Exam Questions PCNSE

Palo Alto Networks Certified Security Engineer (PCNSE)PAN-OS 9.0

https://www.2passeasy.com/dumps/PCNSE/

NEW QUESTION 1
- (Exam Topic 2)
Which CLI command enables an administrator to view details about the firewall including uptime, PAN-OS® version, and serial number?

A. debug system details
B. show session info
C. show system info
D. show system details

Answer: C

Explanation:
Reference:
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/technical-documentation/pan-os-60/PAN CLI-ref.pdf

NEW QUESTION 2
- (Exam Topic 2)
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: B

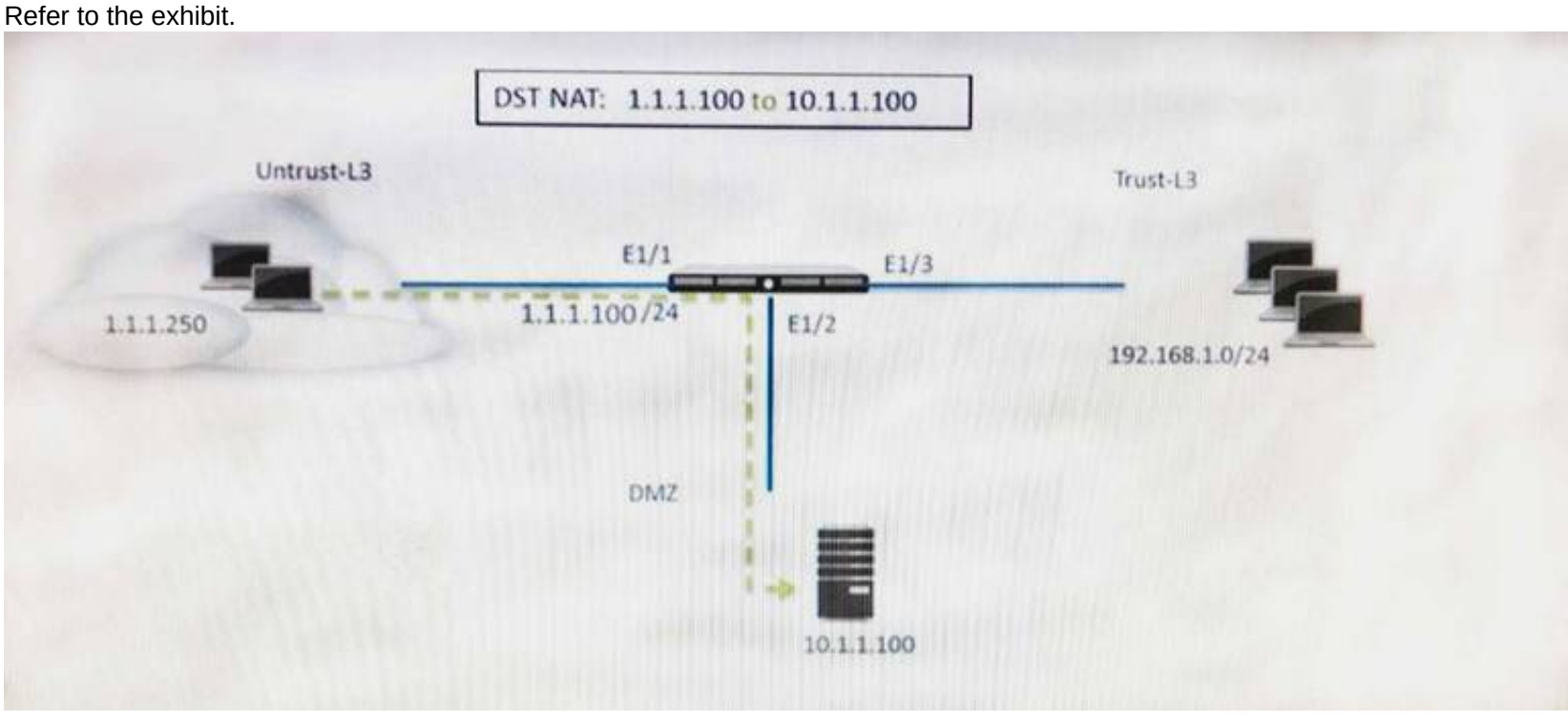
Explanation:
http://live.paloaltonetworks.com//t5/image/serverpage/image-id/12862i950F549C7D4E6309

NEW QUESTION 3
- (Exam Topic 2)
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 4
- (Exam Topic 2)
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: C

Explanation:
https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/networking/nat/nat-configuration-examples/destinat

NEW QUESTION 5
- (Exam Topic 2)
In which two types of deployment is active/active HA configuration supported? (Choose two.)

A. TAP mode
B. Layer 2 mode
C. Virtual Wire mode
D. Layer 3 mode

Answer: CD

NEW QUESTION 6
- (Exam Topic 2)
During the packet flow process, which two processes are performed in application identification? (Choose two.)

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

Answer: AB

Explanation:

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClVHCA0 http://live.paloaltonetworks.com//t5/image/serverpage/image-id/12862i950F549C7D4E6309

NEW QUESTION 7
- (Exam Topic 2)
An administrator has users accessing network resources through Citrix XenApp 7 x. Which User-ID mapping solution will map multiple users who are using Citrix to connect to the network and access resources?

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

Answer: C

NEW QUESTION 8
- (Exam Topic 2)
Which menu item enables a firewall administrator to see details about traffic that is currently active through the NGFW?

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

Answer: C

NEW QUESTION 9
- (Exam Topic 2)
Which log file can be used to identify SSL decryption failures?

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

Answer: D

Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClboCAC

NEW QUESTION 10
- (Exam Topic 2)
A client has a sensitive application server in their data center and is particularly concerned about resource exhaustion because of distributed denial-of-service attacks.
How can the Palo Alto Networks NGFW be configured to specifically protect this server against resource exhaustion originating from multiple IP addresses (DDoS attack)?

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

Answer: D

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

NEW QUESTION 10
- (Exam Topic 2)
A client has a sensitive application server in their data center and is particularly concerned about session flooding because of denial of-service attacks.
How can the Palo Alto Networks NGFW be configured to specifically protect this server against session floods originating from a single IP address?

A. Define a custom App-ID to ensure that only legitimate application traffic reaches the server
B. Add QoS Profiles to throttle incoming requests
C. Add a tuned DoS Protection Profile
D. Add an Anti-Spyware Profile to block attacking IP address

Answer: C

NEW QUESTION 11
- (Exam Topic 2)
An administrator needs to upgrade a Palo Alto Networks NGFW to the most current version of PAN-OS® software. The firewall has internet connectivity through an Ethernet interface, but no internet connectivity from the management interface. The Security policy has the default security rules and a rule that allows all web-browsing traffic from any to any zone. What must the administrator configure so that the PAN-OS® software can be upgraded?

A. Security policy rule
B. CRL
C. Service route
D. Scheduler

Answer: A

NEW QUESTION 15
- (Exam Topic 2)
VPN traffic intended for an administrator's Palo Alto Networks NGFW is being maliciously intercepted and retransmitted by the interceptor. When creating a VPN tunnel, which protection profile can be enabled to prevent this malicious behavior?

A. Zone Protection
B. Replay
C. Web Application
D. DoS Protection

Answer: B

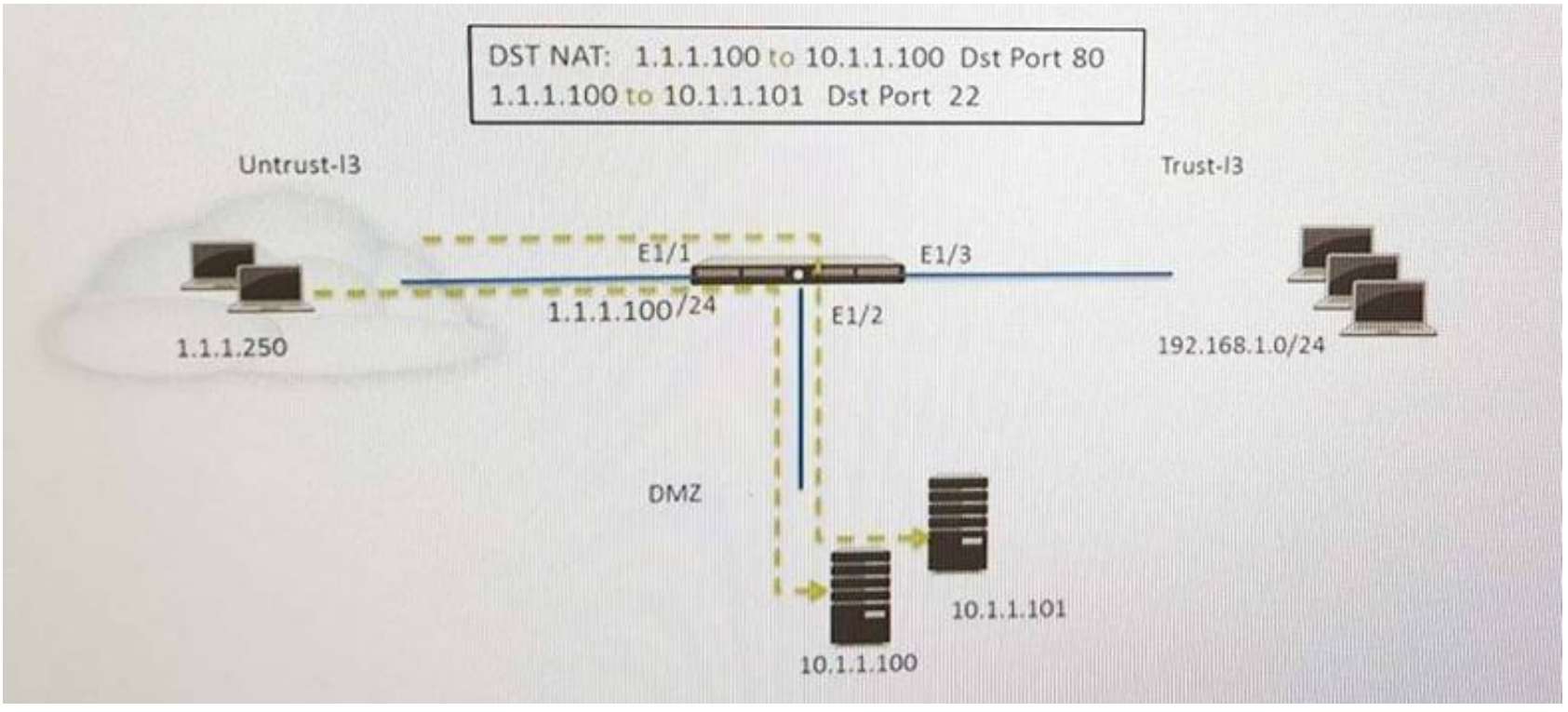
Explanation:
https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/vpns/set-up-site-to-site-vpn/set-up-an-ipsec-tunnel#

NEW QUESTION 17
- (Exam Topic 2)
What are the differences between using a service versus using an application for Security Policy match?

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

Answer: B

NEW QUESTION 18
- (Exam Topic 2)
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 21
- (Exam Topic 2)
What is exchanged through the HA2 link?

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

Answer: C

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

NEW QUESTION 26
- (Exam Topic 2)
What should an administrator consider when planning to revert Panorama to a pre-PAN-OS 8.1 version?

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

Answer: A

NEW QUESTION 27
- (Exam Topic 2)
An administrator has enabled OSPF on a virtual router on the NGFW. OSPF is not adding new routes to the virtual router. Which two options enable the administrator to troubleshoot this issue? (Choose two.)

A. View Runtime Stats in the virtual router.
B. View System logs.
C. Add a redistribution profile to forward as BGP updates.
D. Perform a traffic pcap at the routing stage.

Answer: AB

Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CldcCAC

NEW QUESTION 31
- (Exam Topic 2)
Which item enables a firewall administrator to see details about traffic that is currently active through the NGFW?

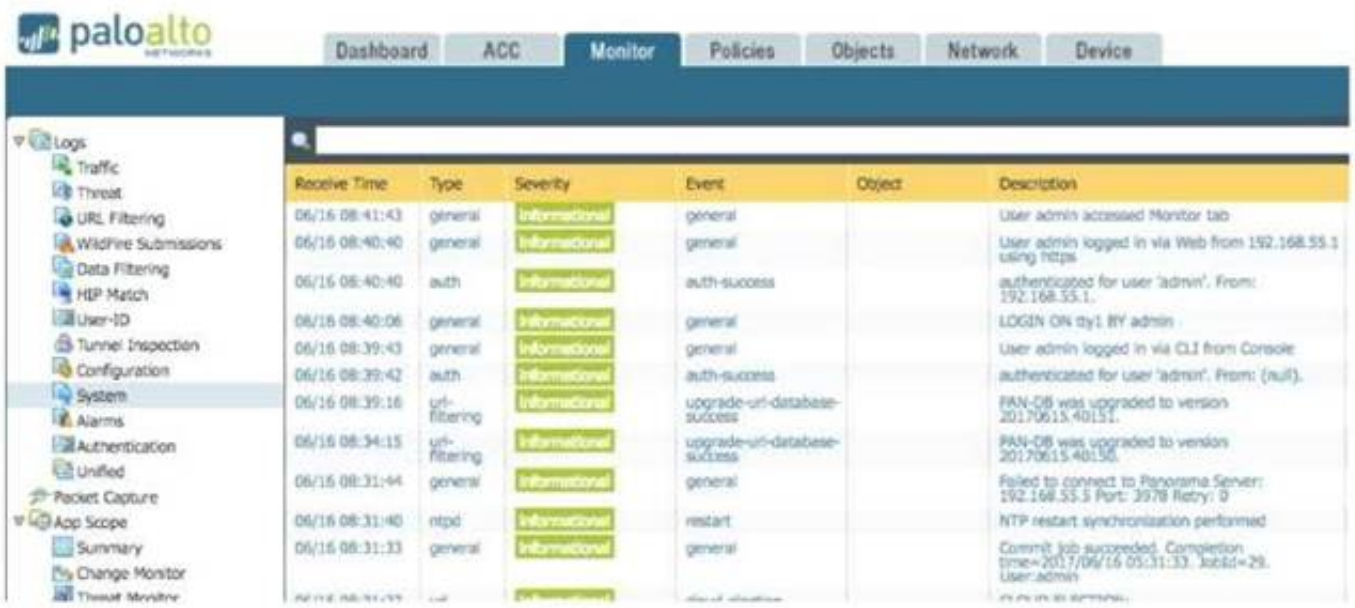
A. ACC

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

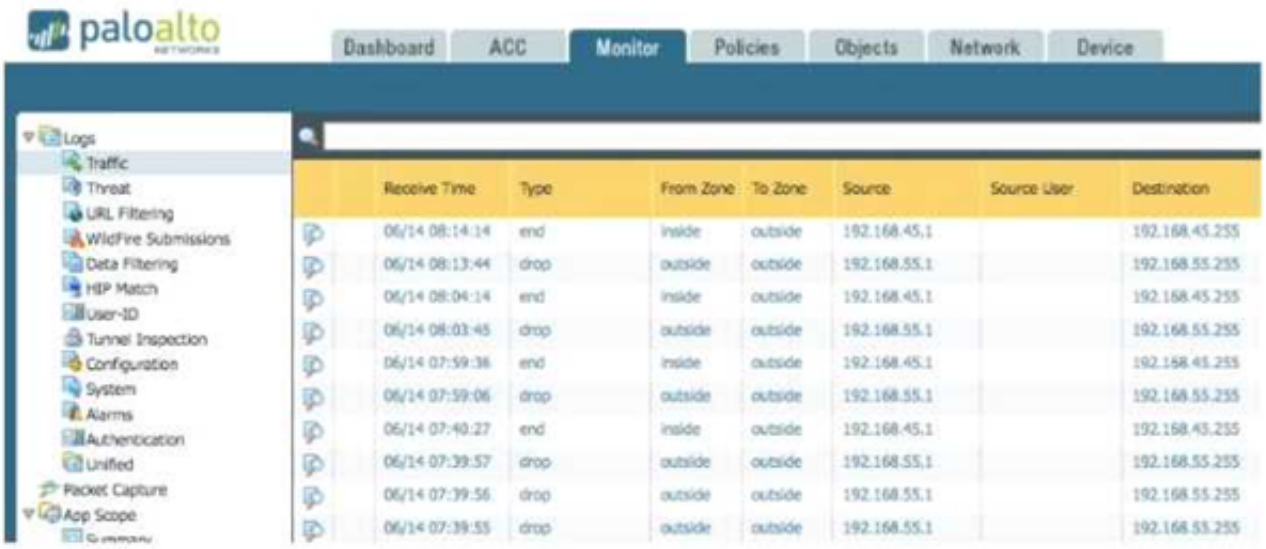
Answer: D

NEW QUESTION 34
- (Exam Topic 2)
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

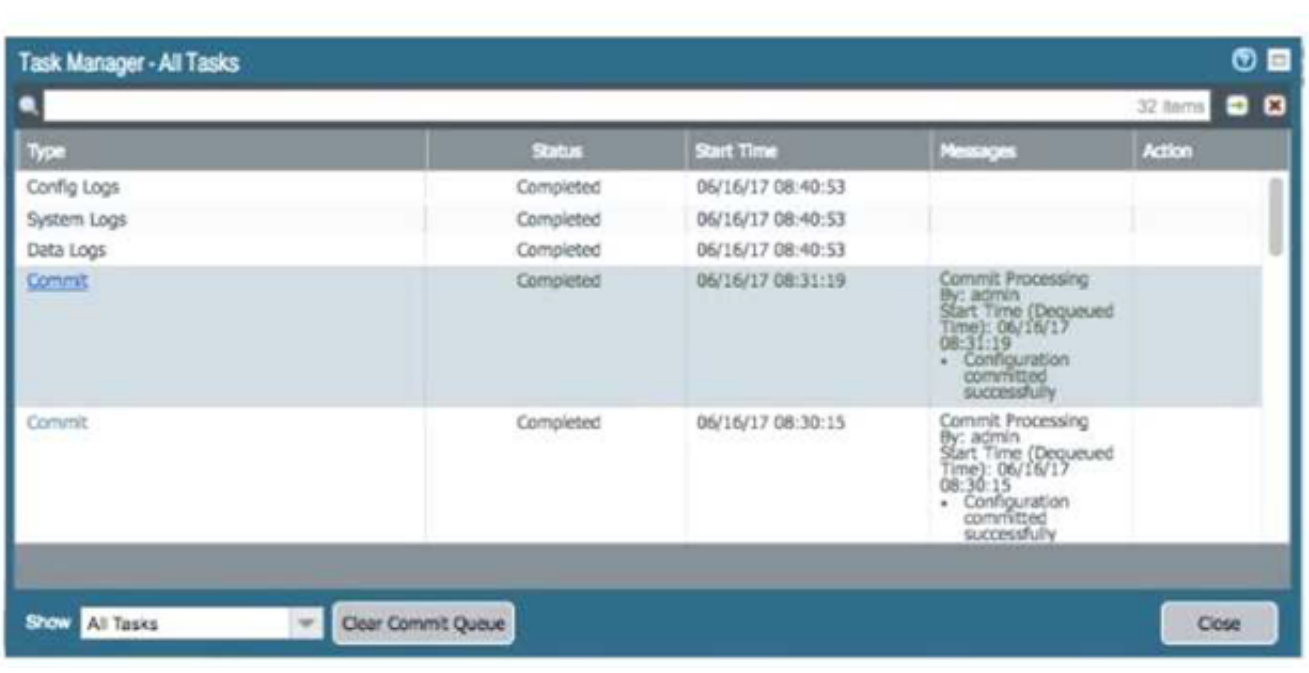


B



C

D



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

Answer: AD

NEW QUESTION 35
- (Exam Topic 2)
A bootstrap USB flash drive has been prepared using a Windows workstation to load the initial configuration of a Palo Alto Networks firewall that was previously being used in a lab. The USB flash drive was formatted using file system FAT32 and the initial configuration is stored in a file named init-cfg txt. The firewall is currently running PAN-OS 10.0 and using a lab config The contents of init-cfg txi in the USB flash drive are as follows:

```
type=dhcp-client
ip-address=
default-gateway=
netmask=
ipv6-address=
ipv6-default-gateway=
hostname=Ca-FW-DC1
panorama-server=10.5.107.20
panorama-server-2=10.5.107.21
tplname=FINANCE_TG4
dgname=finance_dg
dns-primary=10.5.6.6
dns-secondary=10.5.6.7
op-command-modes=multi-vsys,jumbo-frame
dhcp-send-hostname=yes
dhcp-send-client-id=yes
dhcp-accept-server-hostname=yes
dhcp-accept-server-domain=yes
```

The USB flash drive has been inserted in the firewalls' USB port, and the firewall has been restarted using command:> request resort system Upon restart, the firewall fails to begin the bootstrapping process The failure is caused because

A. Firewall must be m factory default state or have all private data deleted for bootstrapping
B. The hostname is a required parameter, but it is missing in imt-cfg txt
C. The USB must be formatted using the ext3 file system, FAT32 is not supported
D. PANOS version must be 91.x at a minimum but the firewall is running 10.0.x
E. The bootstrap.xml file is a required file but it is missing

Answer: C

NEW QUESTION 40
- (Exam Topic 2)
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: DE

Explanation:
Reference:
https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/getting-started/enable-autofocus-threat-inte

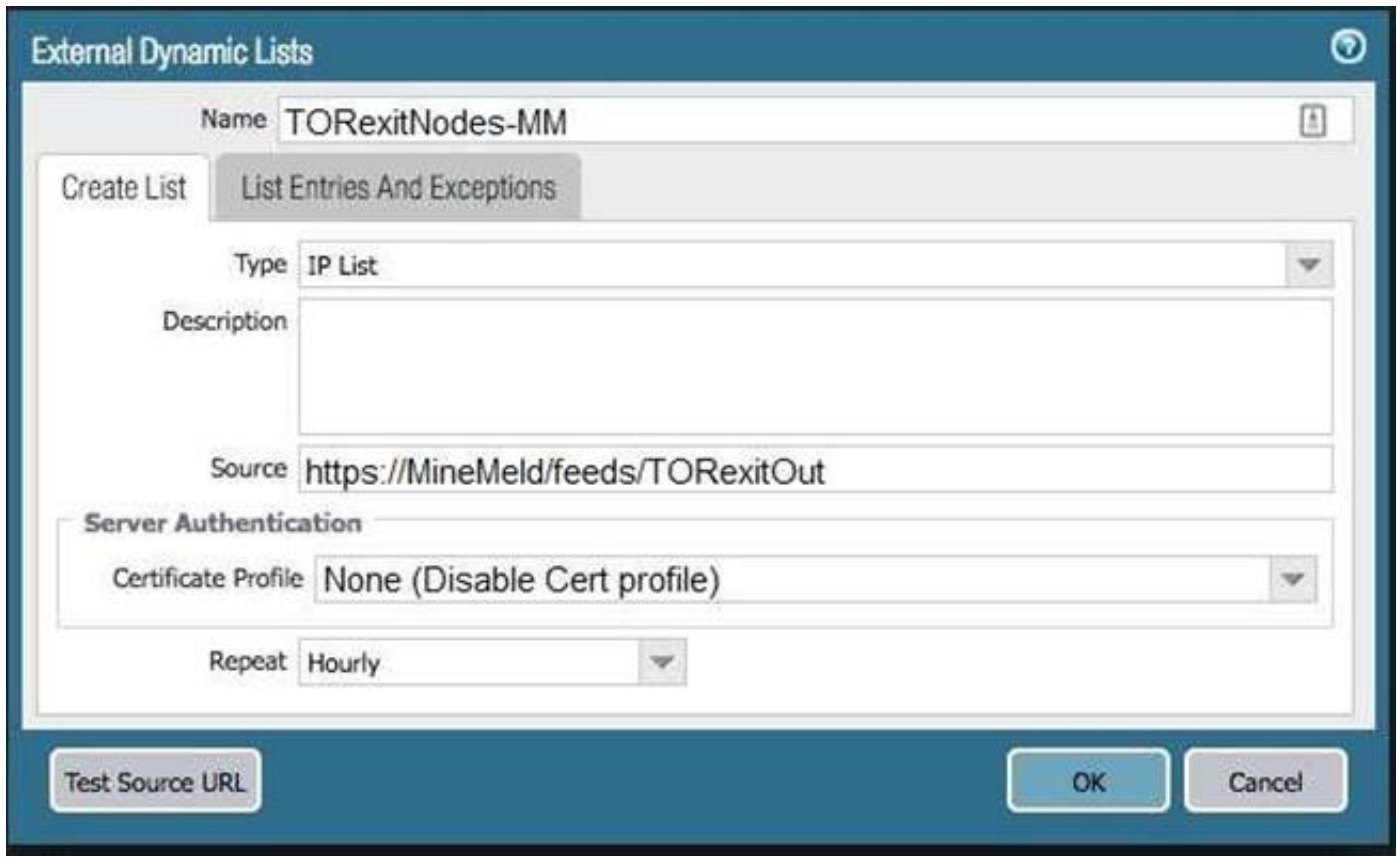
NEW QUESTION 41
- (Exam Topic 2)
An administrator has been asked to configure a Palo Alto Networks NGFW to provide protection against worms and trojans. Which Security Profile type will protect against worms and trojans?

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

Answer: D

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

NEW QUESTION 42
- (Exam Topic 2)
The firewall is not downloading IP addresses from MineMeld. Based, on the image, what most likely is wrong?



A. A Certificate Profile that contains the client certificate needs to be selected.
B. The source address supports only files hosted with an ftp://<address/file>.
C. External Dynamic Lists do not support SSL connections.
D. A Certificate Profile that contains the CA certificate needs to be selected.

Answer: D

NEW QUESTION 47
- (Exam Topic 2)
An administrator creates a custom application containing Layer 7 signatures. The latest application and threat dynamic update is downloaded to the same NGFW. The update contains an application that matches the same traffic signatures as the custom application. Which application should be used to identify traffic traversing the NGFW?

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

Answer: C

NEW QUESTION 49
- (Exam Topic 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 50
- (Exam Topic 2)
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

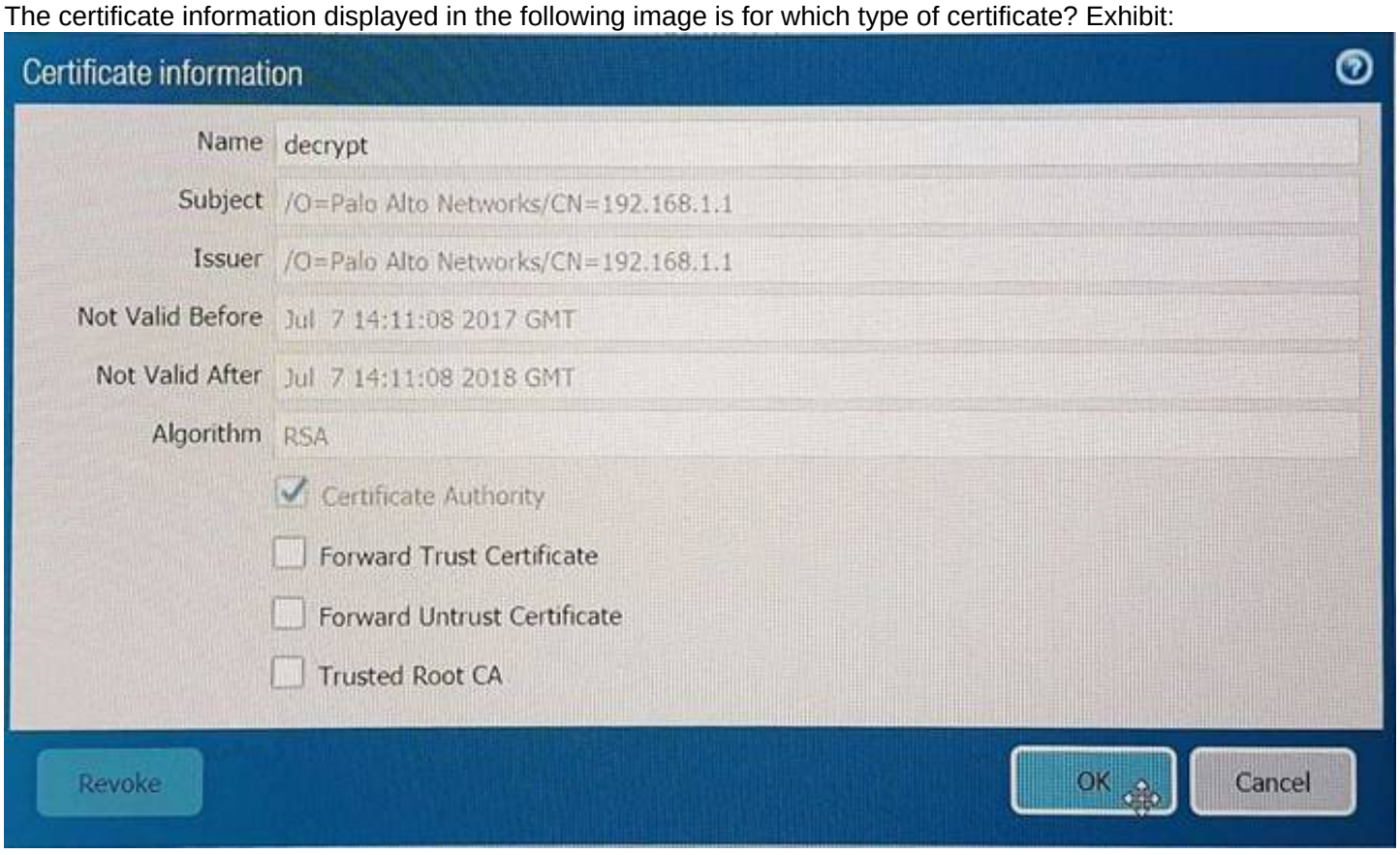
Explanation:
Reference:
https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/monitoring/take-packet-captures/disable-ha offload

NEW QUESTION 54
- (Exam Topic 2)
What is the purpose of the firewall decryption broker?

A. Decrypt SSL traffic a then send it as cleartext to a security chain of inspection tools
B. Force decryption of previously unknown cipher suites
C. Inspection traffic within IPsec tunnel
D. Reduce SSL traffic to a weaker cipher before sending it to a security chain of inspection tools

Answer: A

NEW QUESTION 57
- (Exam Topic 2)
The certificate information displayed in the following image is for which type of certificate? Exhibit:



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

Answer: B

NEW QUESTION 61
- (Exam Topic 2)
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: BDE

Explanation:
https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/firewall-administration/manage-firewall-administra

NEW QUESTION 62
- (Exam Topic 2)
Which CLI command can be used to export the tcpdump capture?

A. scp export tcpdump from mgmt.pcap to <username@host:path>
B. scp extract mgmt-pcap from mgmt.pcap to <username@host:path>
C. scp export mgmt-pcap from mgmt.pcap to <username@host:path>
D. download mgmt.-pcap

Answer: C

Explanation:
Reference:
https://live.paloaltonetworks.com/t5/Management-Articles/How-To-Packet-Capture-tcpdump-On-Management- p/55415

NEW QUESTION 66
- (Exam Topic 2)
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: D

Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClSvCAK
Decrypting SSL Sessions is a dataplane task.DoS Protection is a Dataplane task.Wildfire submissions is a Dataplane task.Generating a SaaS Application report is a Management Plane function.

NEW QUESTION 71
- (Exam Topic 2)
A customer wants to set up a VLAN interface for a Layer 2 Ethernet port.
Which two mandatory options are used to configure a VLAN interface? (Choose two.)

A. Virtual router
B. Security zone
C. ARP entries
D. Netflow Profile

Answer: AB

Explanation:
Reference:
https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/network/network-interfaces/pa
layer-2-interface#idd2bcaacc-54b9-4ec9-a1dd-8064499f5b9d
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClRqCAK
VLAN interface is not necessary but in this scenarion we assume it is. Create VLAN object, VLAN interface and VLAN Zone. Attach VLAN interface to VLAN object together with two L2 interfaces then attach VLAN interface to virtual router. Without VLAN interface you can pass traffic between interfaces on the same network and with VLAN interface you can route traffic to other networks.

NEW QUESTION 74
- (Exam Topic 2)
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

Explanation:
https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/zone-protection-and-dos-protection/zone-defense/z
https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/networking/nat/nat-configuration-examples/destinat

NEW QUESTION 77
- (Exam Topic 2)
An administrator has configured the Palo Alto Networks NGFW’s management interface to connect to the internet through a dedicated path that does not traverse back through the NGFW itself.
Which configuration setting or step will allow the firewall to get automatic application signature updates?

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

Answer: A

Explanation:
Reference:
https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/device/device-dynamic-update

NEW QUESTION 81
- (Exam Topic 2)
Which feature must you configure to prevent users form accidentally submitting their corporate credentials to a phishing website?

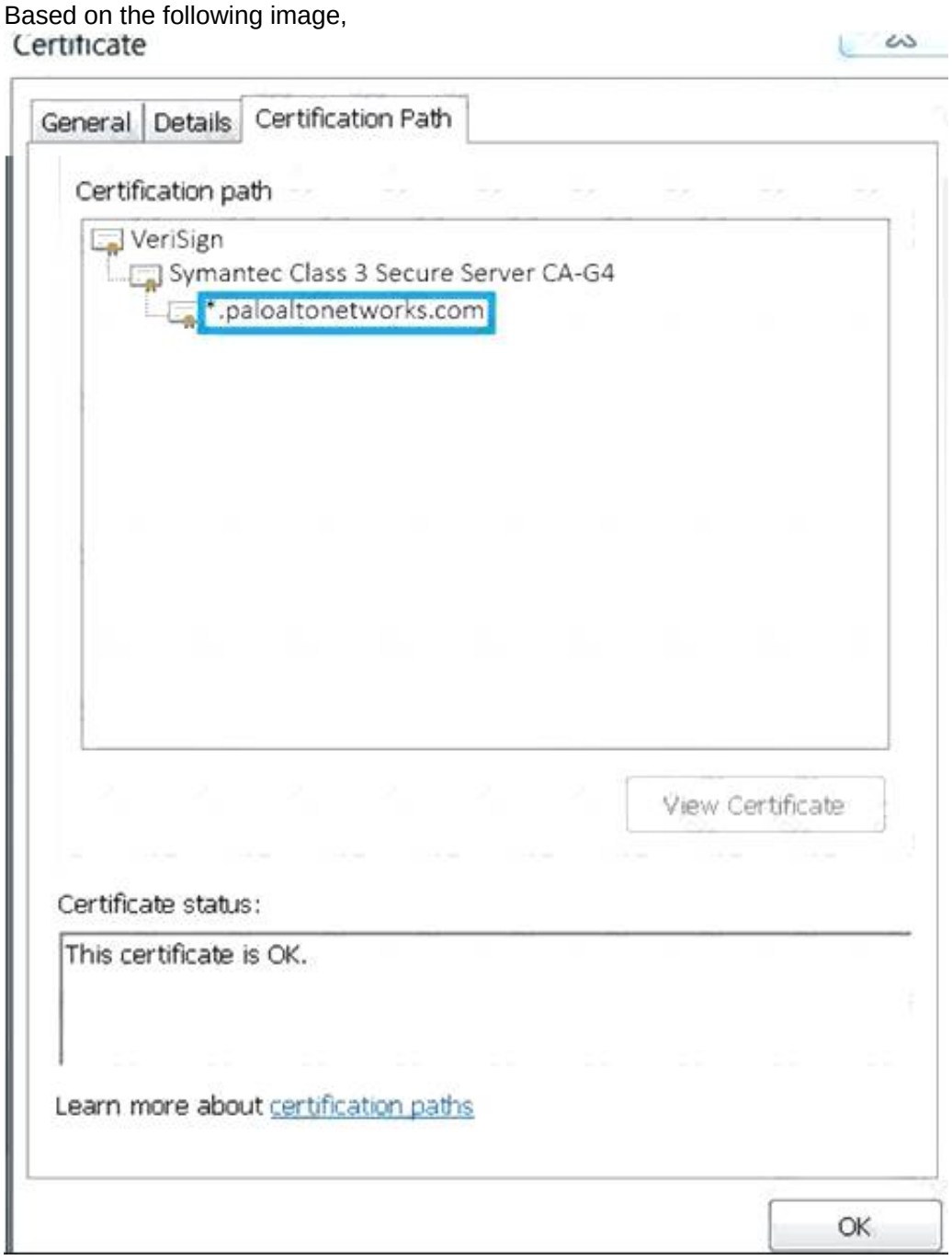
A. URL Filtering profile
B. Zone Protection profile
C. Anti-Spyware profile
D. Vulnerability Protection profile

Answer: A

Explanation:
Reference:

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

NEW QUESTION 82
- (Exam Topic 2)
Based on the following image,



what is the correct path of root, intermediate, and end-user certificate?

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

Answer: B

NEW QUESTION 86
- (Exam Topic 2)
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.

Answer: A

Explanation:
https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-new-features/content-inspection-features/credential-phishi
Reference:
https://www.paloaltonetworks.com/documentation/80/pan-os/newfeaturesguide/content-inspection-features/cred phishing-prevention

NEW QUESTION 87
- (Exam Topic 2)
VPN traffic intended for an administrator’s Palo Alto Networks NGFW is being maliciously intercepted and retransmitted by the interceptor. When creating a VPN tunnel, which protection profile can be enabled to prevent this malicious behavior?

A. Zone Protection
B. DoS Protection
C. Web Application
D. Replay

Answer: D

Explanation:
https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/vpns/set-up-site-to-site-vpn/set-up-an-ipsec

NEW QUESTION 88
- (Exam Topic 2)
Which administrative authentication method supports authorization by an external service?

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

Answer: C

NEW QUESTION 92
- (Exam Topic 2)
Which GlobalProtect Client connect method requires the distribution and use of machine certificates?

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

Answer: D

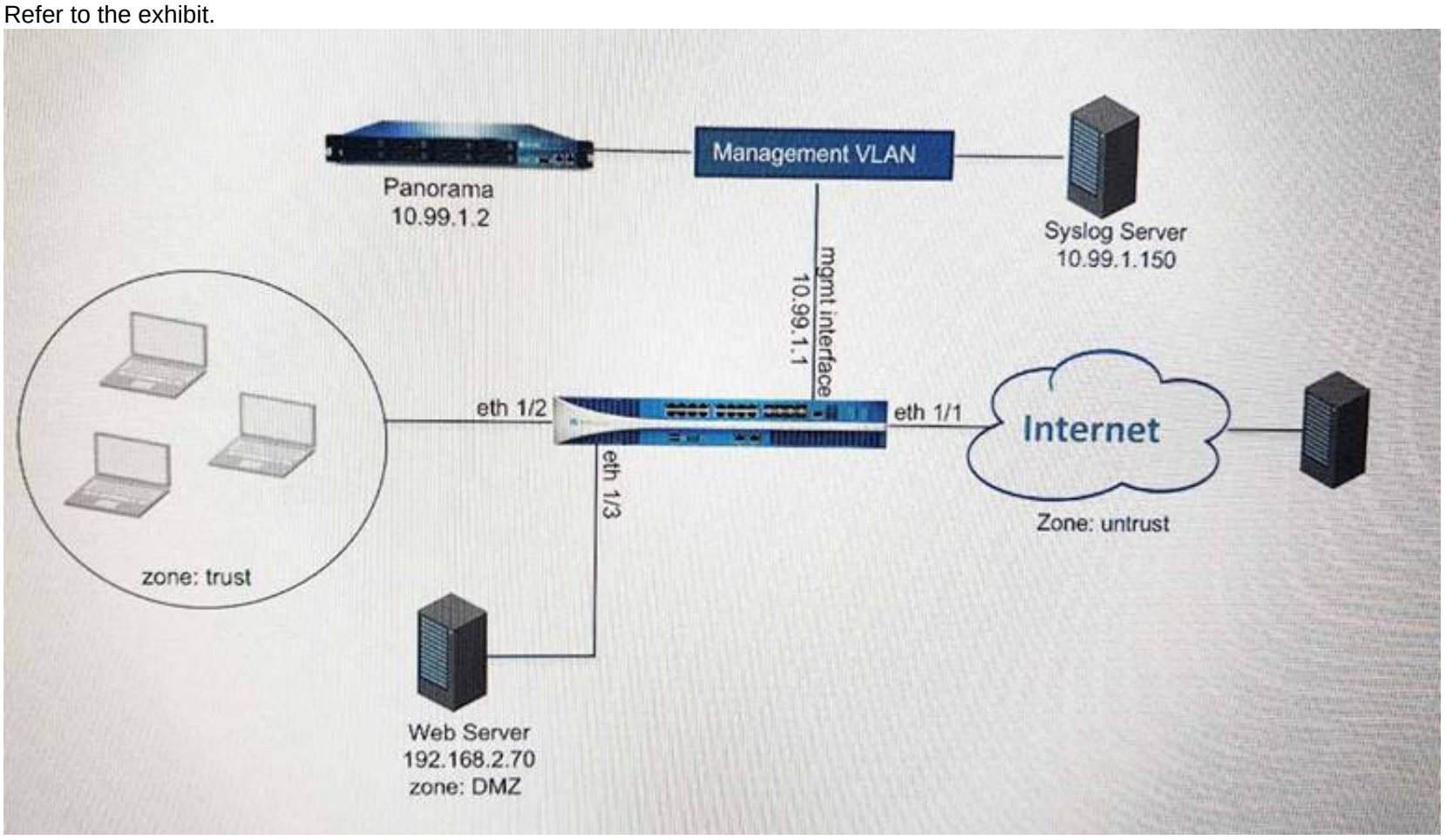
NEW QUESTION 93
- (Exam Topic 2)
When configuring a GlobalProtect Portal, what is the purpose of specifying an Authentication Profile?

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

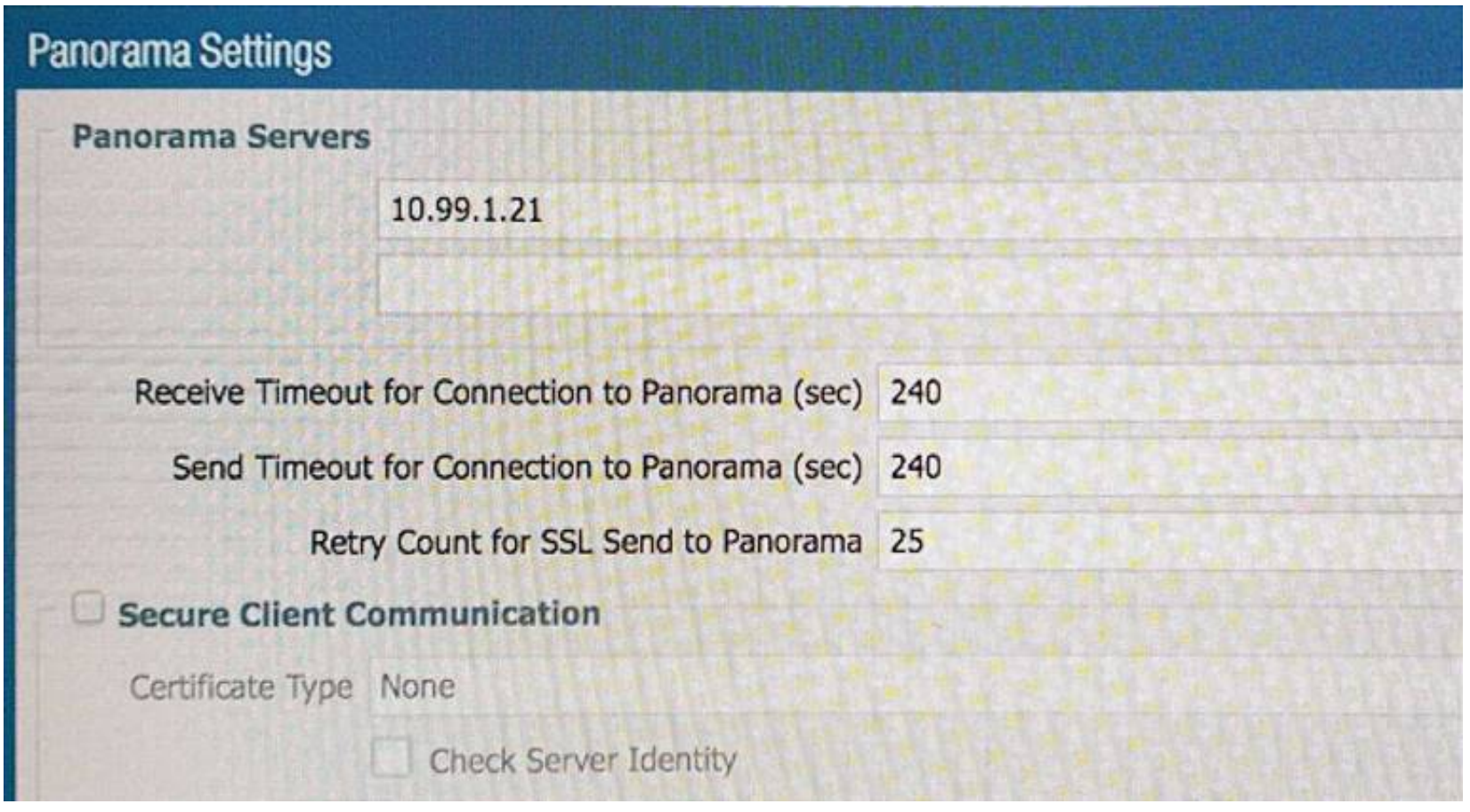
Answer: C

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-globalpr

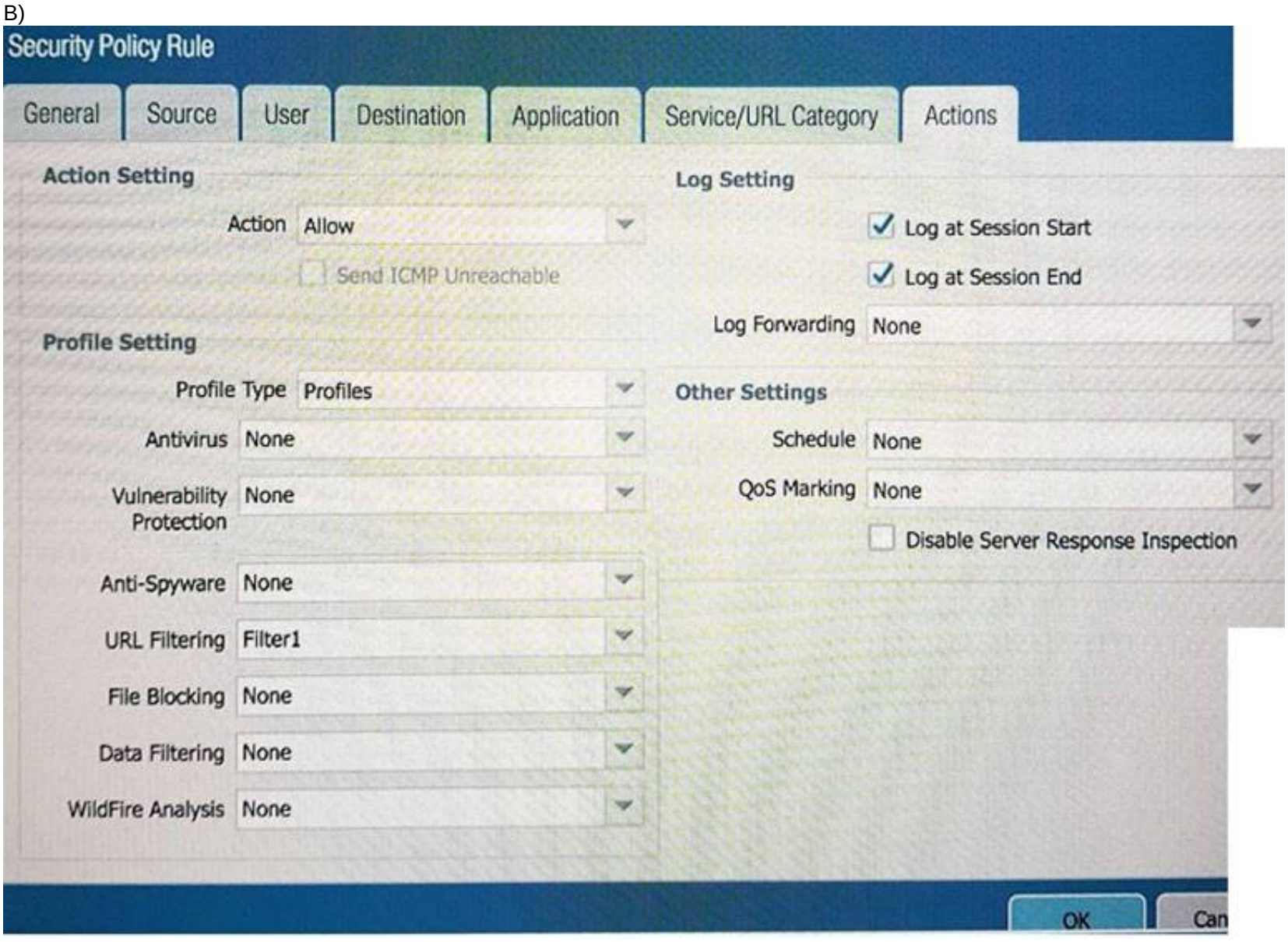
NEW QUESTION 98
- (Exam Topic 2)
Refer to the exhibit.



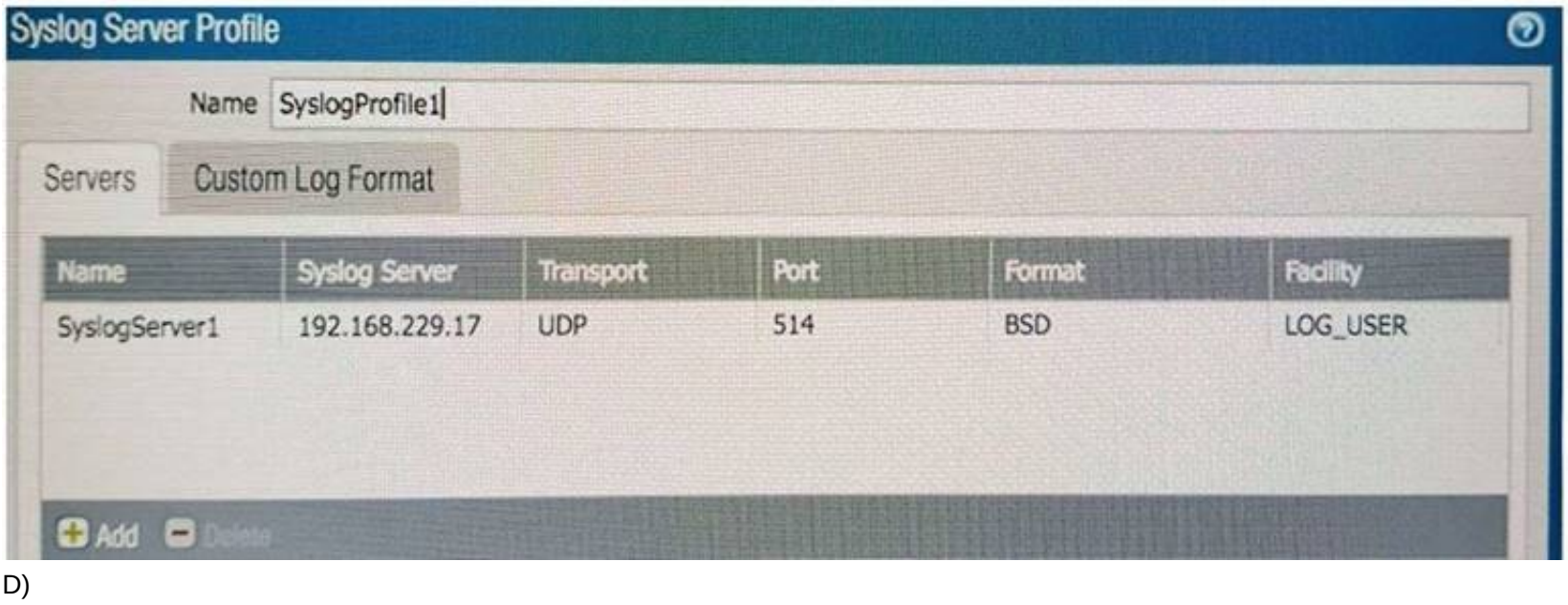
An administrator cannot see any of the Traffic logs from the Palo Alto Networks NGFW on Panorama. The configuration problem seems to be on the firewall side. Where is the best place on the Palo Alto Networks NGFW to check whether the configuration is correct?
A)


Panorama Settings
Panorama Servers
10.99.1.21
Receive Timeout for Connection to Panorama (sec) 240
Send Timeout for Connection to Panorama (sec) 240
Retry Count for SSL Send to Panorama 25
Secure Client Communication
Certificate Type None
Check Server Identity

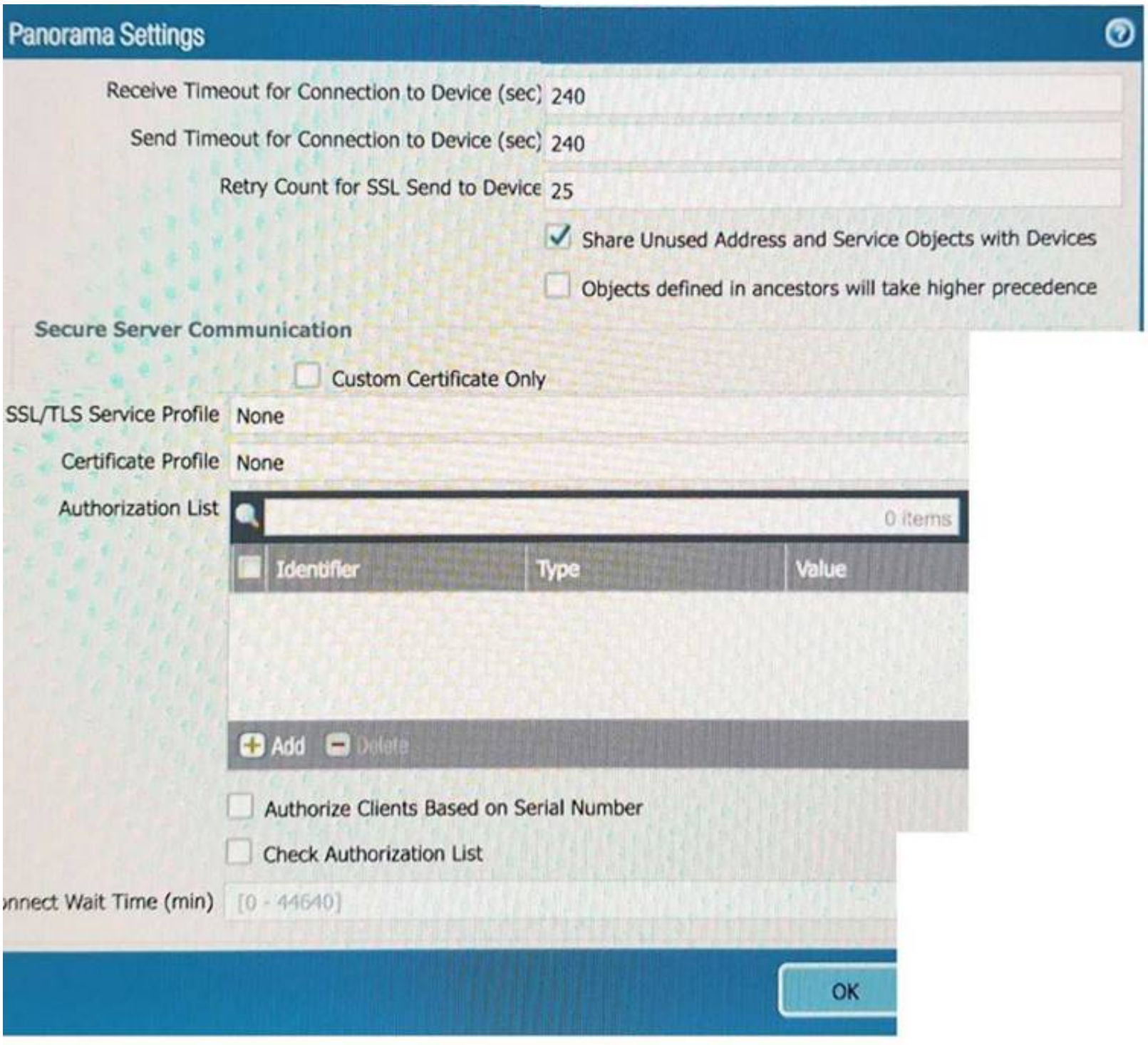
B)


Security Policy Rule
General
Source
User
Destination
Application
Service/URL Category
Actions
Action Setting
Action Allow
Send ICMP Unreachable
Profile Setting
Profile Type Profiles
Antivirus None
Vulnerability Protection None
Anti-Spyware None
URL Filtering Filter1
File Blocking None
Data Filtering None
WildFire Analysis None
Log Setting
Log at Session Start
Log at Session End
Log Forwarding None
Other Settings
Schedule None
QoS Marking None
Disable Server Response Inspection
OK
Can

C)


Syslog Server Profile
Name SyslogProfile1
Servers
Custom Log Format
Name
Syslog Server
Transport
Port
Format
Facility
SyslogServer1
192.168.229.17
UDP
514
BSD
LOG_USER
Add
Delete

D)



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

Answer: A

Explanation:
https://docs.paloaltonetworks.com/panorama/9-0/panorama-admin/manage-log-collection/configure-log-forward

NEW QUESTION 103
- (Exam Topic 2)
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: ABC

NEW QUESTION 106
- (Exam Topic 2)
An administrator sees several inbound sessions identified as unknown-tcp in the Traffic logs. The administrator determines that these sessions are form external users accessing the company's proprietary accounting application. The administrator wants to reliably identify this traffic as their accounting application and to scan this traffic for threats.
Which option would achieve this result?

A. Create a custom App-ID and enable scanning on the advanced tab.
B. Create an Application Override policy.
C. Create a custom App-ID and use the "ordered conditions" check box.
D. Create an Application Override policy and custom threat signature for the application.

Answer: A

Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClRoCAK

NEW QUESTION 110
- (Exam Topic 2)
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 115
- (Exam Topic 2)
A customer has an application that is being identified as unknown-top for one of their custom PostgreSQL database connections. Which two configuration options can be used to correctly categorize their custom database application? (Choose two.)

A. Application Override policy.
B. Security policy to identify the custom application.
C. Custom application.
D. Custom Service object.

Answer: AC

Explanation:
Unlike the App-ID engine, which inspects application packet contents for unique signature elements, the Application Override policy's matching conditions are limited to header-based data only. Traffic matched by an Application Override policy is identified by the App-ID entered in the Application entry box.Choices are limited to applications currently in the App-ID database.Because this traffic bypasses all Layer 7 inspection, the resulting security is that of a Layer-4 firewall. Thus, this traffic should be trusted without the need for Content-ID inspection. The resulting application assignment can be used in other firewall functions such as Security policy and QoS.Use CasesThree primary uses cases for Application Override Policy are:
To identify "Unknown" App-IDs with a different or custom application signature To re-identify an existing application signature
To bypass the Signature Match Engine (within the SP3 architecture) to improve processing timesA discussion of typical uses of application override and specific implementation examples is here:https://live.paloaltonetworks.com/t5/Learning-Articles/Tips-amp-Tricks-How-to-Create-an-Application

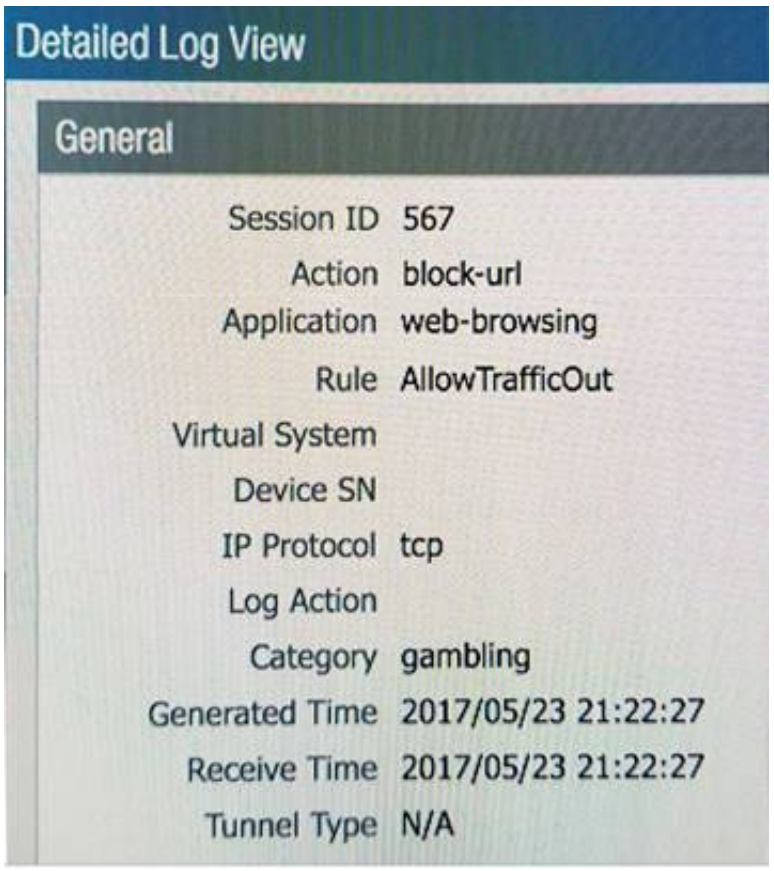
NEW QUESTION 117
- (Exam Topic 2)
Which Captive Portal mode must be configured to support MFA authentication?

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

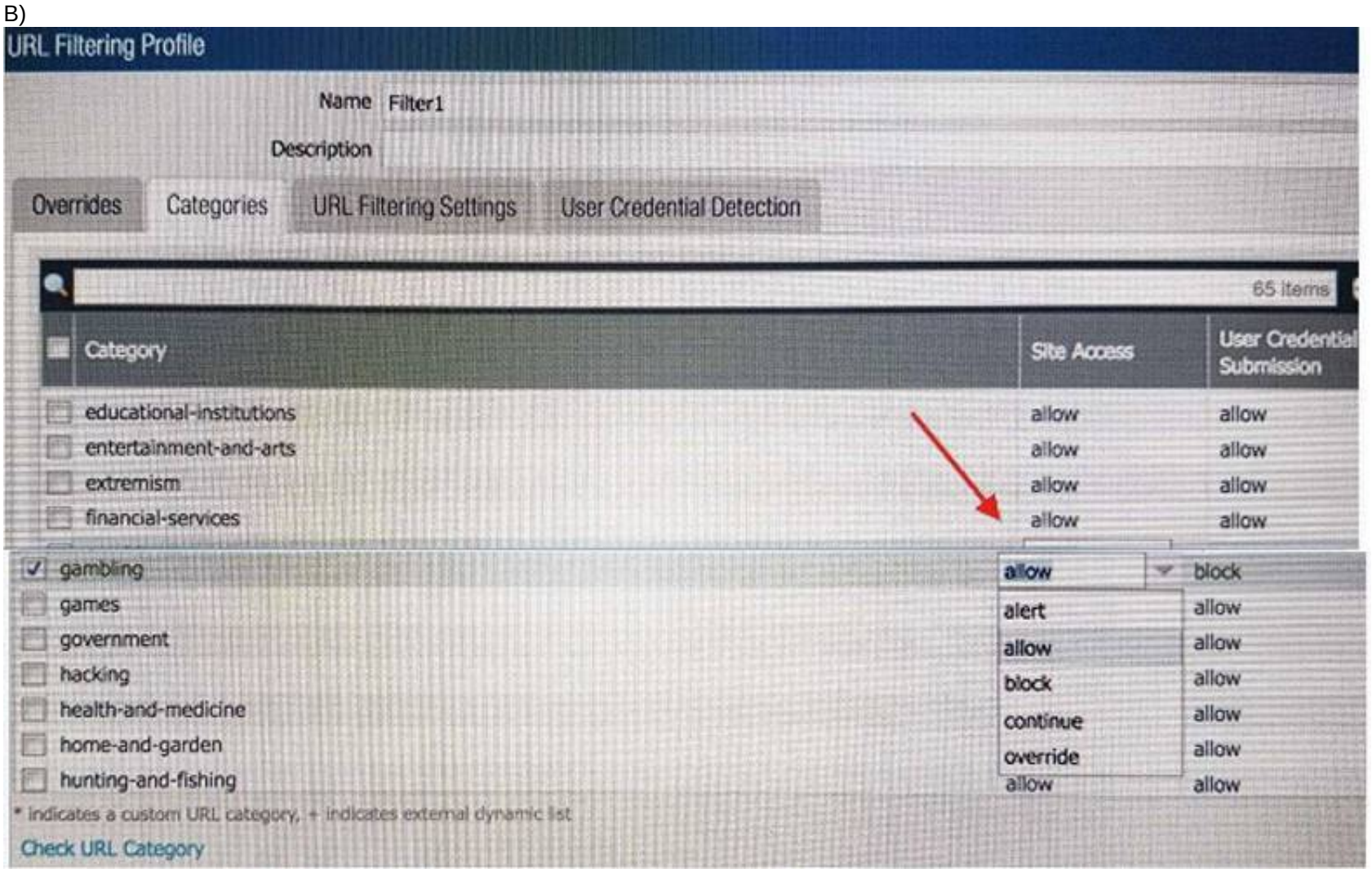
Answer: B

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

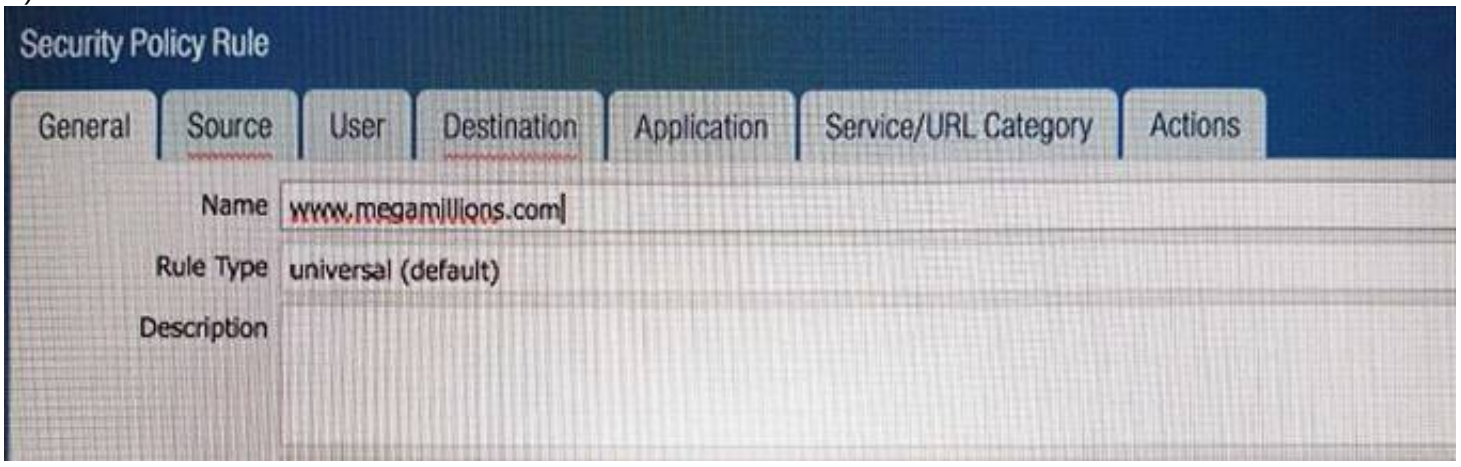
NEW QUESTION 120
- (Exam Topic 2)
An administrator needs to determine why users on the trust zone cannot reach certain websites. The only information available is shown on the following image.
Which configuration change should the administrator make?
A)


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

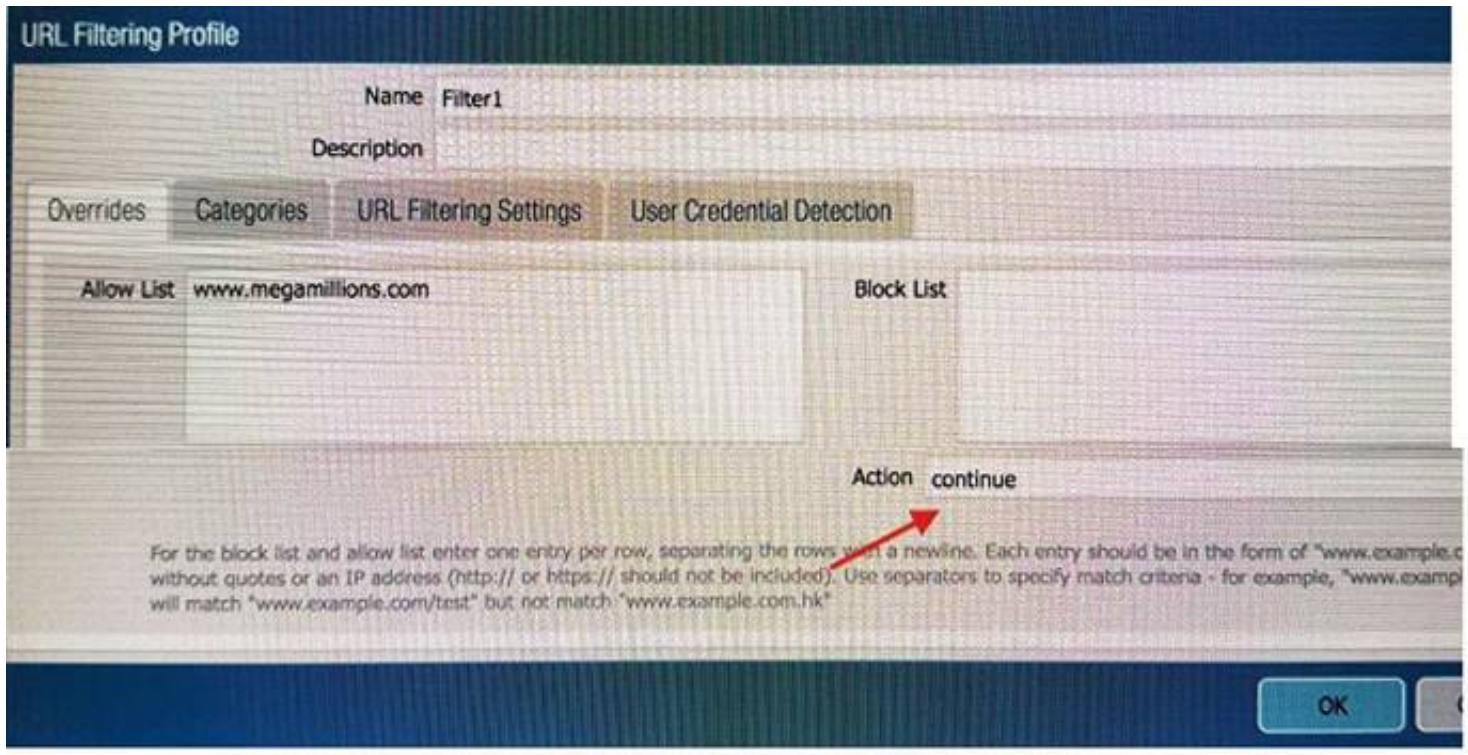
B)


URL Filtering Profile
Name Filter1
Description
Overrides
Categories
URL Filtering Settings
User Credential Detection
65 items
Category
Site Access
User Credential Submission
educational-institutions
entertainment-and-arts
extremism
financial-services
gambling
games
government
hacking
health-and-medicine
home-and-garden
hunting-and-fishing
allow
block
alert
allow
block
continue
override
* indicates a custom URL category, + indicates external dynamic list
Check URL Category

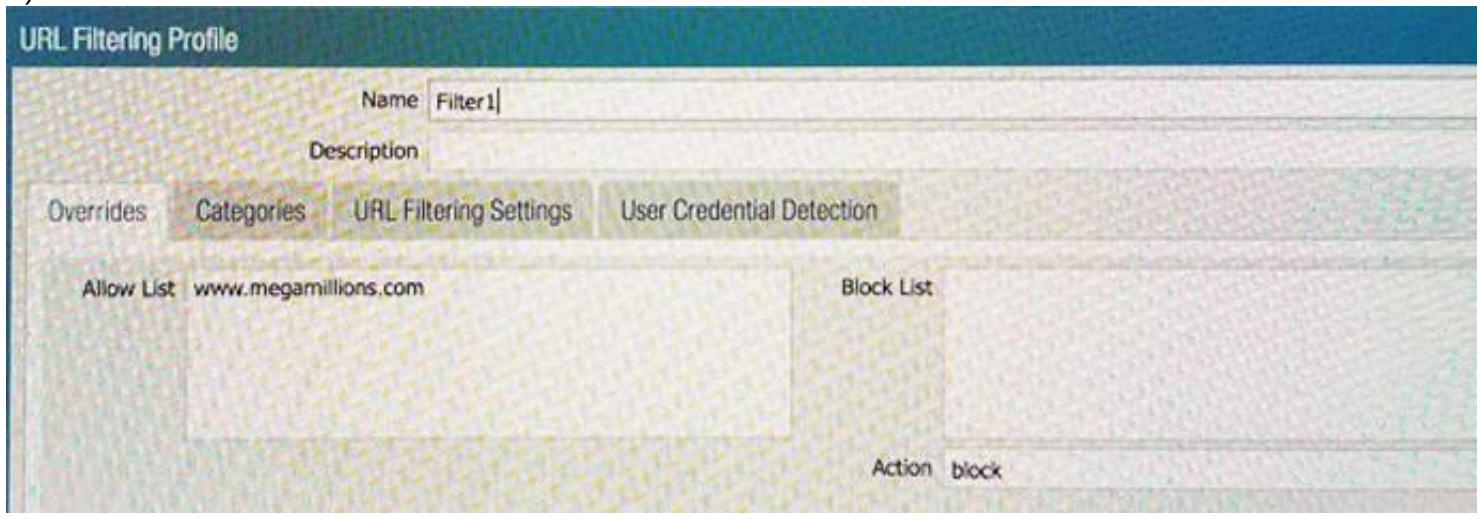
C)


Security Policy Rule
General
Source
User
Destination
Application
Service/URL Category
Actions
Name www.megamillions.com
Rule Type universal (default)
Description

D)



E)



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

Answer: B

NEW QUESTION 122
- (Exam Topic 2)
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

Explanation:
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface-help/network/network-qos/qos-interface-set

NEW QUESTION 127
- (Exam Topic 2)
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: ACD

Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CleLCAS

NEW QUESTION 132

- (Exam Topic 2)
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 133
- (Exam Topic 2)
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: A

NEW QUESTION 138
- (Exam Topic 2)
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 140
- (Exam Topic 2)
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. Wildfire update package
B. User-ID agent
C. Anti virus update package
D. Application and Threats update package

Answer: D

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.
: https://live.paloaltonetworks.com/t5/Featured-Articles/Best-Practices-for-PAN-OS-Upgrade/ta-p/111045

NEW QUESTION 143
- (Exam Topic 2)
Which three firewall states are valid? (Choose three)

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

Answer: ADE

Explanation:

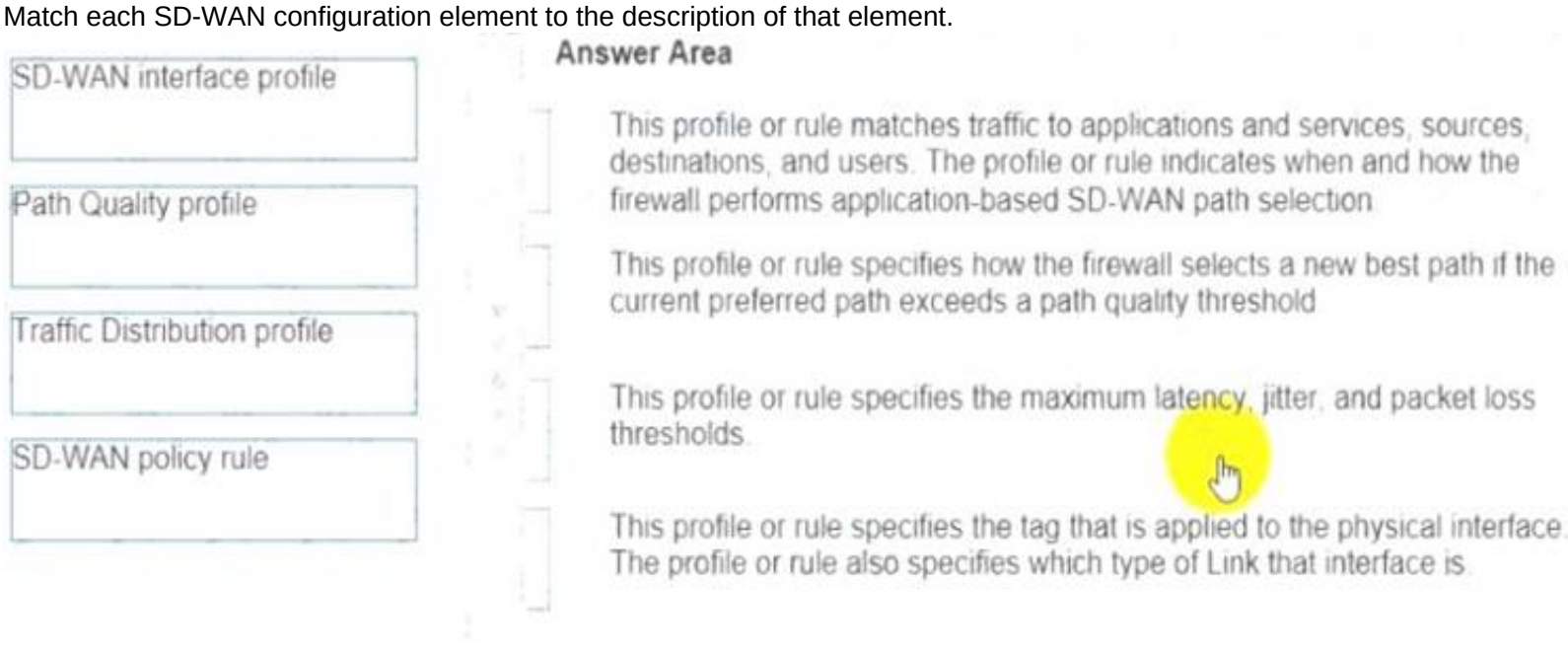
Reference:
https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/high-availability/ha-firewall-states

NEW QUESTION 144
- (Exam Topic 1)
An administrator wants to enable zone protection Before doing so, what must the administrator consider?

A. Activate a zone protection subscription.
B. To increase bandwidth no more than one firewall interface should be connected to a zone
C. Security policy rules do not prevent lateral movement of traffic between zones
D. The zone protection profile will apply to all interfaces within that zone

Answer: A

NEW QUESTION 146
- (Exam Topic 1)
Match each SD-WAN configuration element to the description of that element.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
An SD-WAN Interface Profile
specifies the Tag that you apply to the physical interface, and also specifies the type of Link that interface is (ADSL/DSL, cable modem, Ethernet, fiber, LTE/3G/4G/5G, MPLS, microwave/radio, satellite, WiFi, or other). The Interface Profile is also where you specify the maximum upload and download speeds (in Mbps) of the ISP's connection. You can also change whether the firewall monitors the path frequently or not; the firewall monitors link types appropriately by default.
A Layer3 Ethernet
Interface
with an IPv4 address can support SD-WAN functionalities. You apply an SD-WAN Interface Profile to this
interface (red arrow) to indicate the characteristics of the interface. The blue arrow indicates that physical Interfaces are referenced and grouped in a virtual SD-WAN Interface.
A virtual SD-WAN Interface
is a VPN tunnel or DIA group of one or more interfaces that constitute a numbered, virtual SD-WAN Interface to which you can route traffic. The paths belonging to an SD-WAN Interface all go to the same destination WAN and are all the same type (either DIA or VPN tunnel). (Tag A and Tag B indicate that physical interfaces for the virtual interface can have different tags.)
A Path Quality Profile
specifies maximum latency, jitter, and packet loss thresholds. Exceeding a threshold indicates that the path has deteriorated and the firewall needs to select a new path to the target. A sensitivity setting of high, medium, or low lets you indicate to the firewall which path monitoring parameter is more important for the applications to which the profile applies. The green arrow indicates that you reference a Path Quality Profile in one or more SD-WAN Policy Rules; thus, you can specify different thresholds for rules applied to packets having different applications, services, sources, destinations, zones, and users.
A Traffic Distribution Profile
specifies how the firewall determines a new best path if the current preferred path exceeds a path quality threshold. You specify which Tags the distribution method uses to narrow its selection of a new path; hence, the yellow arrow points from Tags to the Traffic Distribution profile. A Traffic Distribution profile specifies the distribution method for the rule.
The preceding elements come together in
SD-WAN Policy Rules
The purple arrow indicates that you reference a Path Qualify Profile and a Traffic Distribution profile in a rule, along with packet applications/services, sources, destinations, and users to specifically indicate when and how the firewall performs application-based SD-WAN path selection for a packet not belonging to a session.
https://docs.paloaltonetworks.com/sd-wan/1-0/sd-wan-admin/sd-wan-overview/sd-wan-configuration-elements.h

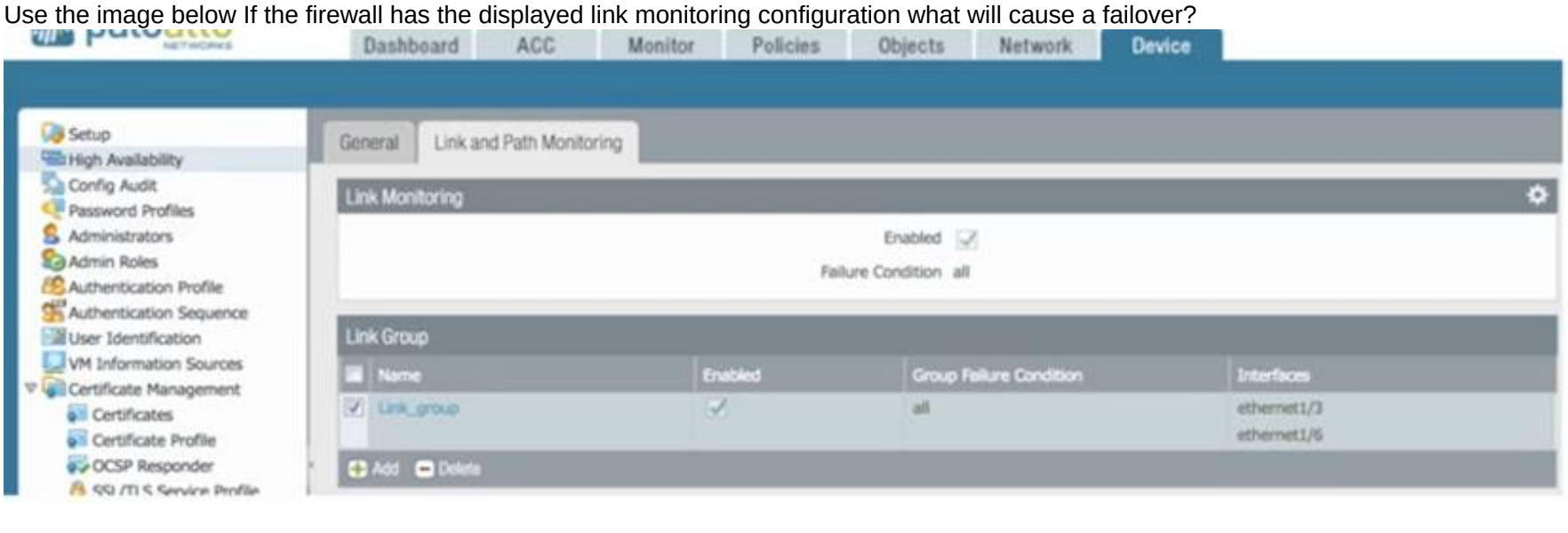
NEW QUESTION 147
- (Exam Topic 1)
In SSL Forward Proxy decryption, which two certificates can be used for certificate signing? (Choose two.)

A. wildcard server certificate

B. enterprise CA certificate
C. client certificate
D. server certificate
E. self-signed CA certificate

Answer: BE

NEW QUESTION 149
- (Exam Topic 1)
Use the image below If the firewall has the displayed link monitoring configuration what will cause a failover?



A. ethernet1/3 and ethernet1/6 going down
B. etheme!1/3 going down
C. ethernet1/6 going down
D. ethernet1/3 or ethernet1/6 going down

Answer: A

NEW QUESTION 150
- (Exam Topic 1)
PBF can address which two scenarios? (Select Two)

A. forwarding all traffic by using source port 78249 to a specific egress interface
B. providing application connectivity the primary circuit fails
C. enabling the firewall to bypass Layer 7 inspection
D. routing FTP to a backup ISP link to save bandwidth on the primary ISP link

Answer: AC

NEW QUESTION 151
- (Exam Topic 1)
An engineer must configure a new SSL decryption deployment
Which profile or certificate is required before any traffic that matches an SSL decryption rule is decrypted?

A. There must be a certificate with both the Forward Trust option and Forward Untrust option selected
B. A Decryption profile must be attached to the Decryption policy that the traffic matches
C. A Decryption profile must be attached to the Security policy that the traffic matches
D. There must be a certificate with only the Forward Trust option selected

Answer: A

NEW QUESTION 152
- (Exam Topic 1)
A firewall is configured with SSL Forward Proxy decryption and has the following four enterprise certificate authorities (Cas)

A. Enterprise-Trusted-CA; which is verified as Forward Trust Certificate (The CA is also installed in the trusted store of the end-user browser and system)i
B. Enterpnse-Untrusted-CA, which is verified as Forward Untrust Certificateii
C. Enterprise-Intermediate-CAi
D. Enterprise-Root-CA which is verified only as Trusted Root CAAn end-user visits https //www example-website com/ with a server certificate Common Name (CN) www example-website com The firewall does the SSL Forward Proxy decryption for the website and the server certificate is not trusted by the firewallThe end-user's browser will show that the certificate for www example-website com was issued by which of the following?
E. Enterprise-Untrusted-CA which is a self-signed CA
F. Enterprise-Trusted-CA which is a self-signed CA
G. Enterprise-Intermediate-CA which wa
H. in turn, issued by Enterprise-Root-CA
I. Enterprise-Root-CA which is a self-signed CA

Answer: B

NEW QUESTION 153
- (Exam Topic 1)

A traffic log might list an application as "not-applicable" for which two reasons'? (Choose two)

A. 0The firewall did not install the session
B. The TCP connection terminated without identifying any application data
C. The firewall dropped a TCP SYN packet
D. There was not enough application data after the TCP connection was established

Answer: AD

NEW QUESTION 154
- (Exam Topic 1)
An engineer must configure the Decryption Broker feature
Which Decryption Broker security chain supports bi-directional traffic flow?

A. Layer 2 security chain
B. Layer 3 security chain
C. Transparent Bridge security chain
D. Transparent Proxy security chain

Answer: B

Explanation:
Together, the primary and secondary interfaces form a pair of decryption forwarding interfaces. Only interfaces that you have enabled to be Decrypt Forward interfaces are displayed here. Your security chain type (Layer 3 or Transparent Bridge) and the traffic flow direction (unidirectional or bidirectional) determine which of the two interfaces forwards allowed, clear text traffic to the security chain, and which interface receives the traffic back from the security chain after it has undergone additional enforcement.

NEW QUESTION 157
- (Exam Topic 1)
Which two statements correctly identify the number of Decryption Broker security chains that are supported on a pair of decryption-forwarding interfaces'? (Choose two)

A. A single transparent bridge security chain is supported per pair of interfaces
B. L3 security chains support up to 32 security chains
C. L3 security chains support up to 64 security chains
D. A single transparent bridge security chain is supported per firewall

Answer: AD

NEW QUESTION 161
- (Exam Topic 1)
What are two common reasons to use a "No Decrypt" action to exclude traffic from SSL decryption? (Choose two.)

A. the website matches a category that is not allowed for most users
B. the website matches a high-risk category
C. the web server requires mutual authentication
D. the website matches a sensitive category

Answer: AD

NEW QUESTION 162
- (Exam Topic 1)
Which configuration task is best for reducing load on the management plane?

A. Disable logging on the default deny rule
B. Enable session logging at start
C. Disable pre-defined reports
D. Set the URL filtering action to send alerts

Answer: A

NEW QUESTION 163
- (Exam Topic 1)
As a best practice, which URL category should you target first for SSL decryption*?

A. Online Storage and Backup
B. High Risk
C. Health and Medicine
D. Financial Services

Answer: A

NEW QUESTION 167
- (Exam Topic 1)
A network administrator wants to use a certificate for the SSL/TLS Service Profile Which type of certificate should the administrator use?

A. certificate authority (CA) certificate

B. client certificate
C. machine certificate
D. server certificate

Answer: A

NEW QUESTION 171
- (Exam Topic 1)
An administrator has a PA-820 firewall with an active Threat Prevention subscription The administrator is considering adding a WildFire subscription
How does adding the WildFire subscription improve the security posture of the organization1?

A. Protection against unknown malware can be provided in near real-time
B. WildFire and Threat Prevention combine to provide the utmost security posture for the firewall
C. After 24 hours WildFire signatures are included in the antivirus update
D. WildFire and Threat Prevention combine to minimize the attack surface

Answer: D

NEW QUESTION 176
- (Exam Topic 1)
In a Panorama template which three types of objects are configurable? (Choose three)

A. HIP objects
B. QoS profiles
C. interface management profiles
D. certificate profiles
E. security profiles

Answer: ACE

NEW QUESTION 181
- (Exam Topic 2)
Which four NGFW multi-factor authentication factors are supported by PAN-OS? (Choose four.)

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

Answer: ABDF

Explanation:
https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/authentication/authentication-types/multi-factor-aut

NEW QUESTION 185
- (Exam Topic 2)
Which two features can be used to tag a username so that it is included in a dynamic user group? (Choose two)

A. log forwarding auto-tagging
B. GlobafProtect agent
C. User-ID Windows-based agent
D. XML API

Answer: BC

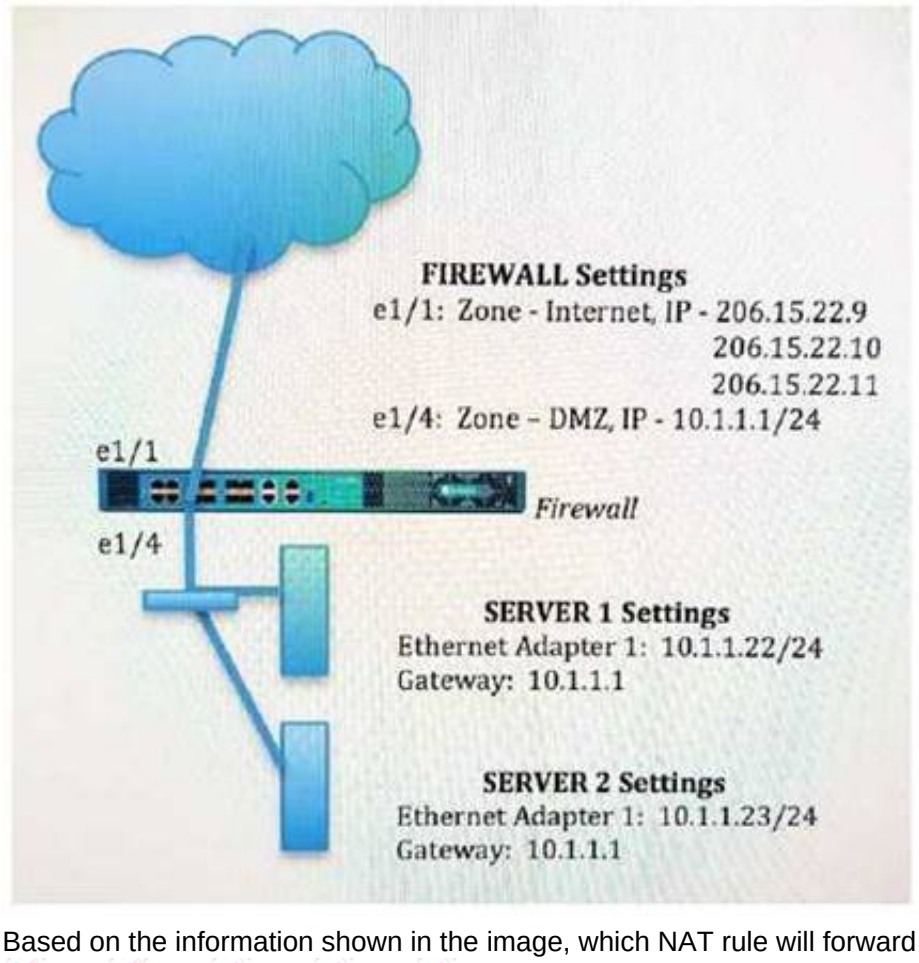
NEW QUESTION 188
- (Exam Topic 2)
Which two settings can be configured only locally on the firewall and not pushed from a Panorama template or template stack? (Choose two)

A. HA1 IP Address
B. Network Interface Type
C. Master Key
D. Zone Protection Profile

Answer: AC

Explanation:
https://docs.paloaltonetworks.com/panorama/7-1/panorama-admin/manage-firewalls/template-capabilities-and-e

NEW QUESTION 193
- (Exam Topic 2)
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



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: C

NEW QUESTION 197

- (Exam Topic 2)
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: DE

NEW QUESTION 198
- (Exam Topic 2)
An administrator needs to optimize traffic to prefer business-critical applications over non-critical applications. QoS natively integrates with which feature to provide service quality?

A. Port Inspection
B. Certificate revocation
C. Content-ID
D. App-ID

Answer: D

Explanation:
Reference:
https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/quality-of-service/qos-for-applications-and

NEW QUESTION 199
- (Exam Topic 2)
An administrator encountered problems with inbound decryption. Which option should the administrator investigate as part of triage?

A. Security policy rule allowing SSL to the target server
B. Firewall connectivity to a CRL
C. Root certificate imported into the firewall with “Trust” enabled
D. Importation of a certificate from an HSM

Answer: A

Explanation:
https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/decryption/configure-ssl-inbound-inspection.html

NEW QUESTION 201
- (Exam Topic 2)
To protect your firewall and network from single source denial of service (DoS) attacks that can overwhelm its packet buffer and cause legitimate traffic to drop, you can configure.

A. BGP (Border Gateway Protocol)
B. PBP (Packet Buffer Protection)
C. PGP (Packet Gateway Protocol)
D. PBP (Protocol Based Protection)

Answer: D

NEW QUESTION 202
- (Exam Topic 2)
Which option describes the operation of the automatic commit recovery feature?

A. It enables a firewall to revert to the previous configuration if rule shadowing is detected
B. It enables a firewall to revert to the previous configuration if a commit causes Panorama connectivity failure.
C. It enables a firewall to revert to the previous configuration if application dependency errors are found
D. It enables a firewall to revert to the previous configuration if a commit causes HA partner connectivity failure

Answer: A

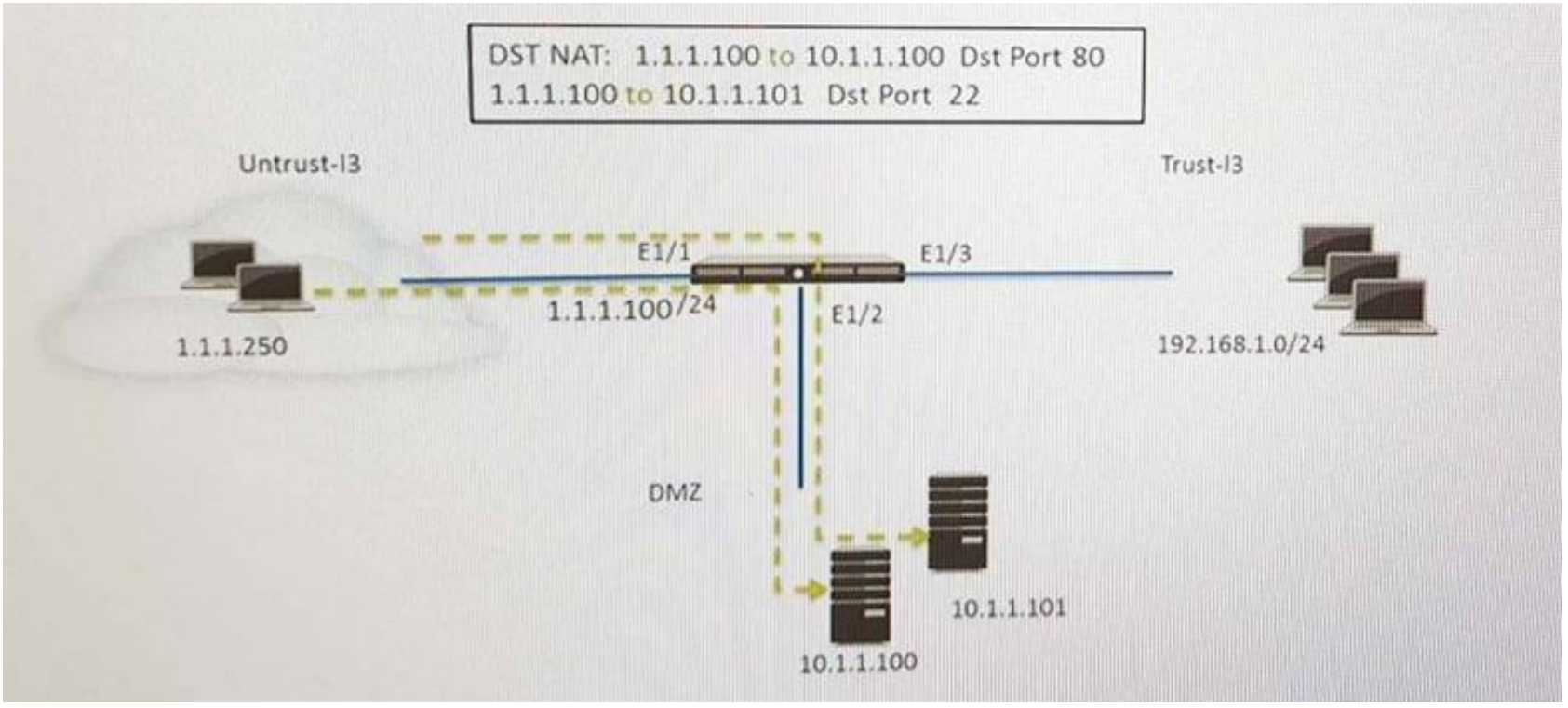
NEW QUESTION 203
- (Exam Topic 2)
When backing up and saving configuration files, what is achieved using only the firewall and is not available in Panorama?

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

Answer: D

NEW QUESTION 205

- (Exam Topic 2)
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 DMZ (10.1.1.100.10.1.1.101), ssh, web-browsing –Allow
B. Untrust (Any) to DMZ (1.1.1.100), web-browsing –Allow
C. Untrust (Any) to Untrust (10.1.1.1), web-browsing –Allow
D. Untrust (Any) to Untrust (10.1.1.1), SSH -Allow
E. Untrust (Any) to DMZ (1.1.1.100), SSH –Allow

Answer: BE

Explanation:
https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/networking/nat/nat-configuration-examples/destinat

NEW QUESTION 208
- (Exam Topic 2)
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 administratorapproves the update.
D. Automatically “download and install” but with the “disable new applications” option used.

Answer: A

Explanation:
For Antivirus and Applications and Threats updates, you have the option to set a minimum Threshold of time that a content update must be available before the firewall installs it. Very rarely, there can be an error in a content update and this threshold ensures that the firewall only downloads content releases that have been available and functioning in customer environments for the specified amount of time. https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/device/device-dynamic-updates

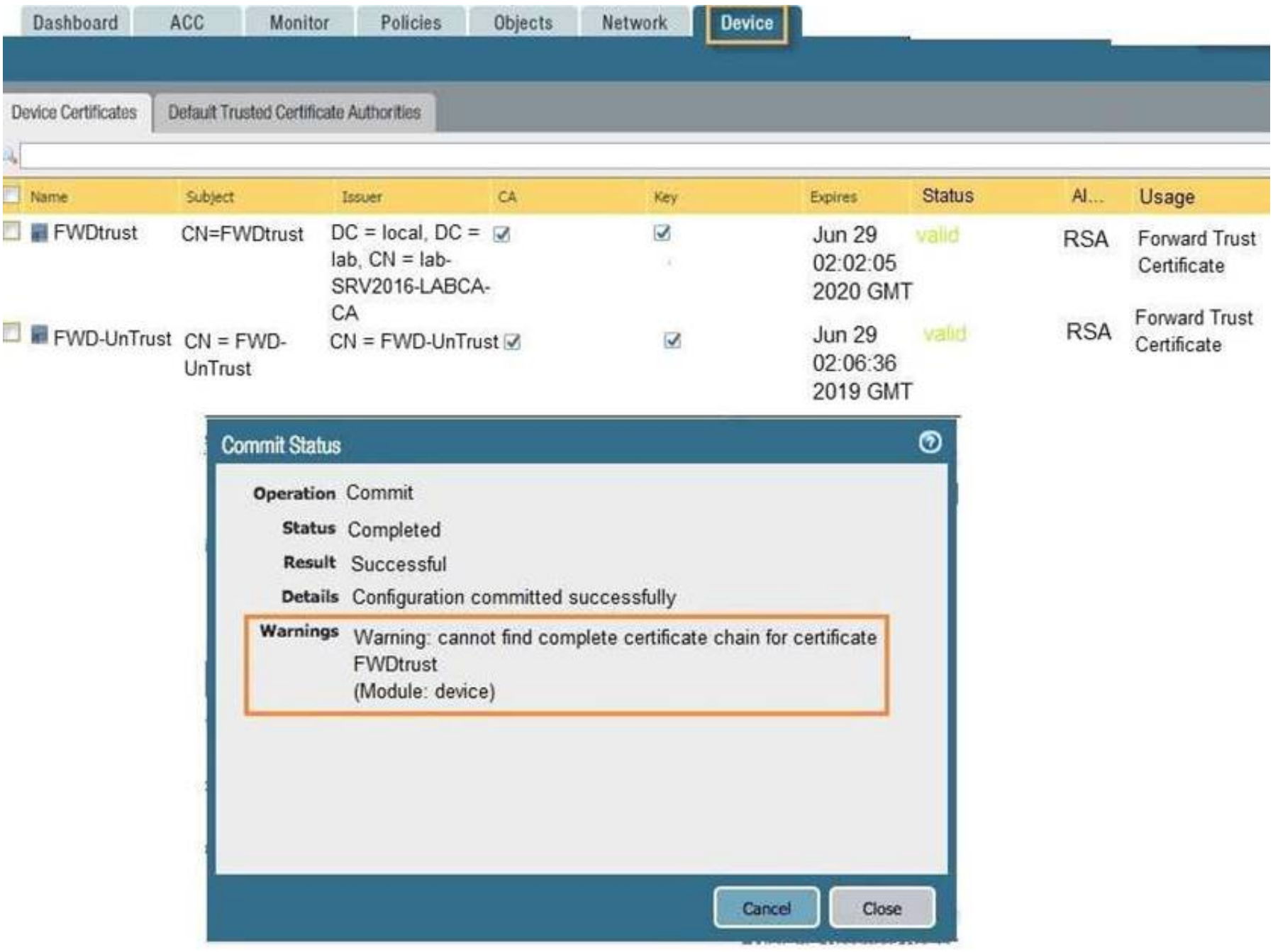
NEW QUESTION 211
- (Exam Topic 2)
An administrator has been asked to configure a Palo Alto Networks NGFW to provide protection against external hosts attempting to exploit a flaw in an operating system on an internal system.
Which Security Profile type will prevent this attack?

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

Answer: A

Explanation:
Reference:
https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/objects/objects-security-profile vulnerability-protection

NEW QUESTION 216
- (Exam Topic 2)
Based on the image, what caused the commit warning?



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

Answer: D

NEW QUESTION 217
- (Exam Topic 2)
Which User-ID method should be configured to map IP addresses to usernames for users connected through a terminal server?

A. port mapping
B. server monitoring
C. client probing
D. XFF headers

Answer: A

Explanation:
https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/user-id/map-ip-addresses-to-users/configure-user-m

NEW QUESTION 218
- (Exam Topic 2)
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: BC

Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClEWCA0

NEW QUESTION 222
- (Exam Topic 3)
Which three fields can be included in a pcap filter? (Choose three)

A. Egress interface
B. Source IP
C. Rule number
D. Destination IP
E. Ingress interface

Answer: BCD

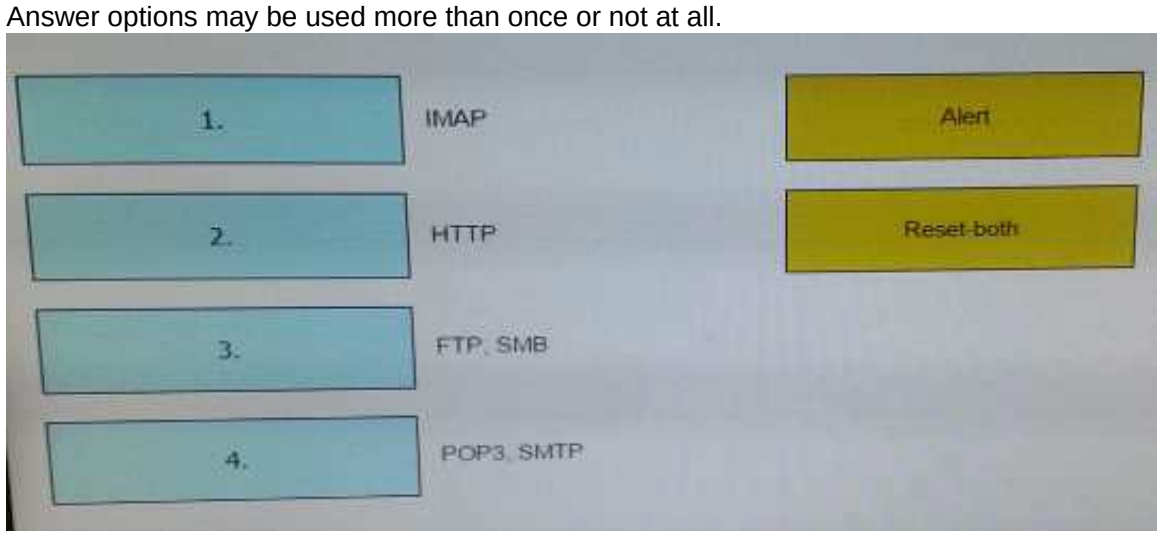
Explanation:
(https://live.paloaltonetworks.com/t5/Featured-Articles/Getting-Started-Packet-Capture/ta-p/72069)

NEW QUESTION 225
- (Exam Topic 3)
The company's Panorama server (IP 10.10.10.5) is not able to manage a firewall that was recently deployed. The firewall's dedicated management port is being used to connect to the management network.
Which two commands may be used to troubleshoot this issue from the CLI of the new firewall? (Choose two)

A. test panoramas-connect 10.10.10.5
B. show panoramas-status
C. show arp all I match 10.10.10.5
D. topdump filter "host 10.10.10.5
E. debug dataplane packet-diag set capture on

Answer: BD

NEW QUESTION 230
- (Exam Topic 3)
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 235
- (Exam Topic 3)
Which two events trigger the operation of automatic commit recovery? (Choose two.)

A. when an aggregate Ethernet interface component fails
B. when Panorama pushes a configuration
C. when a firewall HA pair fails over
D. when a firewall performs a local commit

Answer: BD

NEW QUESTION 236
- (Exam Topic 3)
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 241
- (Exam Topic 3)
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.

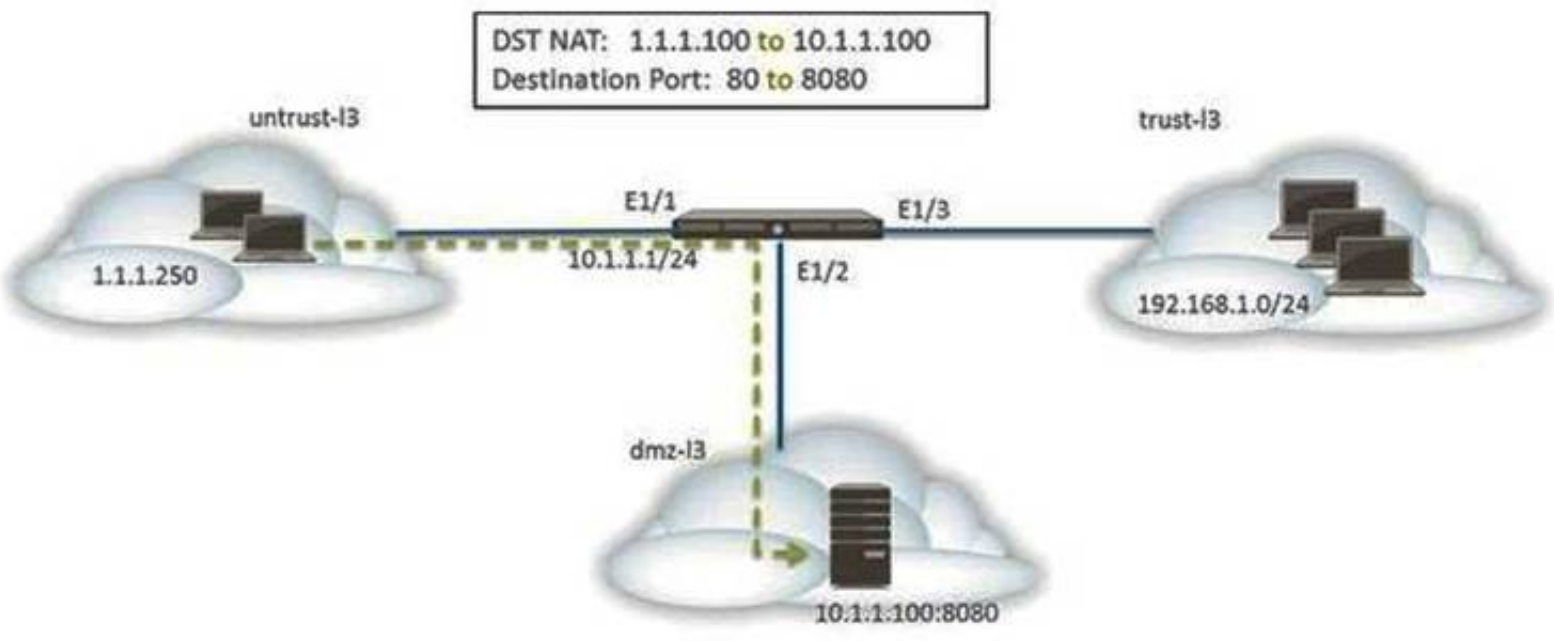
Answer: B

NEW QUESTION 245
- (Exam Topic 3)
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 250
- (Exam Topic 3)
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 251
- (Exam Topic 3)
Support for which authentication method was added in PAN-OS 8.0?

A. RADIUS
B. LDAP
C. Diameter
D. TACACS+

Answer: D

Explanation:
https://www.paloaltonetworks.com/resources/datasheets/whats-new-in-pan-os-7-1

NEW QUESTION 252
- (Exam Topic 3)
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 255
- (Exam Topic 3)
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 258
- (Exam Topic 3)
When is it necessary to activate a license when provisioning a new Palo Alto Networks firewall?

A. When configuring Certificate Profiles
B. When configuring GlobalProtect portal
C. When configuring User Activity Reports
D. When configuring Antivirus Dynamic Updates

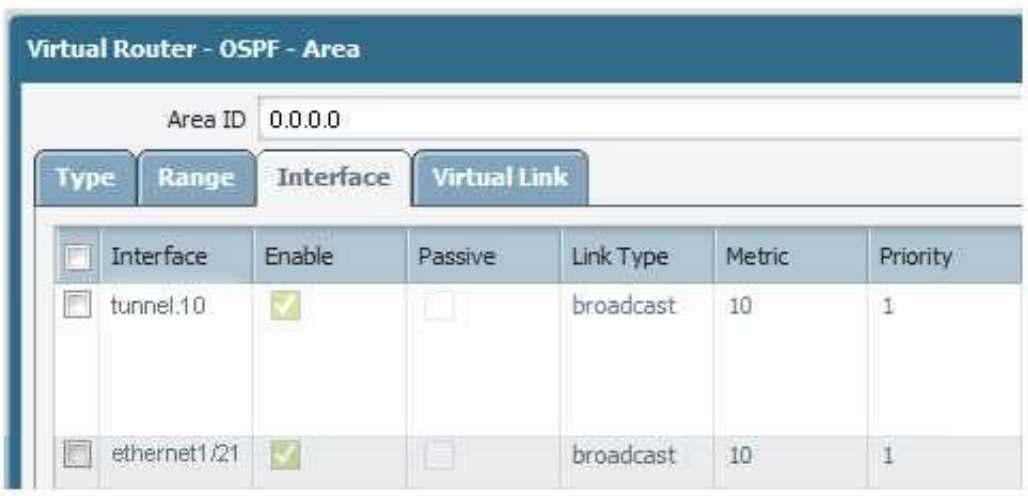
Answer: D

NEW QUESTION 263
- (Exam Topic 3)
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 267
- (Exam Topic 3)
Site-A and Site-B have a site-to-site VPN set up between them. OSPF is configured to dynamically create the routes between the sites. The OSPF configuration in Site-A is configured properly, but the route for the tunner is not being established. The Site-B interfaces in the graphic are using a broadcast Link Type. The administrator has determined that the OSPF configuration in Site-B is using the wrong Link Type for one of its interfaces.



Which Link Type setting will correct the error?

A. Set tunne
B. 1 to p2p
C. Set tunne
D. 1 to p2mp
E. Set Ethernet 1/1 to p2mp
F. Set Ethernet 1/1 to p2p

Answer: A

NEW QUESTION 269
- (Exam Topic 3)
Starting with PAN-OS version 9.1, Global logging information is now recoded in which firewall log?

A. Authentication
B. Globalprotect
C. Configuration
D. System

Answer: D

NEW QUESTION 274
- (Exam Topic 3)
The IT department has received complaints abou VoIP call jitter when the sales staff is making or receiving calls. QoS is enabled on all firewall interfaces, but there is no QoS policy written in the rulebase. The IT
manager wants to find out what traffic is causing the jitter in real time when a user reports the jitter. Which feature can be used to identify, in real time, the applications taking up the most bandwidth?

A. QoS Statistics
B. Applications Report
C. Application Command Center (ACC)
D. QoS Log

Answer: A

NEW QUESTION 276
- (Exam Topic 3)
A network engineer has revived a report of problems reaching 98.139.183.24 through vr1 on the firewall. The routing table on this firewall is extensive and complex.
Which CLI command will help identify the issue?

A. test routing fib virtual-router vr1
B. show routing route type static destination 98.139.183.24
C. test routing fib-lookup ip 98.139.183.24 virtual-router vr1
D. show routing interface

Answer: C

NEW QUESTION 279
- (Exam Topic 3)
An Administrator is configuring an IPSec VPN toa Cisco ASA at the administrator's home and experiencing issues completing the connection. The following is th output from the command:
less mp-log ikemgr.log:

```
less mp-log ikemgr.log:

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

What could be the cause of this problem?

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

Answer: B

NEW QUESTION 283
- (Exam Topic 3)
Which three items are import considerations during SD-WAN configuration planning? (Choose three.)

A. link requirements
B. the name of the ISP
C. IP Addresses
D. branch and hub locations

Answer: ACD

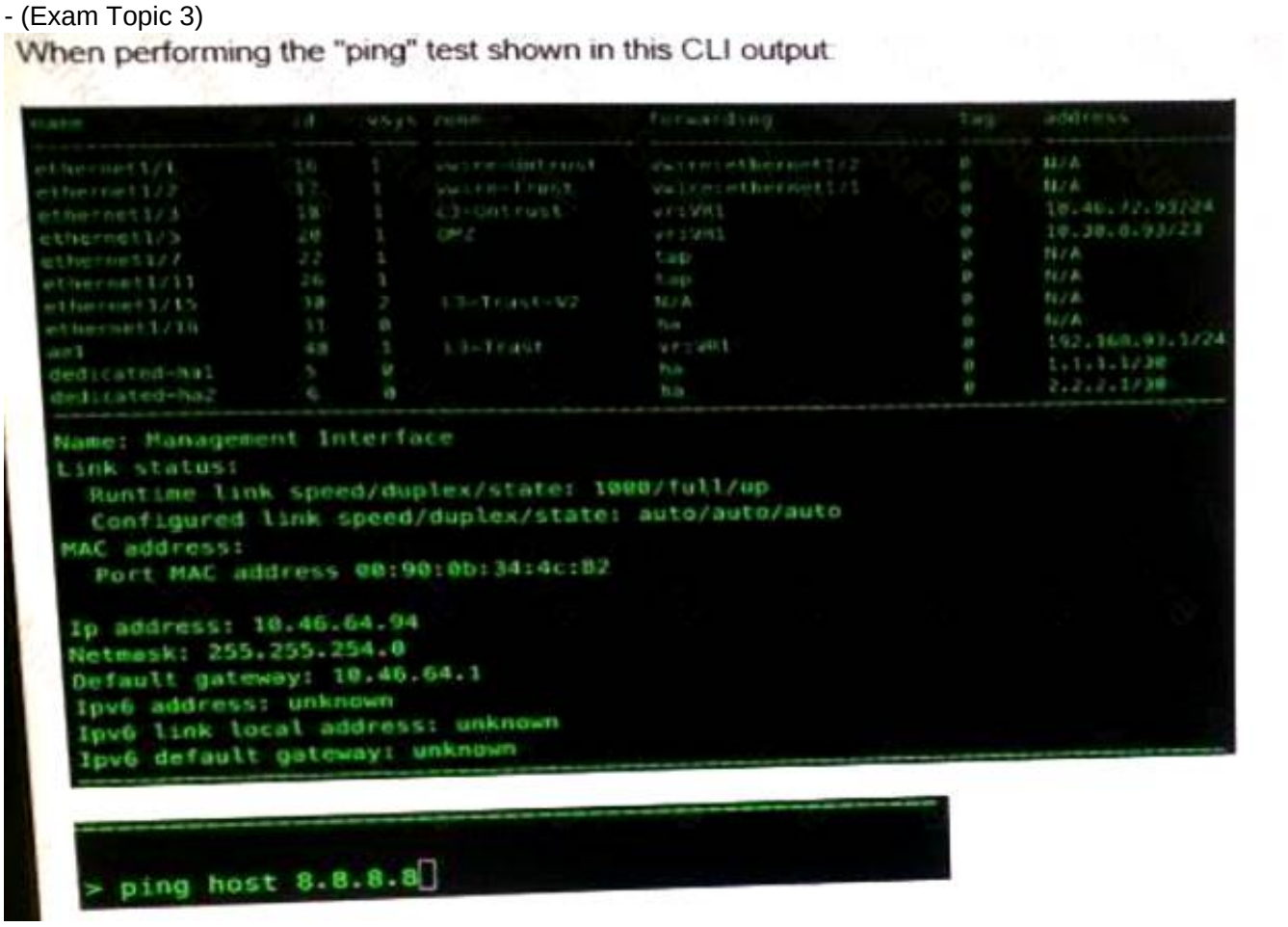
NEW QUESTION 285
- (Exam Topic 3)
A critical US-CERT notification is published regarding a newly discovered botnet. The malware is very evasive and is not reliably detected by endpoint antivirus

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 287
- (Exam Topic 3)



What will be the source address in the ICMP packet?

A. 10.30.0.93
B. 10.46.72.93
C. 10.46.64.94
D. 192.168.93.1

Answer: C

NEW QUESTION 288
- (Exam Topic 3)
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 293
- (Exam Topic 3)
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 296
- (Exam Topic 3) A
users traffic traversing a Palo Alto networks NGFW sometimes can reach http //www company com At other times the session times out. At other times the session times out The NGFW has been configured with a PBF rule that the user traffic matches when it goes to http://www.company.com goes to http://www company com How can the firewall be configured to automatically disable the PBF rule if the next hop goes down?

A. Create and add a monitor profile with an action of fail over in the PBF rule in question
B. Create and add a monitor profile with an action of wait recover in the PBF rule in question

C. Configure path monitoring for the next hop gateway on the default route in the virtual router
D. Enable and configure a link monitoring profile for the external interface of the firewall

Answer: C

NEW QUESTION 300
- (Exam Topic 3)
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 301
- (Exam Topic 3)
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 302
- (Exam Topic 3)
An administrator has left a firewall to use the data of port for all management service which there functions are performed by the data face? (Choose three.)

A. NTP
B. Antivirus
C. Wildfire updates
D. NAT
E. File tracking

Answer: ACD

NEW QUESTION 304
- (Exam Topic 3)
A host attached to Ethernet 1/4 cannot ping the default gateway. The widget on the dashboard shows Ethernet 1/1 and Ethernet 1/4 to be green. The IP address of Ethernet 1/1 is 192.168.1.7 and the IP address of Ethernet 1/4 is 10.1.1.7. The default gateway is attached to Ethernet 1/1. A default route is properly configured. What can be the cause of this problem?

A. No Zone has been configured on Ethernet 1/4.
B. Interface Ethernet 1/1 is in Virtual Wire Mode.
C. DNS has not been properly configured on the firewall.
D. DNS has not been properly configured on the host.

Answer: A

NEW QUESTION 308
- (Exam Topic 3)
Panorama provides which two SD_WAN functions? (Choose two.)

A. data plane
B. physical network links
C. network monitoring
D. control plane

Answer: CD

NEW QUESTION 312
- (Exam Topic 3)
Which CLI command displays the current management plan memory utilization?

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

Answer: B

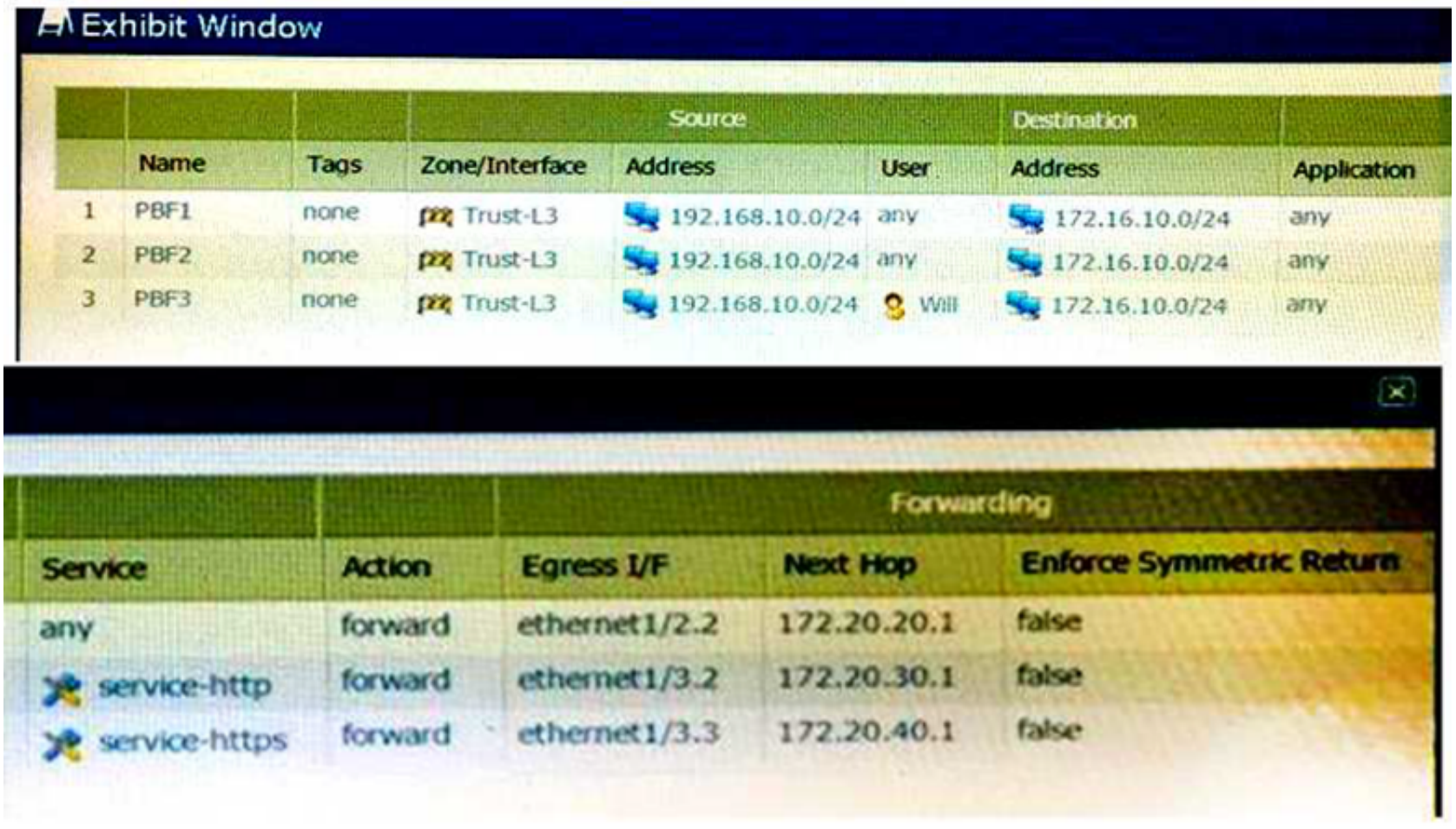
Explanation:
https://live.paloaltonetworks.com/t5/Management-Articles/Show-System-Resource-Command-Displays-CPU-U

NEW QUESTION 317
- (Exam Topic 3)
Which field is optional when creating a new Security Policy rule?

A. Name
B. Description
C. Source Zone
D. Destination Zone
E. Action

Answer: B

NEW QUESTION 320
- (Exam Topic 3)
Click the Exhibit button below,



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 324
- (Exam Topic 3)
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 329
- (Exam Topic 3)
Which interface configuration will accept specific VLAN IDs?

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

Answer: B

NEW QUESTION 331
- (Exam Topic 3)
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 335
- (Exam Topic 3)
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-u

NEW QUESTION 338
- (Exam Topic 3)
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 343
- (Exam Topic 3)
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 348
- (Exam Topic 3)
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/Management-Articles/How-to-Verify-DNS-Sinkhole-Function-is-Working/

NEW QUESTION 353
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual PCNSE Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the PCNSE Product From:

https://www.2passeasy.com/dumps/PCNSE/

Money Back Guarantee

PCNSE Practice Exam Features:

* PCNSE Questions and Answers Updated Frequently

* PCNSE Practice Questions Verified by Expert Senior Certified Staff

* PCNSE Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* PCNSE Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year