERT notification is published regarding a newly discovered botnet. The malware is very evasive and is not reliably detected by endpoint antivirus software. Furthermore, SSL is used to tunnel malicious traffic to command-and-control servers on the internet and SSL Forward Proxy Decryption is not enabled.
Which component once enabled on a perirneter firewall will allow the identification of existing infected hosts in an environment?

A. Anti-Spyware profiles applied outbound security policies with DNS Query action set to sinkhole
B. File Blocking profiles applied to outbound security policies with action set to alert
C. Vulnerability Protection profiles applied to outbound security policies with action set to block
D. Antivirus profiles applied to outbound security policies with action set to alert

Answer: A

NEW QUESTION 213
How does Panorama handle incoming logs when it reaches the maximum storage capacity?

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

Answer: D

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

NEW QUESTION 214
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 217
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

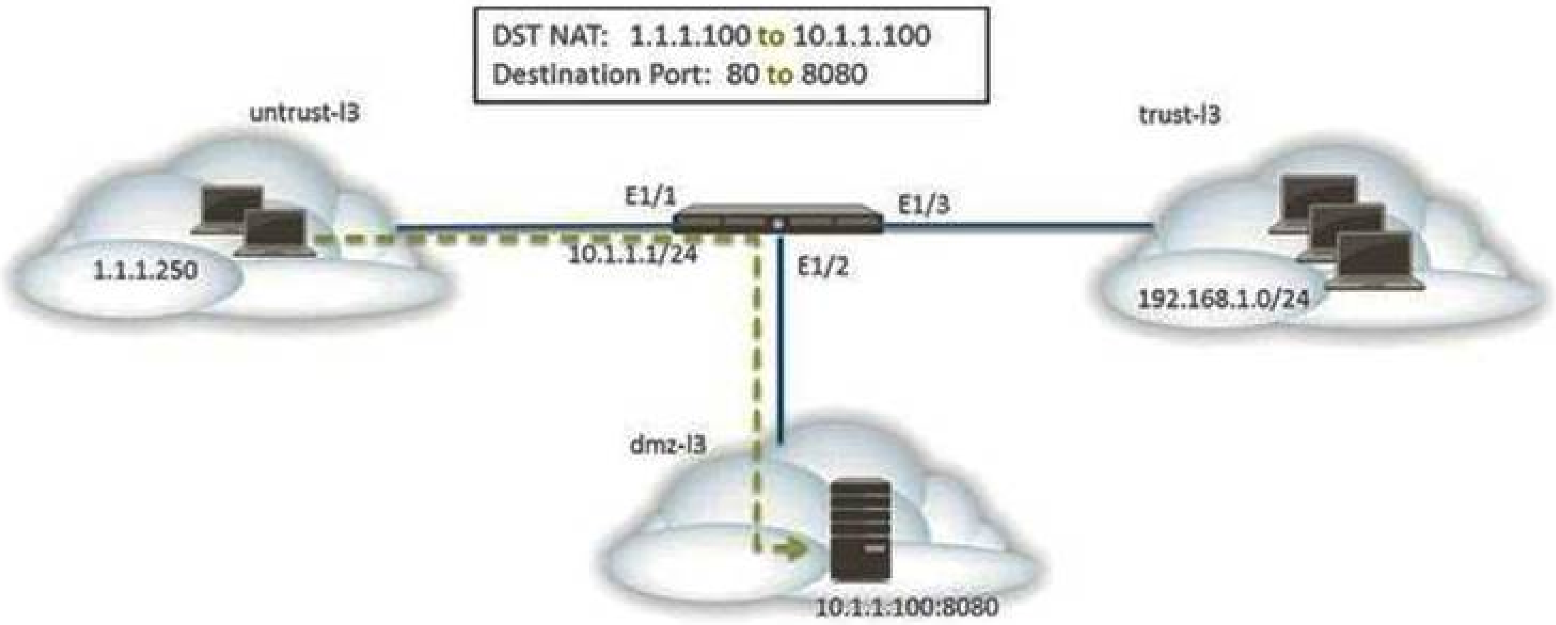
NEW QUESTION 219
Which two options are required on an M-100 appliance to configure it as a Log Collector? (Choose two)

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 the 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)

NEW QUESTION 222
The web server is configured to listen for HTTP traffic on port 8080. The clients access the web server using the IP address 1.1.1.100 on TCP Port 80. The destination NAT rule is configured to translate both IP address and report to 10.1.1.100 on TCP Port 8080.



Which NAT and security rules must be configured on the firewall? (Choose two)

A. A security policy with a source of any from untrust-I3 Zone to a destination of 10.1.1.100 in dmz-I3 zone using web-browsing application
B. A NAT rule with a source of any from untrust-I3 zone to a destination of 10.1.1.100 in dmz-zone using service-http service.
C. A NAT rule with a source of any from untrust-I3 zone to a destination of 1.1.1.100 in untrust-I3 zone using service-http service.
D. A security policy with a source of any from untrust-I3 zone to a destination of 1.1.100 in dmz-I3 zone using web-browsing application.

Answer: BD

NEW QUESTION 226
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 230
A company has a web server behind a Palo Alto Networks next-generation firewall that it wants to make accessible to the public at 1.1.1.1. The company has decided to configure a destination NAT Policy rule.
Given the following zone information:
• DMZ zone: DMZ-L3
• Public zone: Untrust-L3
• Guest zone: Guest-L3
• Web server zone: Trust-L3
• Public IP address (Untrust-L3): 1.1.1.1
• Private IP address (Trust-L3): 192.168.1.50
What should be configured as the destination zone on the Original Packet tab of NAT Policy rule?

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

Answer: A

NEW QUESTION 234
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 238
What must be used in Security Policy Rule that contain addresses where NAT policy applies?

A. Pre-NAT addresse and Pre-NAT zones
B. Post-NAT addresse and Post-Nat zones
C. Pre-NAT addresse and Post-Nat zones
D. Post-Nat addresses and Pre-NAT zones

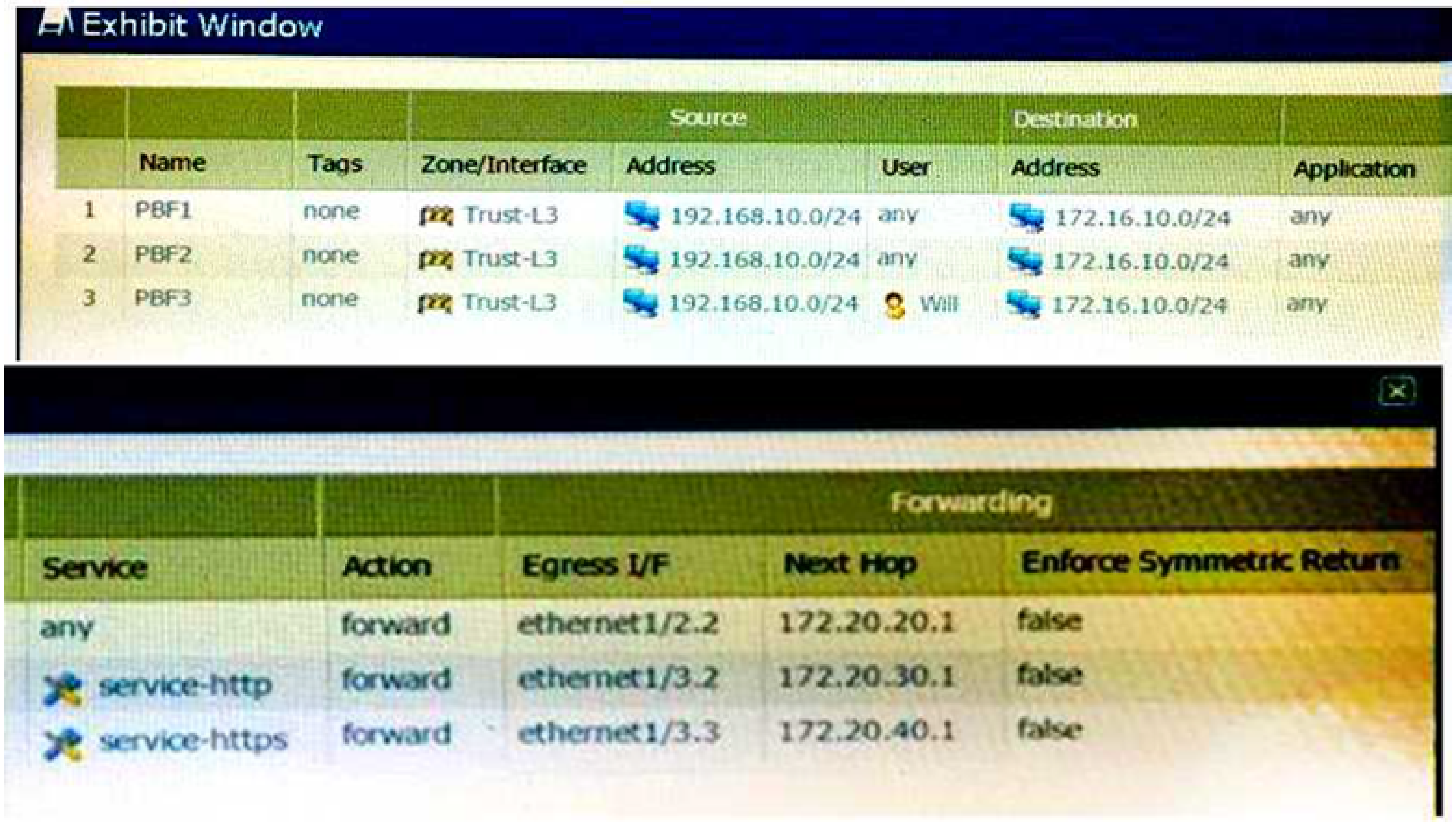
Answer: C

NEW QUESTION 243
A network administrator uses Panorama to push security polices to managed firewalls at branch offices. Which policy type should be configured on Panorama if the administrators at the branch office sites to override these products?

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

Answer: A

NEW QUESTION 247
Click the Exhibit button below,



			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 250
Which Security Policy Rule configuration option disables antivirus and anti-spyware scanning of server-to-client flows only?

A. Disable Server Response Inspection
B. Apply an Application Override
C. Disable HIP Profile
D. Add server IP Security Policy exception

Answer: A

NEW QUESTION 253
How are IPV6 DNS queries configured to user interface ethernet1/3?

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

Answer: D

NEW QUESTION 255
A firewall administrator is troubleshooting problems with traffic passing through the Palo Alto Networks firewall. Which method shows the global counters associated with the traffic after configuring the appropriate packet filters?

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

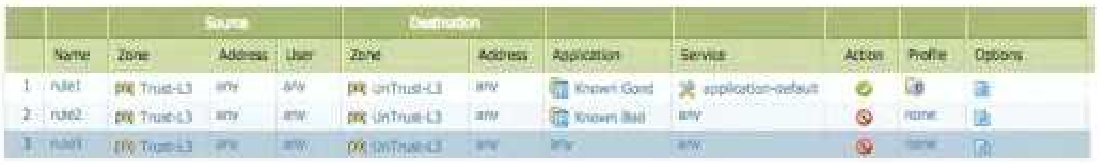
Answer: B

NEW QUESTION 258
Which interface configuration will accept specific VLAN IDs?

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

Answer: B

NEW QUESTION 262
A company has a policy that denies all applications it classifies as bad and permits only application it classifies as good. The firewall administrator created the following security policy on the company's
firewall.



		Source			Destination						
	Name	Zone	Address	User	Zone	Address	Application	Service	Action	Profile	Options
1	rule1	Trust-L3	any	any	UnTrust-L3	any	Known Good	application-default	✓		
2	rule2	Trust-L3	any	any	UnTrust-L3	any	Known Bad	any	⊘	none	
3	rule3	Trust-L3	any	any	UnTrust-L3	any	any	any	⊘	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 263
A client is deploying a pair of PA-5000 series firewalls using High Availability (HA) in Active/Passive mode. Which statement is true about this deployment?

A. The two devices must share a routable floating IP address
B. The two devices may be different models within the PA-5000 series
C. The HA1 IP address from each peer must be on a different subnet
D. The management port may be used for a backup control connection

Answer: D

NEW QUESTION 265
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 267
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 272
Which option is an IPv6 routing protocol?

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

Answer: B

NEW QUESTION 275
Several offices are connected with VPNs using static IPv4 routes. An administrator has been tasked with implementing OSPF to replace static routing.
Which step is required to accomplish this goal?

A. Assign an IP address on each tunnel interface at each site
B. Enable OSPFv3 on each tunnel interface and use Area ID 0.0.0.0
C. Assign OSPF Area ID 0.0.0.0 to all Ethernet and tunnel interfaces
D. Create new VPN zones at each site to terminate each VPN connection

Answer: C

NEW QUESTION 279
Which URL Filtering Security Profile action togs the URL Filtering category to the URL Filtering log?

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

Answer: B

NEW QUESTION 281
A network security engineer has a requirement to allow an external server to access an internal web server. The internal web server must also initiate connections with the external server.
What can be done to simplify the NAT policy?

A. Configure ECMP to handle matching NAT traffic
B. Configure a NAT Policy rule with Dynamic IP and Port
C. Create a new Source NAT Policy rule that matches the existing traffic and enable the Bi-directional option
D. Create a new Destination NAT Policy rule that matches the existing traffic and enable the Bi- directional option

Answer: C

Explanation: https://www.paloaltonetworks.com/documentation/70/pan-os/pan-os/networking/nat-configuration-examples

NEW QUESTION 286
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 288
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 292
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 295
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 300
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"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"paloHYPERLINK "https://live.paloaltonetworks.com/t5/Learning-Articles/How-to-Interpret-show-system- resources/ta-p/59364"altonetworHYPERLINK "https://live.paloaltonetworks.com/t5/Learning- Articles/How-to-Interpret-show-system-resources/ta-p/59364"ks.com/t5/Learning-Articles/How-to- Interpret-show-system-resources/ta-p/59364

NEW QUESTION 302
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 305
Refer to Exhibit:

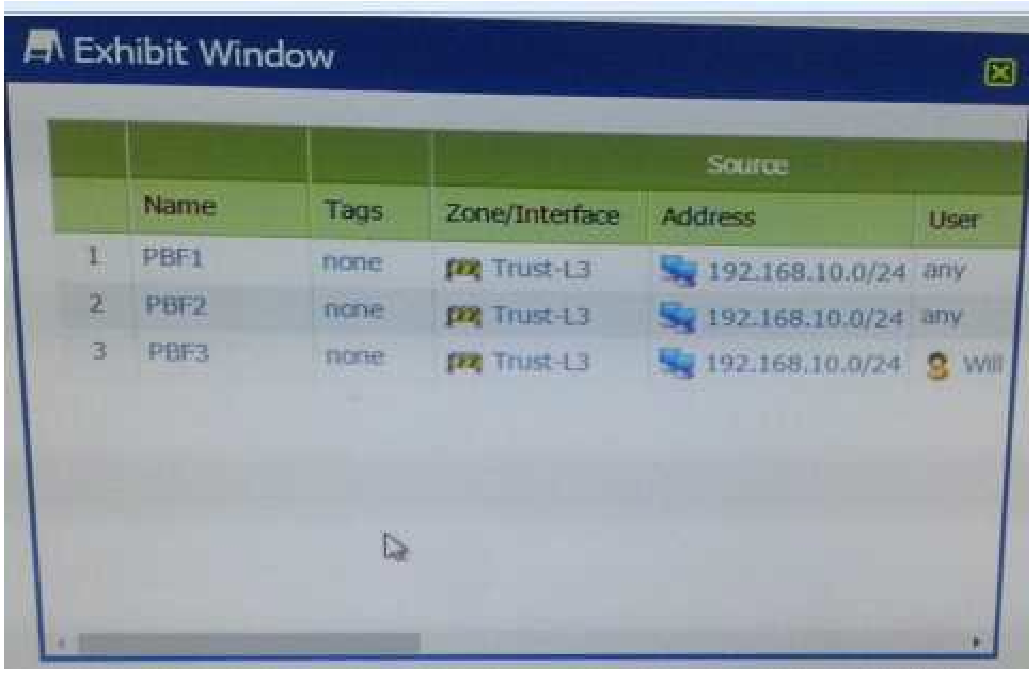


Exhibit Window

			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	Wil

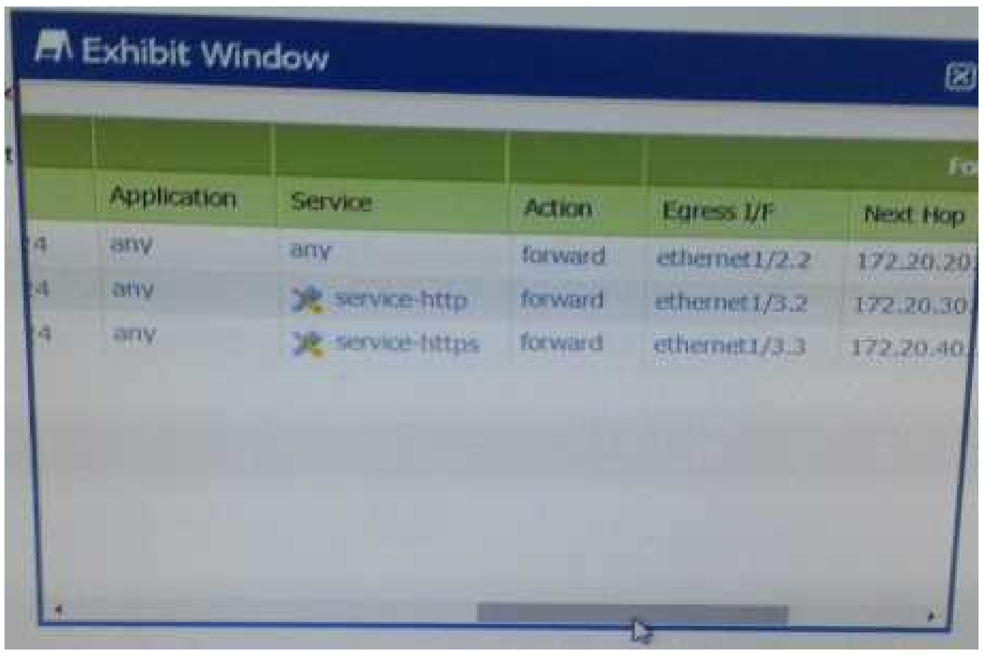


Exhibit Window

				Fo
Application	Service	Action	Egress I/F	Next Hop
any	any	forward	ethernet1/2.2	172.20.20
any	service-http	forward	ethernet1/3.2	172.20.30
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 306
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 309
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 310
......