Paloalto-Networks

Exam Questions PCNSE

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

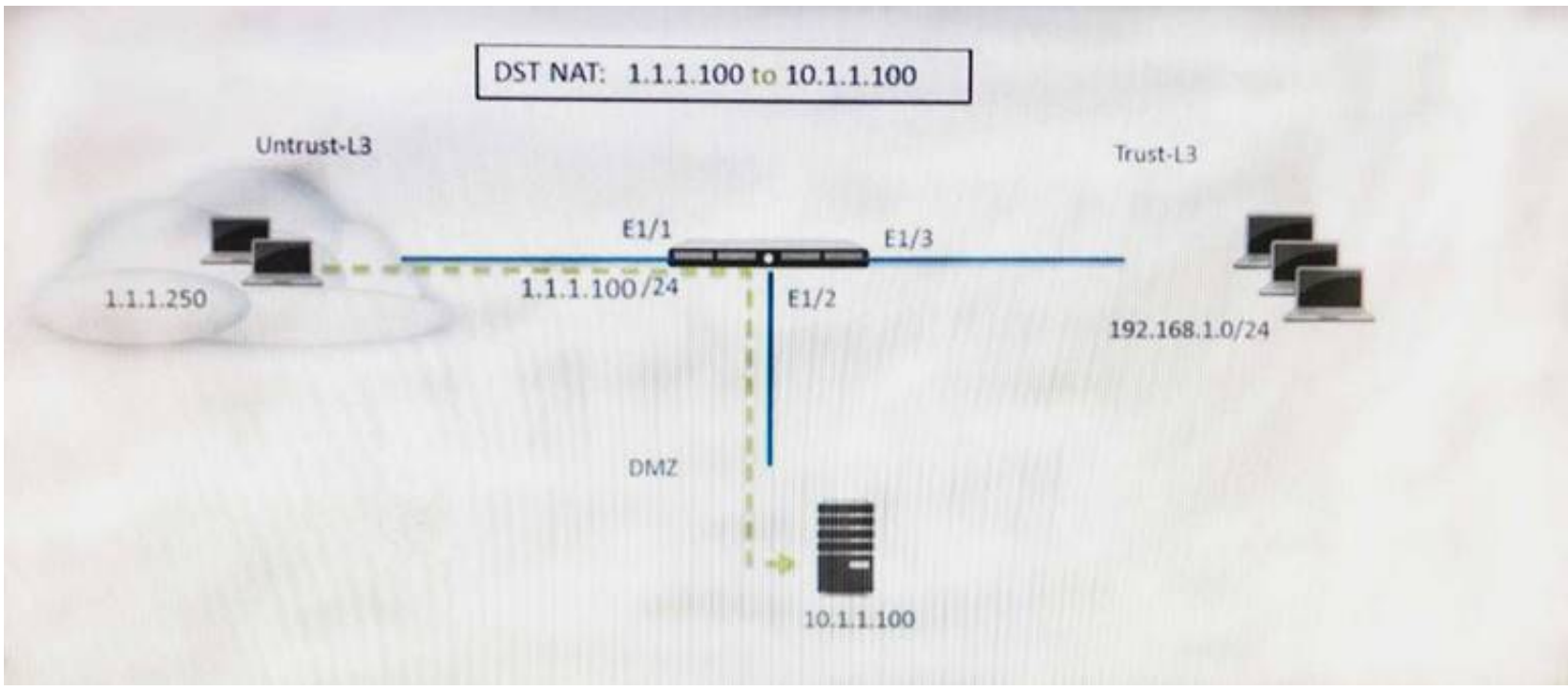
NEW QUESTION 1
- (Exam Topic 2)
Which CLI command enables an administrator to view details about the firewall including uptime, PAN-OS® version, and serial number?

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)
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 3
- (Exam Topic 2)
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: BDE

NEW QUESTION 4
- (Exam Topic 2)
A customer wants to combine multiple Ethernet interfaces into a single virtual interface using link aggregation. Which two formats are correct for naming aggregate interfaces? (Choose two.)

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

Answer: AC

NEW QUESTION 5
- (Exam Topic 2)

How can a candidate or running configuration be copied to a host external from Panorama?

A. Commit a running configuration.
B. Save a configuration snapshot.
C. Save a candidate configuration.
D. Export a named configuration snapshot.

Answer: D

Explanation:
Reference:
https://www.paloaltonetworks.com/documentation/71/panorama/panorama_adminguide/administer-panorama/ba panorama-and-firewall-configurations

NEW QUESTION 6
- (Exam Topic 2)
An administrator just submitted a newly found piece of spyware for WildFire analysis. The spyware passively monitors behavior without the user's knowledge.
What is the expected verdict from WildFire?

A. Grayware
B. Malware
C. Spyware
D. Phishing

Answer: A

Explanation:
Wildfire verdictions are as follow1-Begnin2-Greyware3-Mallicious4-Phishing https://www.paloaltonetworks.com/documentation/80/wildfire/wf_admin/wildfire-overview/wildfire-concepts/v

NEW QUESTION 7
- (Exam Topic 2)
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 8
- (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 9
- (Exam Topic 2)
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: AD

Explanation:
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/app-id/application-level-gateways#

NEW QUESTION 10
- (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.)

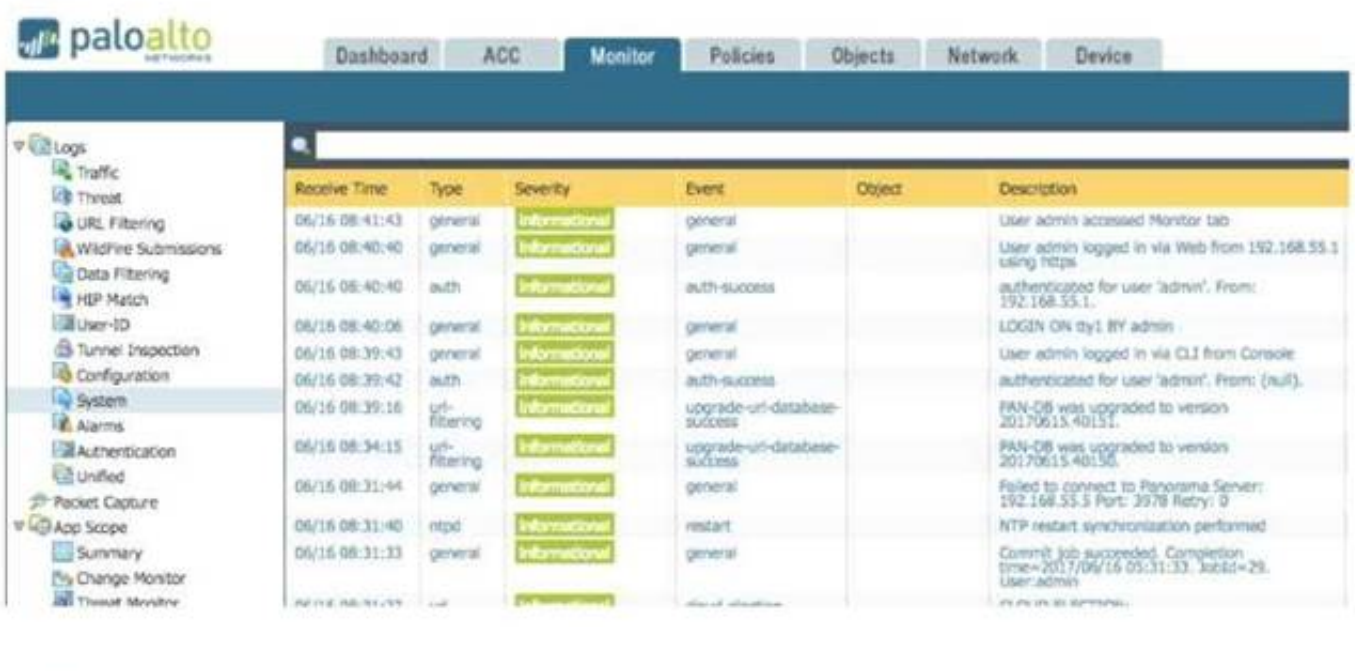
A. View Runtime Stats in the virtual router.
B. View System logs.
C. Add a redistribution profile to forward as BGP updates.
D. Perform a traffic pcap at the routing stage.

Answer: AB

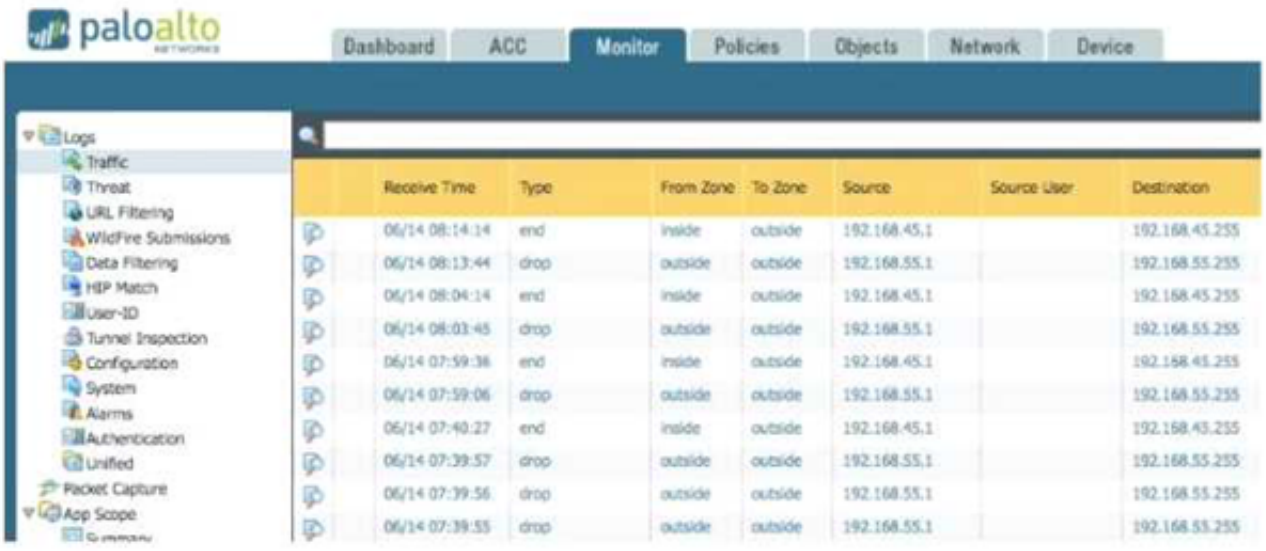
Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CldcCAC

NEW QUESTION 10
- (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

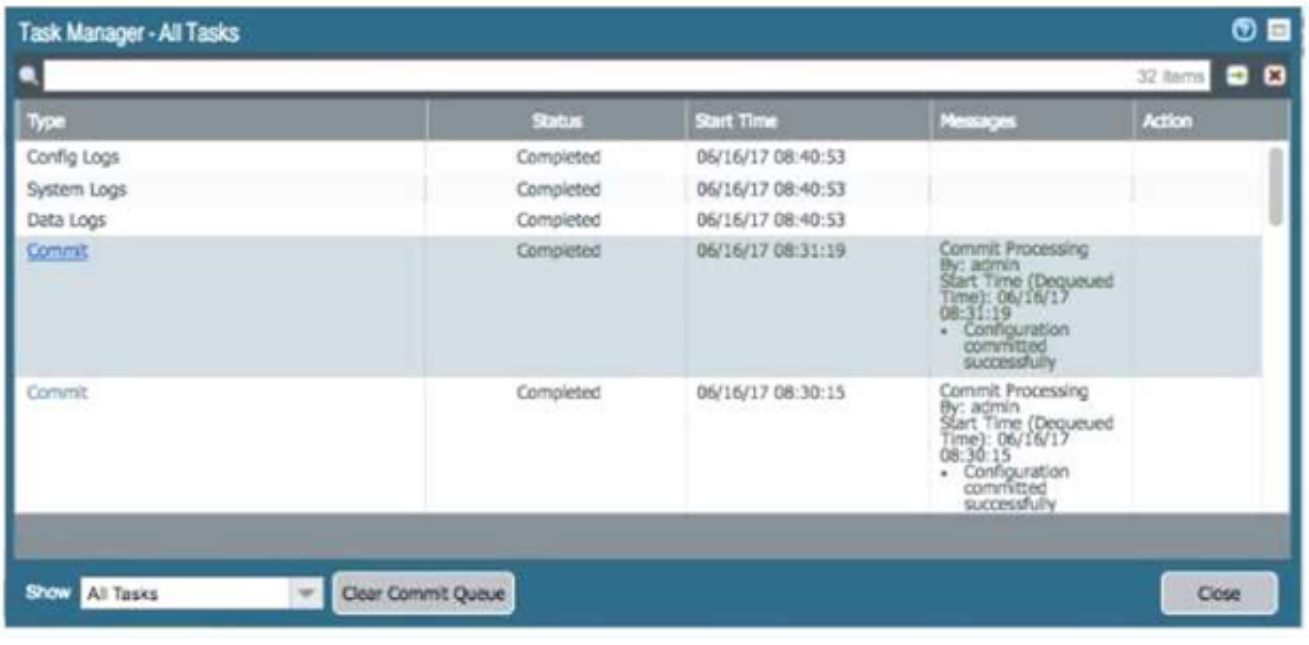


B



C

D



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

Answer: AD

NEW QUESTION 13

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

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

Answer: D

NEW QUESTION 14
- (Exam Topic 2)
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

Explanation:
https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-new-features/management-features/pa-7000-series-firewal

NEW QUESTION 19
- (Exam Topic 2)
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-mana ssltls-service-profile

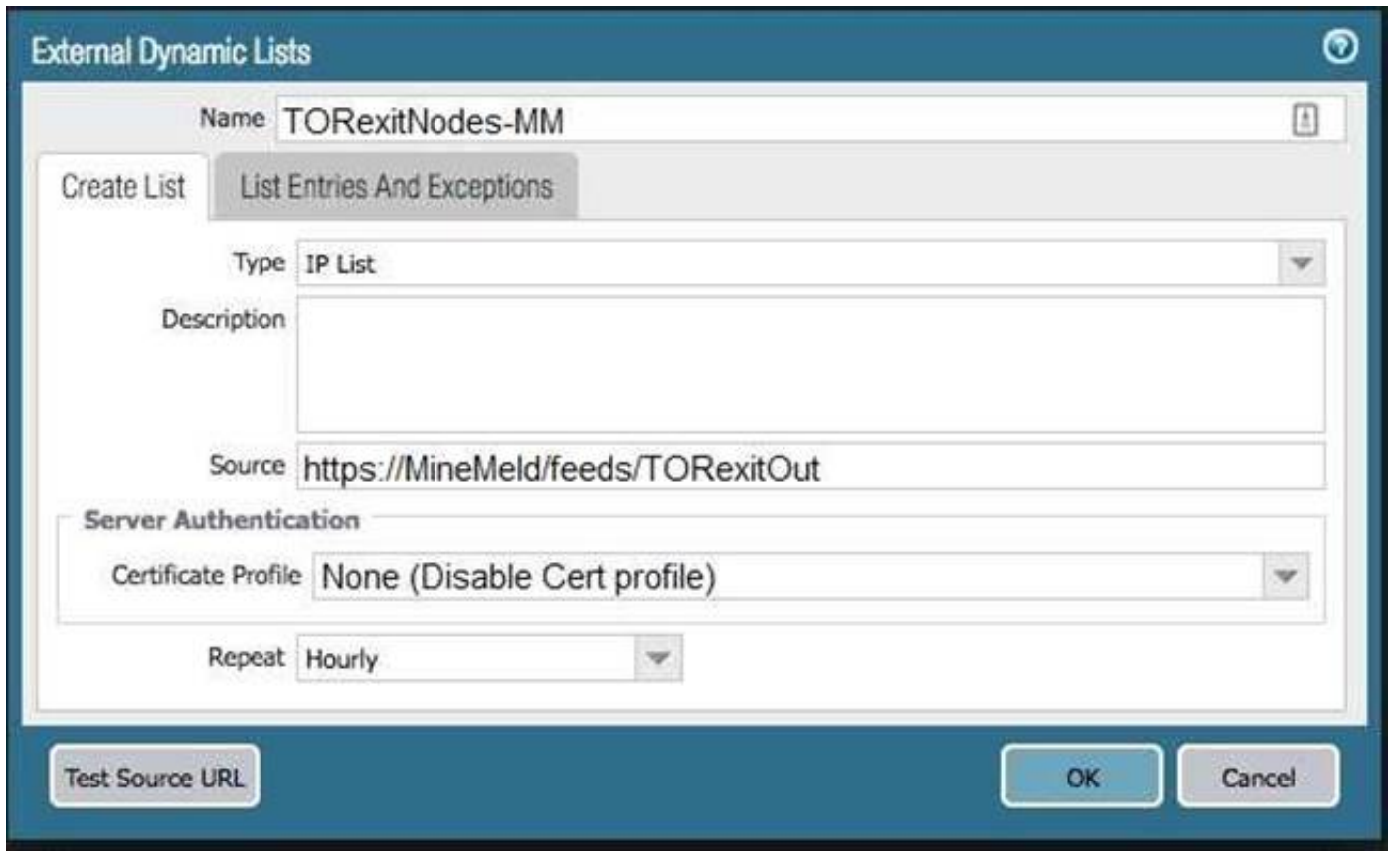
NEW QUESTION 21
- (Exam Topic 2)
Which two virtualization platforms officially support the deployment of Palo Alto Networks VM-Series firewalls? (Choose two.)

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

Answer: BD

Explanation:
Reference:
https://www.paloaltonetworks.com/products/secure-the-network/virtualized-next-generation-firewall/vm-series
docs.paloaltonetworks.com/vm-series/8-0/vm-series-deployment/about-the-vm-series-firewall/vm-series-deploy

NEW QUESTION 25
- (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 28
- (Exam Topic 2)
To more easily reuse templates and template slacks , you can create term plate variables in place of firewall-specific and appliance-specific IP literals in your configurations
Which one is the correct configuration?

A. @Panorama
B. #Pancrama
C. &Panorama
D. $Panorama

Answer: D

NEW QUESTION 33
- (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 35
- (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 38
- (Exam Topic 2)
Which two are valid ACC GlobalProtect Activity tab widgets? (Choose two)

A. Successful GlobalProtect Connection Activity
B. Successful GlobalProtect Deployed Activity
C. GlobalProtect Quarantine Activity
D. GlobalProtect Deployment Activity

Answer: AC

NEW QUESTION 39
- (Exam Topic 2)
An administrator needs to implement an NGFW between their DMZ and Core network. EIGRP Routing between the two environments is required. Which interface type would support this business requirement?

A. Virtual Wire interfaces to permit EIGRP routing to remain between the Core and DMZ
B. Layer 3 or Aggregate Ethernet interfaces, but configuring EIGRP on subinterfaces only
C. Tunnel interfaces to terminate EIGRP routing on an IPsec tunnel (with the GlobalProtect License to support LSVPN and EIGRPprotocols)
D. Layer 3 interfaces, but configuring EIGRP on the attached virtual router

Answer: A

NEW QUESTION 40
- (Exam Topic 2)
On the NGFW. how can you generate and block a private key from export and thus harden your security posture and prevent rogue administrators or other bad actors from misusing keys?

A. * 1.Select Device > Certificate Management > Certificates >Devace > Certificates* 2. Import the certificate.* 3 Select Import Private Key* 4 Click Generate to generate the new certificate
B. * 1 Select Device > Certificates * 2 Select Certificate Profile* 3 Generate the certificate* 4 Select Block Private Key Export.
C. * 1 Select Device > Certificates * 2 Select Certificate Profile.* 3 Generate the certificate* 4 Select Block Private Key Export
D. * 1 Select Device > Certificate Management > Certificates > Device > Certificates * 2 Generate the certificate* 3 Select Block Private Key Export* 4 Click Genet ale to generate the new certificate.

Answer: D

NEW QUESTION 43
- (Exam Topic 2)
A session in the Traffic log is reporting the application as “incomplete.” What does “incomplete” mean?

A. The three-way TCP handshake was observed, but the application could not be identified.
B. The three-way TCP handshake did not complete.
C. The traffic is coming across UDP, and the application could not be identified.
D. Data was received but was instantly discarded because of a Deny policy was applied before App-ID could be applied.

Answer: B

Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClibCAC

NEW QUESTION 45
- (Exam Topic 2)
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: AD

Explanation:
https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/app-id/manage-custom-or-unknown-applic

NEW QUESTION 50
- (Exam Topic 2)
Which CLI command enables an administrator to check the CPU utilization of the dataplane?

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

Answer: A

Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClXwCAK

NEW QUESTION 53
- (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 57
- (Exam Topic 2)
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 60
- (Exam Topic 2)
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
“Before you can enable Decryption Mirroring, you must obtain and install a Decryption Port Mirror license. The license is free of charge and can be activated through the support portal as described in the following procedure. After you install the Decryption Port Mirror license and reboot the firewall, you can enable decryption port mirroring. “

NEW QUESTION 64
- (Exam Topic 2)
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: ACF

Explanation:
https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/firewall-administration/manage-firewall-administra
The administrative accounts are defined on an external SAML, TACACS+, or RADIUS server. The server performs both authentication and authorization. For authorization, you define Vendor-Specific Attributes (VSAs) on the TACACS+ or RADIUS server, or SAML attributes on the SAML server. PAN-OS maps the attributes to administrator roles, access domains, user groups, and virtual systems that you define on the firewall. For details, see:
Configure SAML AuthenticationConfigure TACACS+ AuthenticationConfigure RADIUS Authentication

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)
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.

Answer: B

Explanation:
Reference:
https://live.paloaltonetworks.com/t5/Learning-Articles/Tips-amp-Tricks-How-to-Create-an-Application-Overrid
https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-admin/app-id/manage-custom-or-unknown- applications#

NEW QUESTION 73
- (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 75
- (Exam Topic 2)
A client is concerned about resource exhaustion because of denial-of-service attacks against their DNS servers. Which option will protect the individual servers?

A. Enable packet buffer protection on the Zone Protection Profile.
B. Apply an Anti-Spyware Profile with DNS sinkholing.
C. Use the DNS App-ID with application-default.
D. Apply a classified DoS Protection Profile.

Answer: D

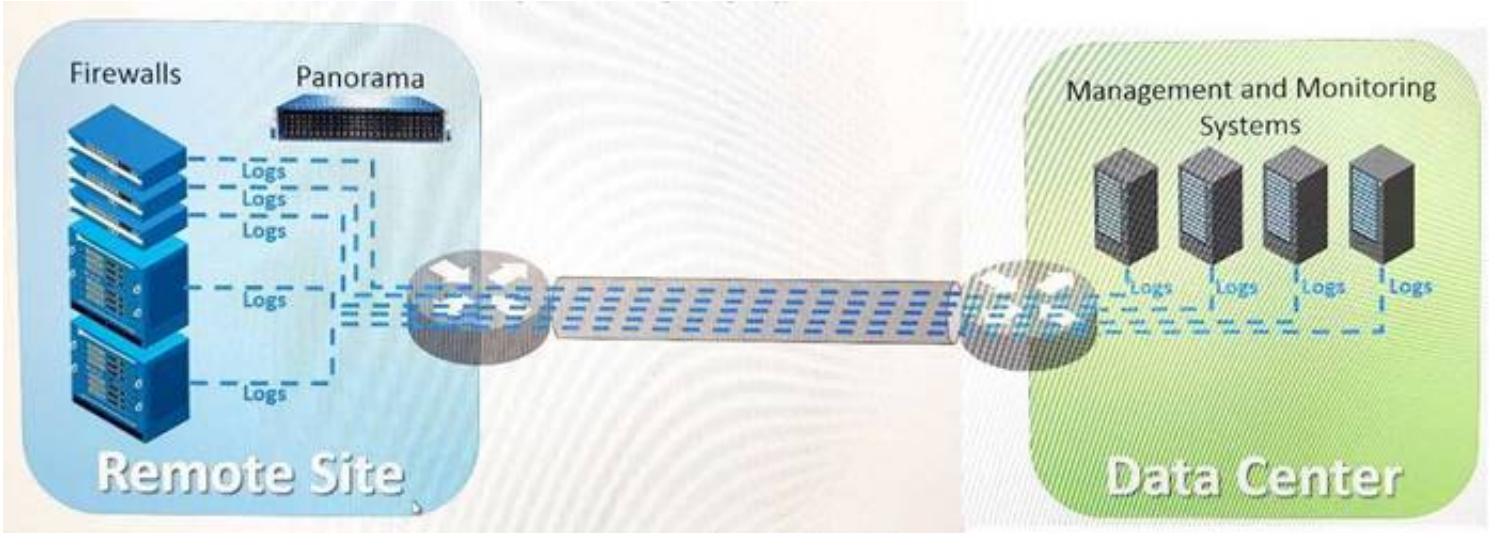
Explanation:
https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/zone-protection-and-dos-protection/zone-defense/d To protect critical web or DNS servers on your network, protect the individual servers. To do this, set
appropriate flooding and resource protection thresholds in a DoS protection profile, and create a DoS protection policy rule that applies the profile to each server’s IP address by adding the IP addresses as the rule’s destination criteria.

NEW QUESTION 77
- (Exam Topic 2)
An administrator needs to upgrade an NGFW to the most current version of PAN-OS® software. The following is occurring:
•Firewall has Internet connectivity through e1/1.
•Default security rules and security rules allowing all SSL and web-browsing traffic to and from any zone.
•Service route is configured, sourcing update traffic from e1/1.
•A communication error appears in the System logs when updates are performed.
•Download does not complete.
What must be configured to enable the firewall to download the current version of PAN-OS software?

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

Answer: D

NEW QUESTION 80
- (Exam Topic 2)
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

Explanation:
https://docs.paloaltonetworks.com/panorama/8-1/panorama-admin/panorama-overview/centralized-logging-and
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClKFCA0
"When this has to be done over a WAN link with bandwidth limitation, it is necessary to consider reducing the number of log streams that are sent over the link"
"With this configuration, firewalls will forward logs to Panorama, assuming that log forwarding was configured correctly on the firewall. The logs are forwarded to the syslog server, thus reducing the number of log streams significantly."

NEW QUESTION 81
- (Exam Topic 2)
Which data flow describes redistribution of user mappings?

A. User-ID agent to firewall
B. firewall to firewall
C. Domain Controller to User-ID agent
D. User-ID agent to Panorama

Answer: B

Explanation:
https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/user-id/configure-firewalls-to-redistribute-

NEW QUESTION 84
- (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 86
- (Exam Topic 2)
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/5

NEW QUESTION 91
- (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 92
- (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 95
- (Exam Topic 2)
Which PAN-OS® policy must you configure to force a user to provide additional credentials before he is allowed to access an internal application that contains highly-sensitive business data?

A. Security policy
B. Decryption policy
C. Authentication policy
D. Application Override policy

Answer: C

NEW QUESTION 98
- (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 101
- (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 103
- (Exam Topic 2)
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: AD

Explanation:
https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/decryption/configure-decryption-exception

NEW QUESTION 108
- (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 110
- (Exam Topic 2)
What are the two behavior differences between Highlight Unused Rules and the Rule Usage Hit counter when a firewall is rebooted? (Choose two.)

A. Rule Usage Hit counter will not be reset
B. Highlight Unused Rules will highlight all rules.
C. Highlight Unused Rules will highlight zero rules.
D. Rule Usage Hit counter will reset.

Answer: AB

NEW QUESTION 114
- (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 117
- (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

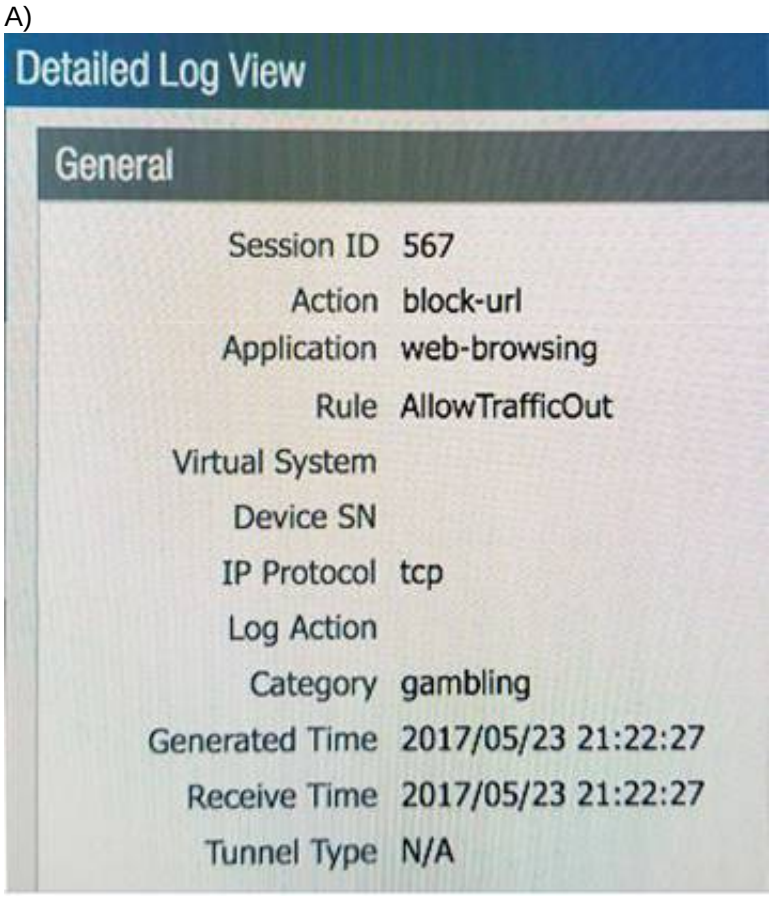
NEW QUESTION 119
- (Exam Topic 2)
Which Captive Portal mode must be configured to support MFA authentication?

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

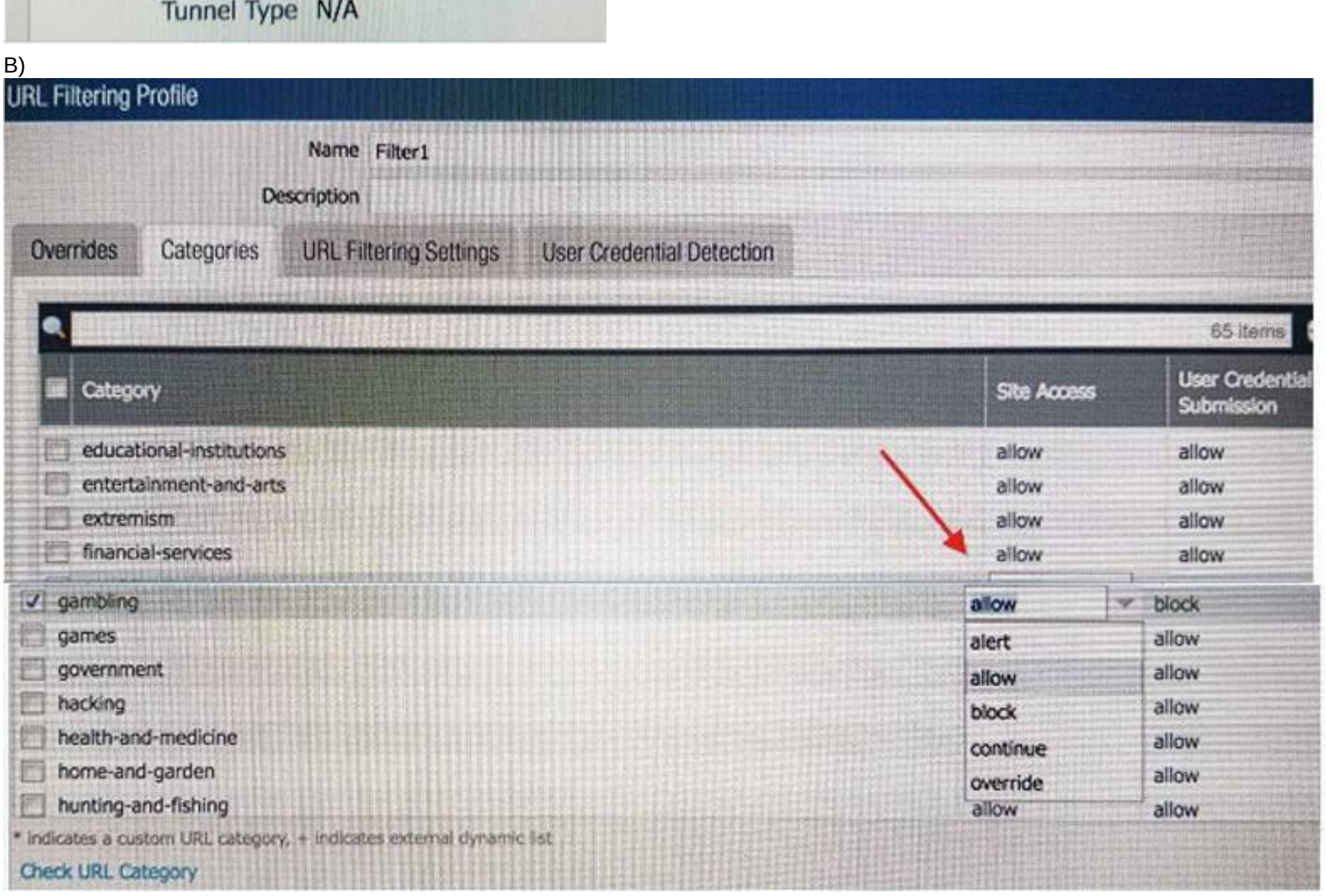
Answer: B

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

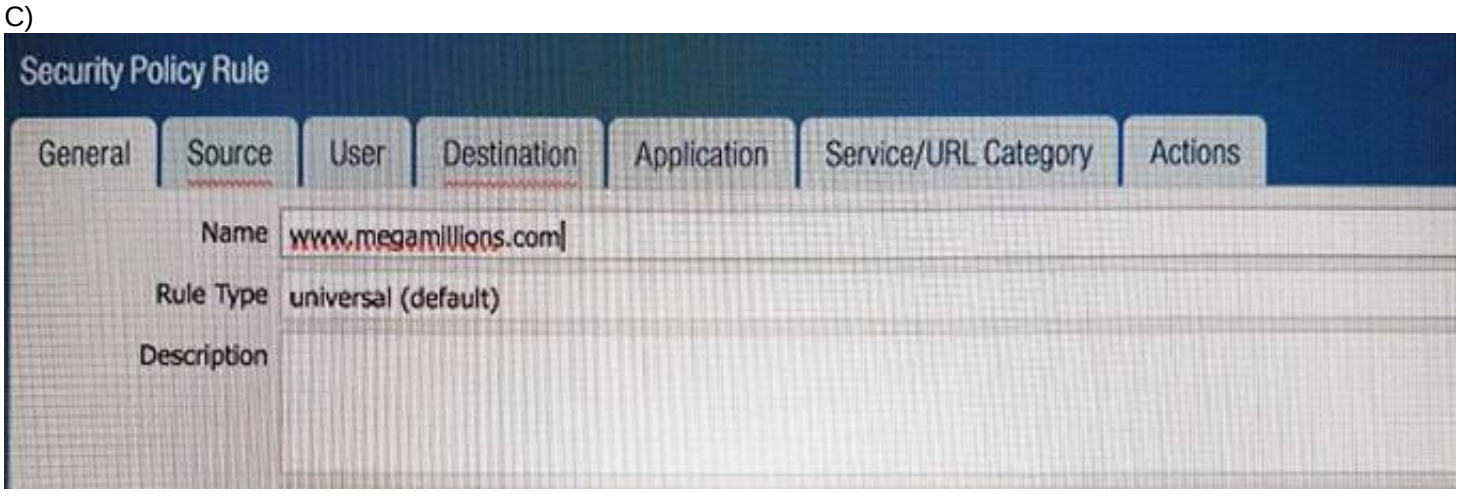
NEW QUESTION 124
- (Exam Topic 2)
An administrator needs to determine why users on the trust zone cannot reach certain websites. The only information available is shown on the following image.
Which configuration change should the administrator make?
A)



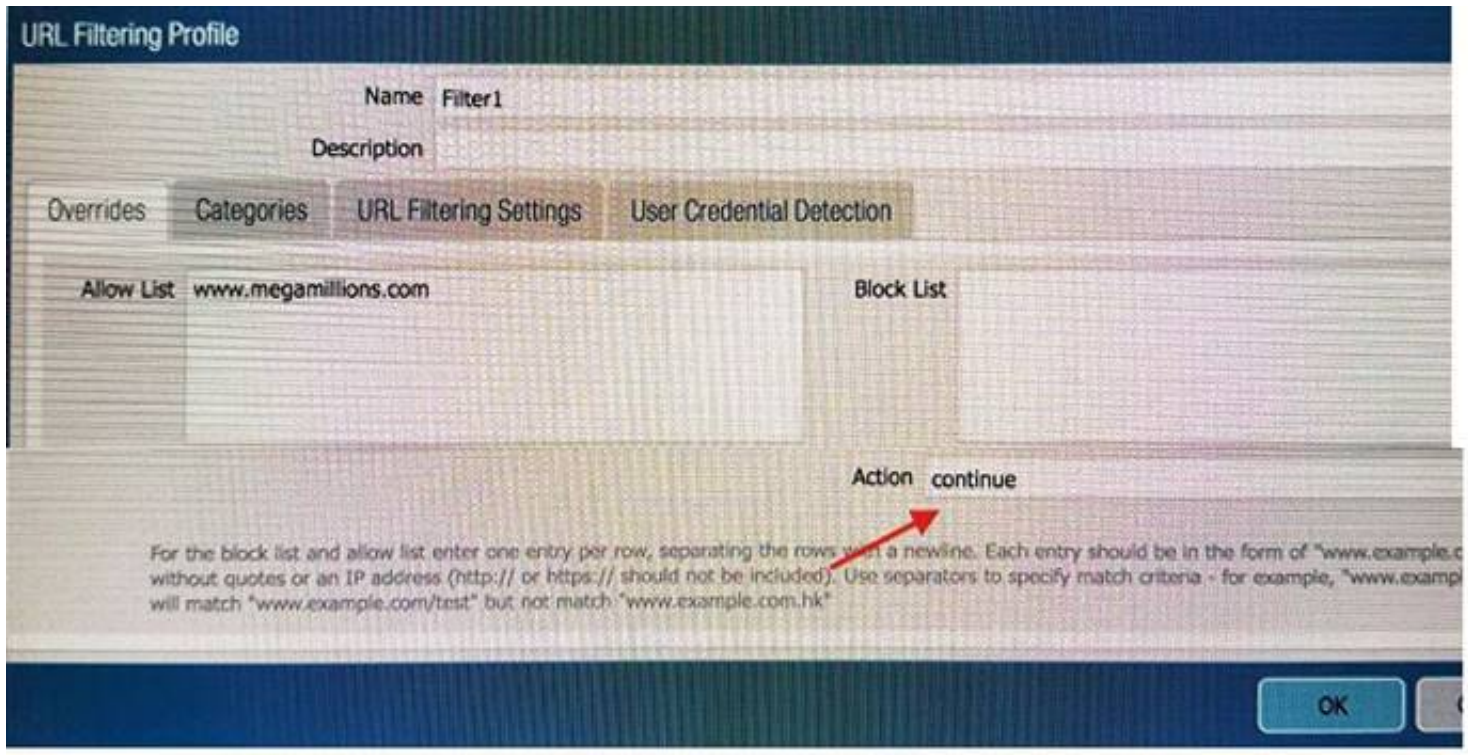
B)



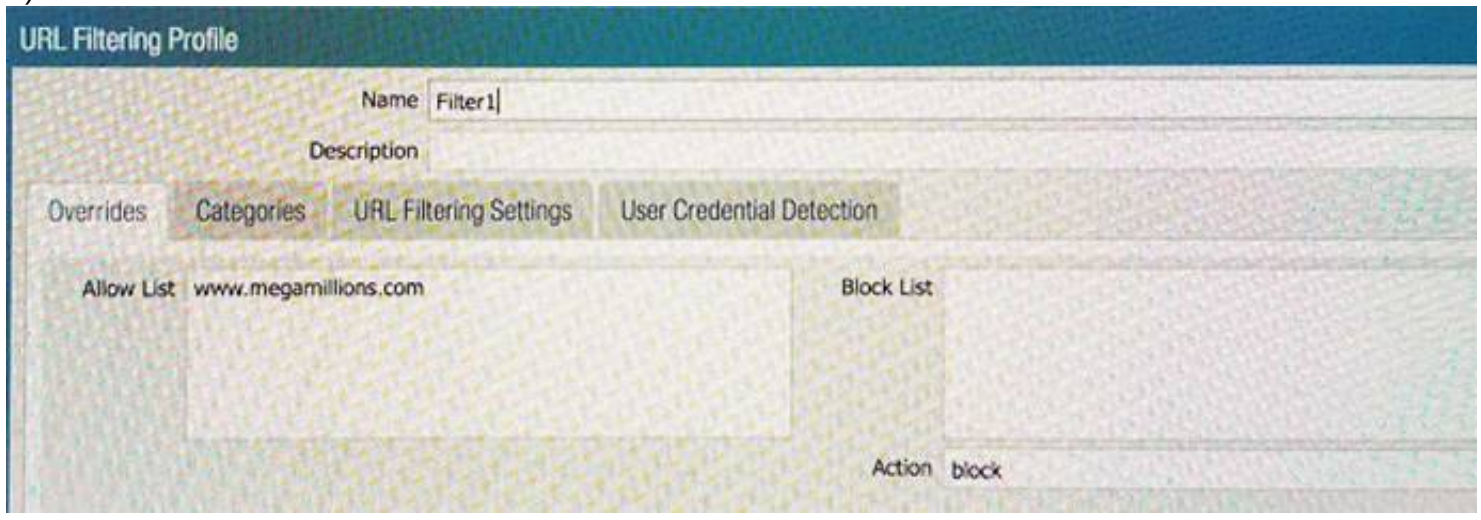
C)



D)



E)



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

Answer: B

NEW QUESTION 128
- (Exam Topic 2)
When configuring the firewall for packet capture, what are the valid stage types?

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

Answer: D

NEW QUESTION 131
- (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 135
- (Exam Topic 2)
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 https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/monitoring/take-packet-captures/take-a-packet-capt

NEW QUESTION 138
- (Exam Topic 2)
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

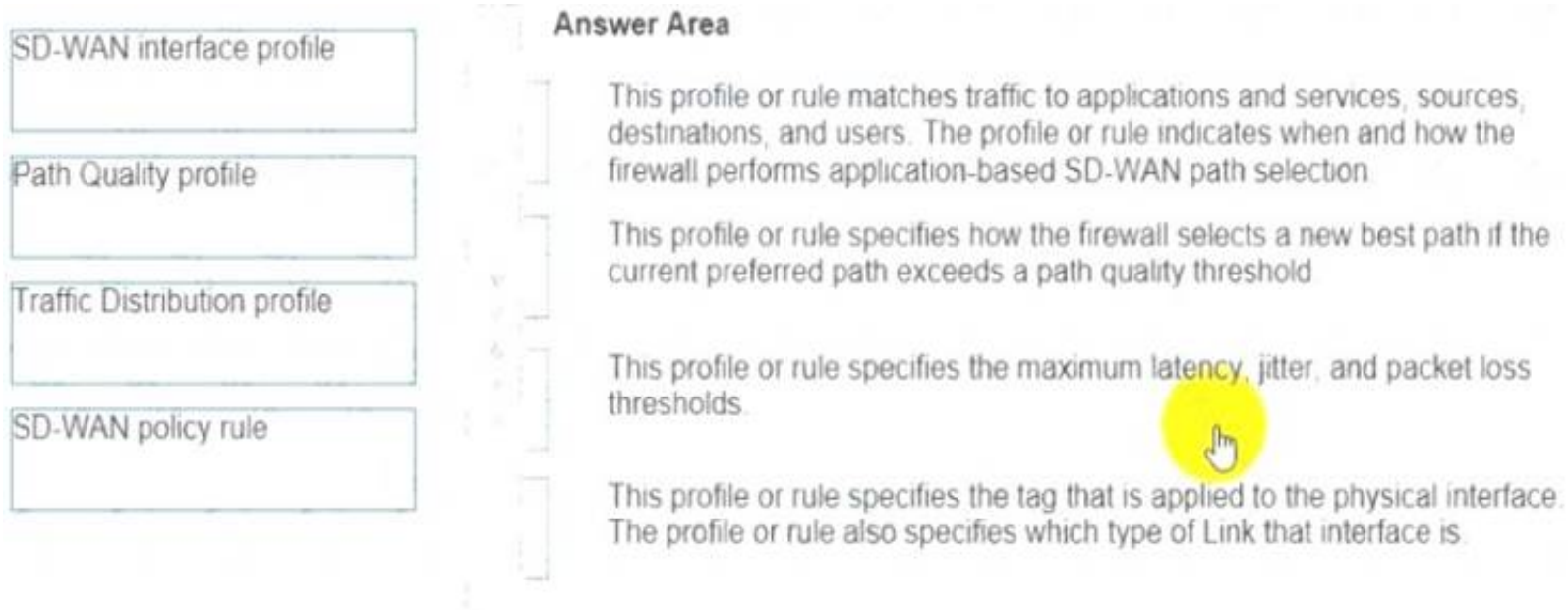
Answer: D

NEW QUESTION 143
- (Exam Topic 2)
Which two methods can be configured to validate the revocation status of a certificate? (Choose two.)

A. CRL
B. CRT
C. OCSP
D. Cert-Validation-Profile
E. SSL/TLS Service Profile

Answer: AC

NEW QUESTION 144
- (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.

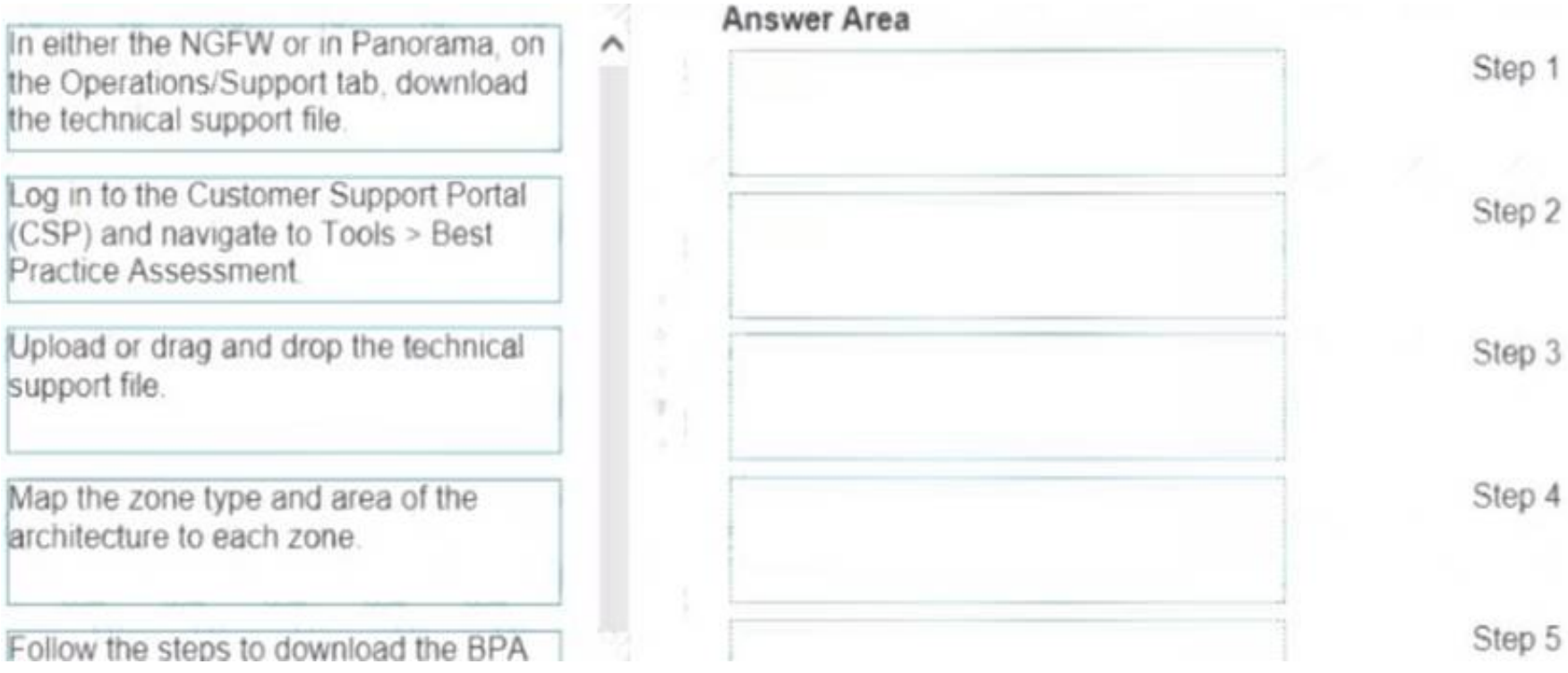
The preceding elements come together in
SD-WAN Policy Rules
The purple arrow indicates that you reference a Path Qualify Profile and a Traffic Distribution profile in a rule, along with packet applications/services, sources, destinations, and users to specifically indicate when and how the firewall performs 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 148
- (Exam Topic 1)
An organization has recently migrated its infrastructure and configuration to NGFWs, for which Panorama manages the devices The organization is coming from a L2-L4 firewall vendor, but wants to use App-ID while identifying policies that are no longer needed
Which Panorama tool can help this organization?

A. Config Audit
B. Policy Optimizer
C. Application Groups
D. Test Policy Match

Answer: A

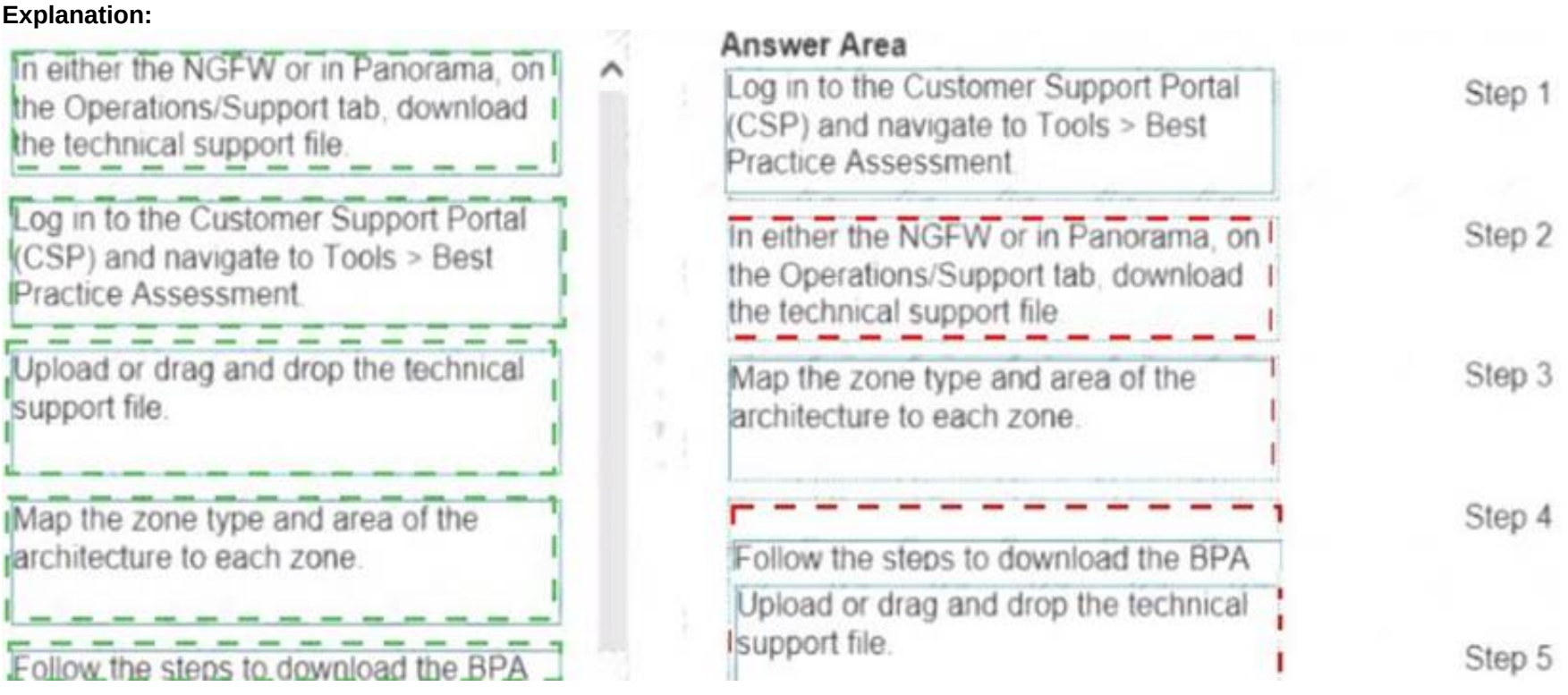
NEW QUESTION 151
- (Exam Topic 1)
Below are the steps in the workflow for creating a Best Practice Assessment in a firewall and Panorama configuration Place the steps in order.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 152
- (Exam Topic 1)
When an in-band data port is set up to provide access to required services, what is required for an interface that is assigned to service routes?

A. The interface must be used for traffic to the required services
B. You must enable DoS and zone protection
C. You must set the interface to Layer 2 Layer 3. or virtual wire
D. You must use a static IP address

Answer: A

NEW QUESTION 154
- (Exam Topic 1)
When setting up a security profile which three items can you use? (Choose three)

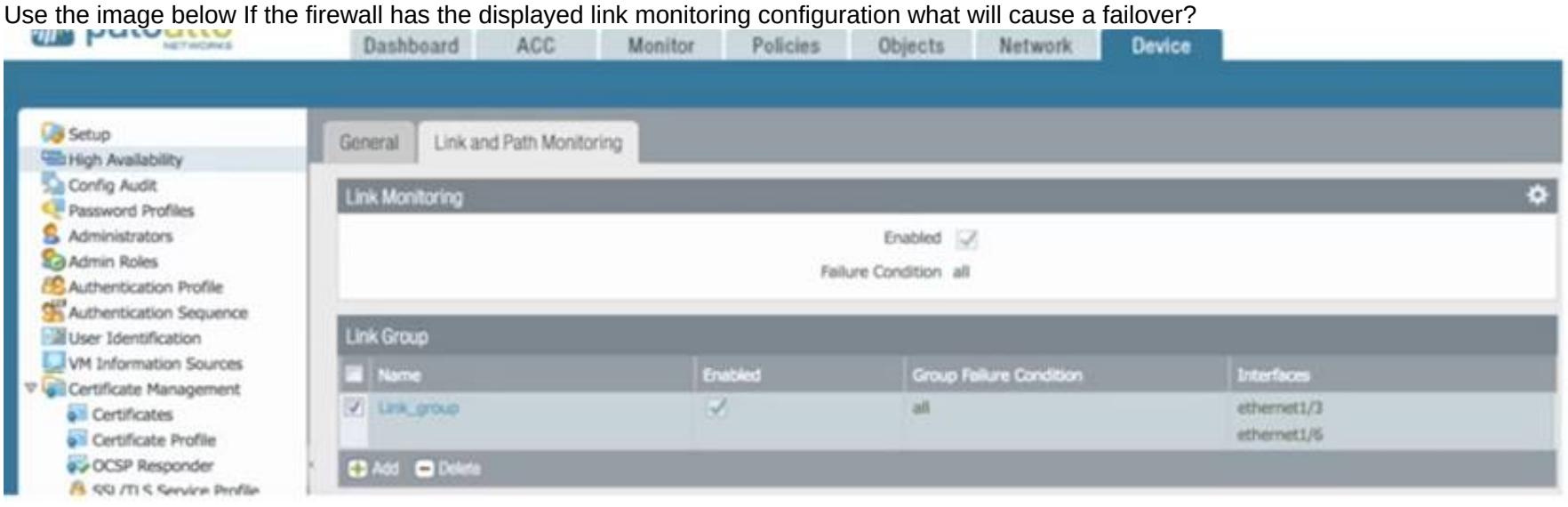
A. Wildfire analysis
B. anti-ransom ware
C. antivirus
D. URL filtering
E. decryption profile

Answer: ACD

Explanation:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/security-profiles

NEW QUESTION 155
- (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 160
- (Exam Topic 1)
Given the following snippet of a WildFire submission log. did the end-user get access to the requested information and why or why not?

TYPE	APPLICATION	ACTION	RULE	RULE UUID	BYTES	SEVERITY	CATEGORY	URL CATEGORY LIST	VERDICT
wildfire	smtp-base	allow	Watch Public DNS and SMTP	d96eb449-2...		high			malicious
wildfire	smtp-base	allow	Watch Public DNS and SMTP	d96eb449-2...		high			malicious
wildfire	smtp-base	allow	Watch Public DNS and SMTP	d96eb449-2...		high			malicious
wildfire	smtp-base	allow	Watch Public DNS and SMTP	d96eb449-2...		high			malicious
wildfire	smtp-base	allow	Watch Public DNS and SMTP	d96eb449-2...		high			malicious
file	smtp-base	alert	Watch Public DNS and SMTP	d96eb449-2...		low	any		
file	smtp-base	alert	Watch Public DNS and SMTP	d96eb449		low	any		

A. Ye
B. because the action is set to "allow "
C. No because WildFire categorized a file with the verdict "malicious"
D. Yes because the action is set to "alert"
E. No because WildFire classified the seventy as "high."

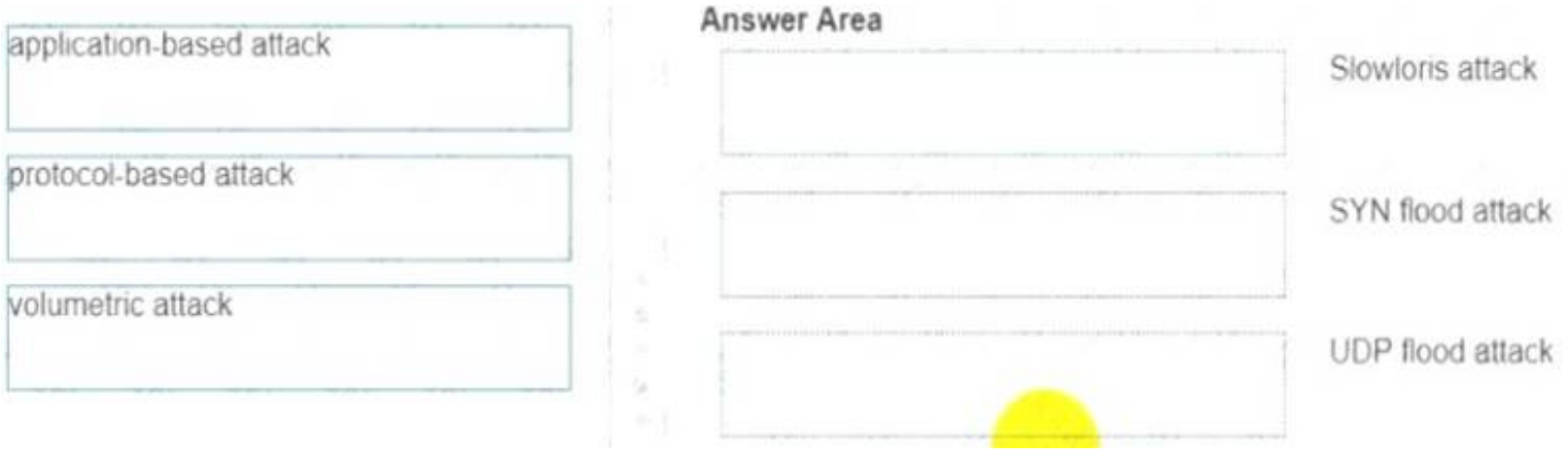
Answer: B

NEW QUESTION 164
- (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 168
- (Exam Topic 1)
Match each type of DoS attack to an example of that type of attack



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Plan to defend your network against different types of DoS attacks:

- Application-Based Attacks

—Target weaknesses in a particular application and try to exhaust its resources so legitimate users can't use it. An example of this is the Slowloris attack.

- Protocol-Based Attacks

—Also known as state-exhaustion attacks, these attacks target protocol weaknesses. A common example is a SYN flood attack.

- Volumetric Attacks

—High-volume attacks that attempt to overwhelm the available network resources, especially bandwidth, and bring down the target to prevent legitimate users from accessing those resources. An example of this is a UDP flood attack.
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/zone-protection-and-dos-protection/zone-defense.ht

NEW QUESTION 169
- (Exam Topic 1)
When you configure a Layer 3 interface what is one mandatory step?

A. Configure Security profiles, which need to be attached to each Layer 3 interface
B. Configure Interface Management profiles which need to be attached to each Layer 3 interface
C. Configure virtual routers to route the traffic for each Layer 3 interface
D. Configure service routes to route the traffic for each Layer 3 interface

Answer: A

NEW QUESTION 170
- (Exam Topic 1)
Before you upgrade a Palo Alto Networks NGFW what must you do?

A. Make sure that the PAN-OS support contract is valid for at least another year
B. Export a device state of the firewall
C. Make sure that the firewall is running a version of antivirus software and a version of WildFire that support the licensed subscriptions.
D. Make sure that the firewall is running a supported version of the app + threat update

Answer: B

NEW QUESTION 171
- (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 173
- (Exam Topic 1)
An administrator needs to implement an NGFW between their DMZ and Core network EIGRP Routing between the two environments is required Which interface type would support this business requirement?

A. Layer 3 interfaces but configuring EIGRP on the attached virtual router
B. Virtual Wire interfaces to permit EIGRP routing to remain between the Core and DMZ

C. Layer 3 or Aggregate Ethernet interfaces but configuring EIGRP on subinterfaces only
D. Tunnel interfaces to terminate EIGRP routing on an IPsec tunnel {with the GlobalProtect License to support LSVPN and EIGRP protocols)

Answer: D

NEW QUESTION 176
- (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

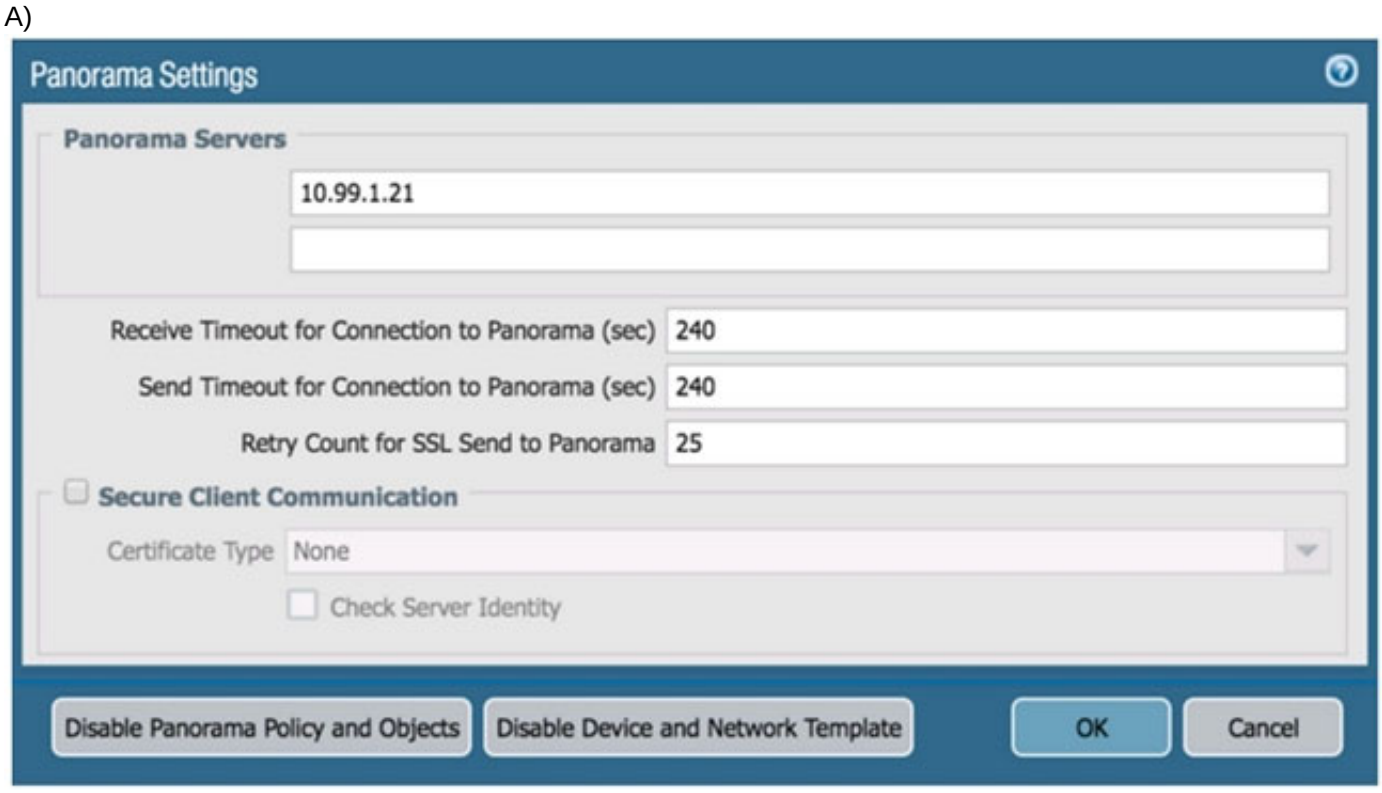
NEW QUESTION 181
- (Exam Topic 1)
What does SSL decryption require to establish a firewall as a trusted third party and to establish trust between a client and server to secure an SSL/TLS connection?

A. link state
B. stateful firewall connection
C. certificates
D. profiles

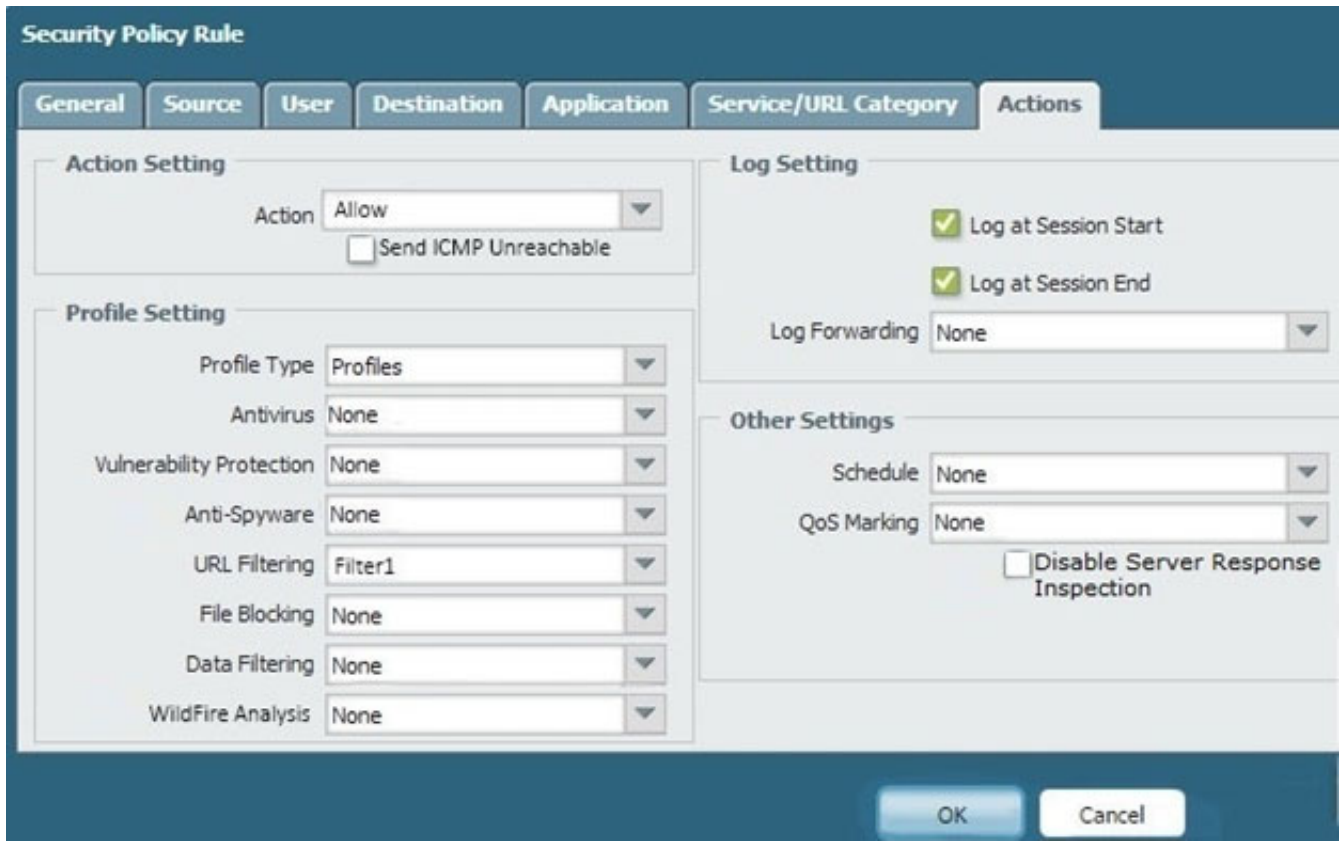
Answer: C

Explanation:
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/decryption/decryption-overview.html#:~:text=SSL

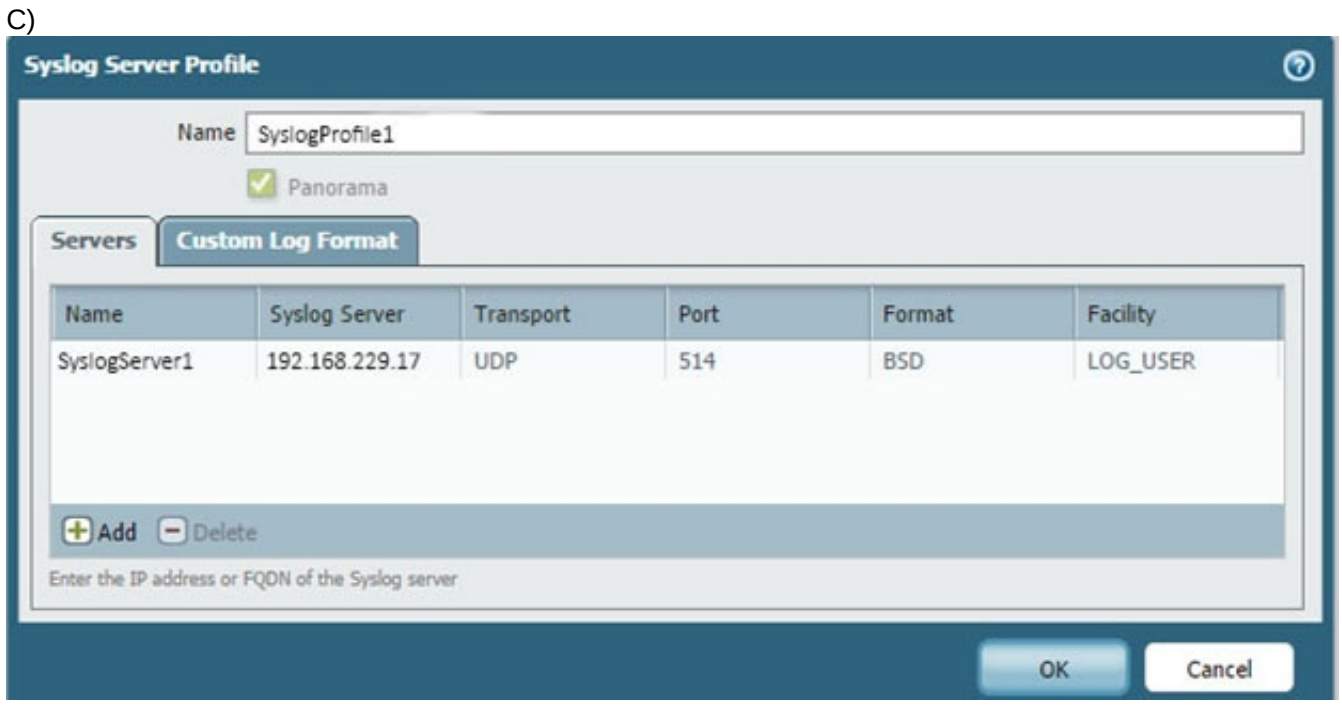
NEW QUESTION 185
- (Exam Topic 1)
An administrator cannot see any Traffic logs from the Palo Alto Networks NGFW in Panorama reports. The configuration problem seems to be on the firewall
Which settings, if configured incorrectly, most likely would stop only Traffic logs from being sent from the NGFW to Panorama?
A)



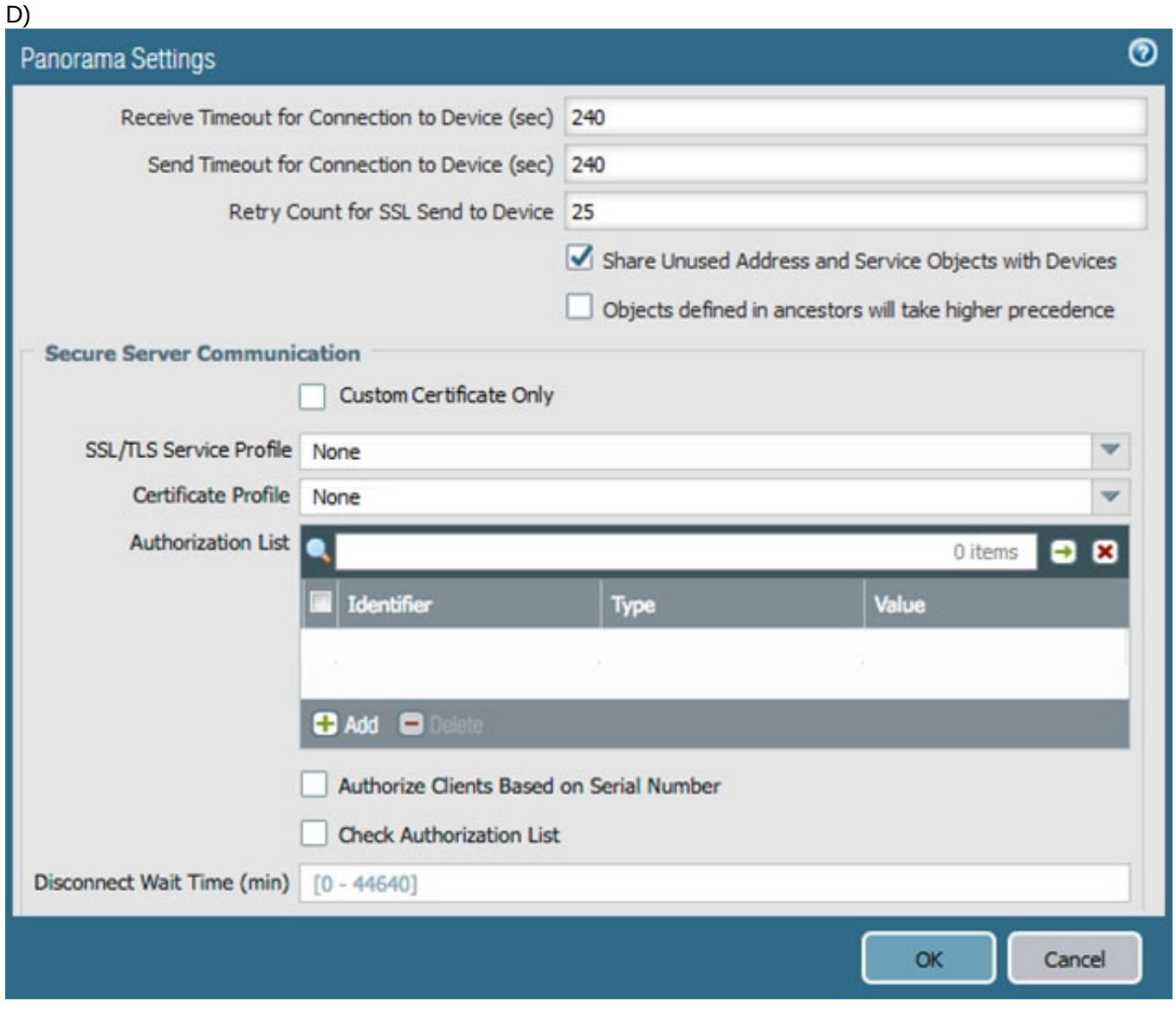
B)



C)



D)



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

D. Option D

Answer: B

NEW QUESTION 189
- (Exam Topic 1)
The SSL Forward Proxy decryption policy is configured. The following four certificate authority (CA) certificates are installed on the firewall.
An end-user visits the untrusted website https //www firewall-do-not-trust-website com

Which certificate authority (CA) certificate will be used to sign the untrusted webserver certificate?

A. Forward-Untrust-Certificate
B. Forward-Trust-Certificate
C. Firewall-CA
D. Firewall-Trusted-Root-CA

Answer: B

NEW QUESTION 194
- (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 199
- (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 202
- (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 205
- (Exam Topic 1)
An administrator is considering upgrading the Palo Alto Networks NGFW and central management Panorama version
What is considered best practice for this scenario?

A. Perform the Panorama and firewall upgrades simultaneously
B. Upgrade the firewall first wait at least 24 hours and then upgrade the Panorama version
C. Upgrade Panorama to a version at or above the target firewall version
D. Export the device state perform the update, and then import the device state

Answer: A

NEW QUESTION 207
- (Exam Topic 1)
An administrator wants to upgrade a firewall HA pair to PAN-OS 10.1 The firewalls are currently running PAN-OS 8.1.17.
Which upgrade path maintains synchronization of the HA session (and prevents network outage)?

A. Upgrade directly to the target major version

B. Upgrade one major version at a time
C. Upgrade the HA pair to a base image
D. Upgrade two major versions at a time

Answer: D

NEW QUESTION 211
- (Exam Topic 1)
A company needs to preconfigure firewalls to be sent to remote sites with the least amount of preconfiguration Once deployed each firewall must establish secure tunnels back to multiple regional data centers to include the future regional data centers
Which VPN preconfigured configuration would adapt to changes when deployed to the future site?

A. IPsec tunnels using IKEv2
B. PPTP tunnels
C. GlobalProtect satellite
D. GlobalProtect client

Answer: C

NEW QUESTION 213
- (Exam Topic 1)
Given the following configuration, which route is used for destination 10.10.0.4?

```
set network virtual-router 2 routing-table ip static-route "Route 1" nexthop ip-address
192.168.1.2
set network virtual-router 2 routing-table ip static-route "Route 1" metric 30
set network virtual-router 2 routing-table ip static-route "Route 1" destination
10.10.0.0/24
set network virtual-router 2 routing-table ip static-route "Route 1" route-table unicast
set network virtual-router 2 routing-table ip static-route "Route 2" nexthop ip-address
192.168.1.2
set network virtual-router 2 routing-table ip static-route "Route 2" metric 20
set network virtual-router 2 routing-table ip static-route "Route 2" destination
10.10.0.0/24
set network virtual-router 2 routing-table ip static-route "Route 2" route-table unicast
set network virtual-router 2 routing-table ip static-route "Route 3" nexthop ip-address
10.10.20.1
set network virtual-router 2 routing-table ip static-route "Route 3" metric 5
set network virtual-router 2 routing-table ip static-route "Route 3" destination 0.0.0.0/0
set network virtual-router 2 routing-table ip static-route "Route 3" route-table unicast
set network virtual-router 2 routing-table ip static-route "Route 4" nexthop ip-address
192.168.1.2
set network virtual-router 2 routing-table ip static-route "Route 4" metric 10
set network virtual-router 2 routing-table ip static-route "Route 4" destination
10.10.1.0/25
set network virtual-router 2 routing-table ip static-route "Route 4" route-table unicast
```

A. Route 4
B. Route 3
C. Route 1
D. Route 3

Answer: A

NEW QUESTION 218
- (Exam Topic 1)
When you configure an active/active high availability pair which two links can you use? (Choose two)

A. HA2 backup
B. HA3
C. Console Backup
D. HSCI-C

Answer: AC

NEW QUESTION 220
- (Exam Topic 1)
Which Panorama objects restrict administrative access to specific device-groups?

A. templates
B. admin roles
C. access domains
D. authentication profiles

Answer: C

NEW QUESTION 223
- (Exam Topic 1)
An administrator has 750 firewalls The administrator's central-management Panorama instance deploys dynamic updates to the firewalls
The administrator notices that the dynamic updates from Panorama do not appear on some of the firewalls If Panorama pushes the configuration of a dynamic update schedule to managed firewalls, but the
configuration does not appear what is the root cause?

A. Panorama has no connection to Palo Alto Networks update servers
B. Panorama does not have valid licenses to push the dynamic updates
C. No service route is configured on the firewalls to Palo Alto Networks update servers
D. Locally-defined dynamic update settings take precedence over the settings that Panorama pushed

Answer: D

NEW QUESTION 224
- (Exam Topic 2)
View the GlobalProtect configuration screen capture.

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-po the-globalprotect-client-authentication-configurations/define-the-globalprotect-agent-configurations
"Select this option to allow the GlobalProtect agent to determine if it is inside the enterprise network. This option applies only to endpoints that are configured to communicate with internal gateways.When the user attempts to log in, the agent does a reverse DNS lookup of an internal host using the specified Hostname to the specified IP Address. The host serves as a reference point that is reachable if the endpoint is inside the
enterprise network. If the agent finds the host, the endpoint is inside the network and the agent connects to an internal gateway; if the agent fails to find the internal host, the endpoint is outside the network and the agent establishes a tunnel to one of the external gateways"

NEW QUESTION 229
- (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 230
- (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 235
- (Exam Topic 2)
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: D

Explanation:
“By default, the firewall uses management interface to communicate to various servers including DNS, Email, Palo Alto Updates, User-ID agent, Syslog, Panorama etc. Service routes are used so that the communication between the firewall and servers go through the dataplane.”https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClGJCA0
“The firewall uses the service route to connect to the Update Server and checks for new content release versions and, if there are updates available, displays them at the top of the list.”https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-web-interface-help/device/device-dynamic-updates#

NEW QUESTION 239
- (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 244
- (Exam Topic 2)
A web server is hosted in the DMZ, and the server is configured to listen for incoming connections only on TCP port 8080. A Security policy rule allowing access from the Trust zone to the DMZ zone need to be configured to enable we browsing access to the server.
Which application and service need to be configured to allow only cleartext web-browsing traffic to thins server on tcp/8080.

A. application: web-browsing; service: application-default
B. application: web-browsing; service: service-https
C. application: ssl; service: any
D. application: web-browsing; service: (custom with destination TCP port 8080)

Answer: D

Explanation:
If you check in the FW the default port for web-browsing is TCP 80, so you will need a custom app. admin@PA-LAB-01# show predefined application web-browsing web-browsing { category general-internet; subcategory internet-utility; technology browser-based; analysis 'Web browsing continues to evolve. Initially used to simply view HTML formatted information, web browsers have become the client, through which, users can access new applications that provide functionality far beyond simple information browsing. These applications include web mail, instant messaging, streaming media, web conferencing, blogs, file sharing and other social networkingapplications. Much of the plain web-browsing activities has effectively been overshadowed by all the other applications. } default { port tcp/80; } tunnel-applications http-proxy; risk 4; } [edit]

NEW QUESTION 248
- (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 252
- (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 255
- (Exam Topic 2)
How can an administrator configure the NGFW to automatically quarantine a device using GlobalProtect?

A. by adding the device's Host ID to a quarantine list and configure GlobalProtect to prevent users fromconnecting to the GlobalProtect gateway from a quarantined device
B. by using secunty policies, log forwarding profiles, and log settings.
C. by exporting the list of quarantined devices to a pdf or csv file by selecting PDF/CSV at the bottom of the Device Quarantine page and leveraging the approbate XSOAR playbook
D. There is no native auto-quarantine feature so a custom script would need to be leveraged.

Answer: A

NEW QUESTION 257
- (Exam Topic 2)
An administrator wants to upgrade an NGFW from PAN-OS® 9.0 to PAN-OS® 10.0. The firewall is not a part of an HA pair. What needs to be updated first?

A. XML Agent
B. Applications and Threats
C. WildFire
D. PAN-OS® Upgrade Agent

Answer: B

Explanation:
https://www.paloaltonetworks.com/documentation/80/pan-os/newfeaturesguide/upgrade-to-pan-os-80/upgrade-t

NEW QUESTION 260
- (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

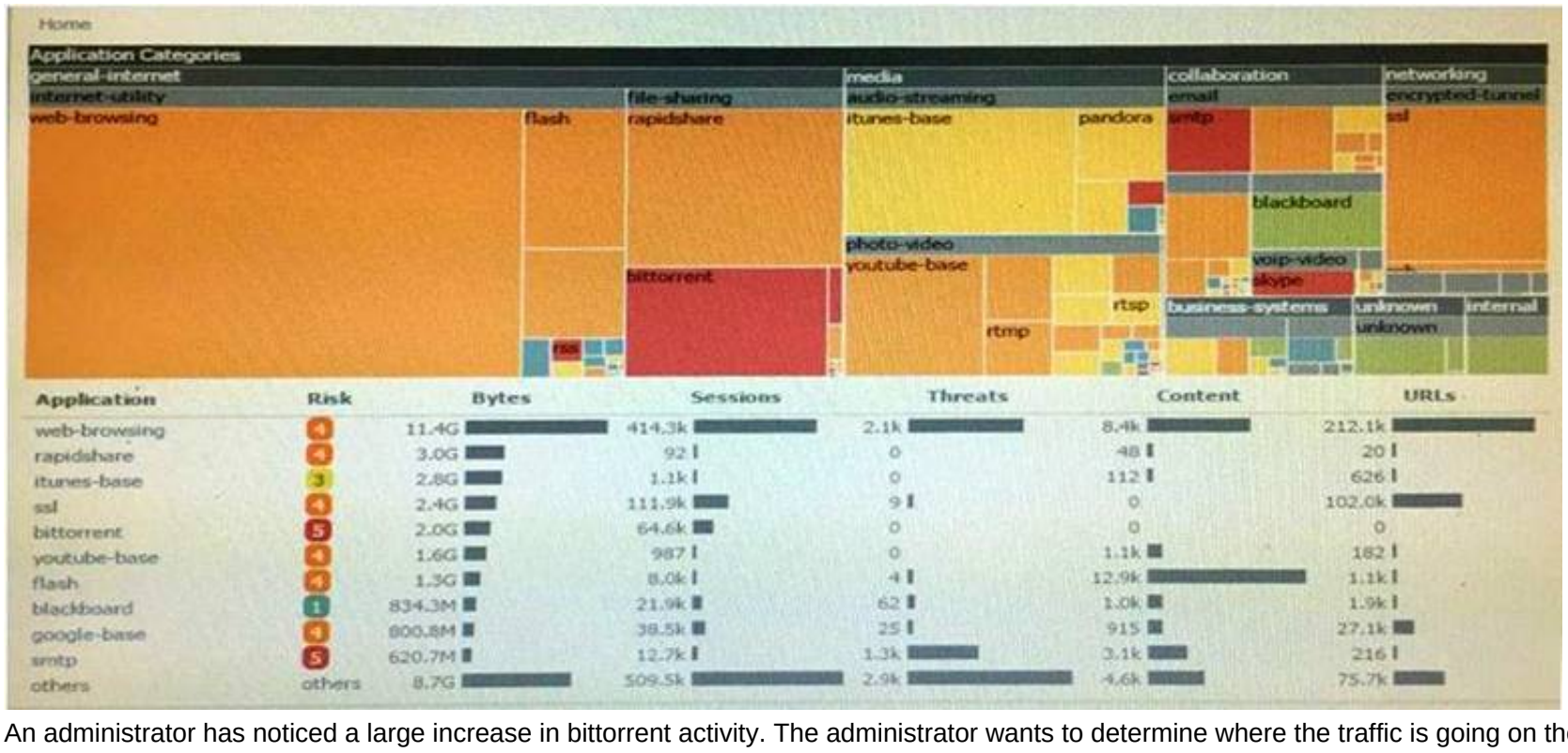
Answer: BDE

NEW QUESTION 264
- (Exam Topic 3)
Which two methods can be used to mitigate resource exhaustion of an application server? (Choose two)

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

Answer: BD

NEW QUESTION 269
- (Exam Topic 3)
Click the Exhibit button



An administrator has noticed a large increase in bittorrent activity. The administrator wants to determine where the traffic is going on the company.

What would be the administrator's next step?

A. Right-Click on the bittorrent link and select Value from the context menu
B. Create a global filter for bittorrent traffic and then view Traffic logs.
C. Create local filter for bittorrent traffic and then view Traffic logs.
D. Click on the bittorrent application link to view network activity

Answer: D

NEW QUESTION 271
- (Exam Topic 3)
Which Device Group option is assigned by default in Panorama whenever a new device group is created to manage a Firewall?

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

Answer: C

NEW QUESTION 273
- (Exam Topic 3)
During the packet flow process, which two processes are performed in application identification? (Choose two.)

A. pattern based application identification
B. application changed from content inspection
C. session application identified
D. application override policy match

Answer: AD

NEW QUESTION 277
- (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 280
- (Exam Topic 3)
A VPN connection is set up between Site-A and Site-B, but no traffic is passing in the system log of Site-A, there is an event logged as like-nego-p1-fail-psk.
What action will bring the VPN up and allow traffic to start passing between the sites?

A. Change the Site-B IKE Gateway profile version to match Site-A,
B. Change the Site-A IKE Gateway profile exchange mode to aggressive mode.
C. Enable NAT Traversal on the Site-A IKE Gateway profile.
D. Change the pre-shared key of Site-B to match the pre-shared key of Site-A

Answer: D

NEW QUESTION 281
- (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 285
- (Exam Topic 3)
Which command can be used to validate a Captive Portal policy?

A. eval captive-portal policy <criteria>
B. request cp-policy-eval <criteria>
C. test cp-policy-match <criteria>
D. debug cp-policy <criteria>

Answer: C

NEW QUESTION 289
- (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 294
- (Exam Topic 3)
Which setting allow a DOS protection profile to limit the maximum concurrent sessions from a source IP address?

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

Answer: C

NEW QUESTION 297
- (Exam Topic 3)
Which authentication source requires the installation of Palo Alto Networks software, other than PAN-OS 7x, to obtain a username-to-IP-address mapping?

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

Answer: B

NEW QUESTION 299
- (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 304
- (Exam Topic 3)
A company is upgrading its existing Palo Alto Networks firewall from version 7.0.1 to 7.0.4.
Which three methods can the firewall administrator use to install PAN-OS 8.0.4 across the enterprise?(Choose three)

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

Answer: ACF

NEW QUESTION 305
- (Exam Topic 3)
Which three rule types are available when defining policies in Panorama? (Choose three.)

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

Answer: ABC

Explanation:
https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/panorama-web-interface/defini

NEW QUESTION 307
- (Exam Topic 3)
A company.com wants to enable Application Override. Given the following screenshot:

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

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

Answer: AC

NEW QUESTION 311
- (Exam Topic 3)
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 316
- (Exam Topic 3)
A network security engineer is asked to perform a Return Merchandise Authorization (RMA) on a firewall Which part of files needs to be imported back into the replacement firewall that is using Panorama?

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

Answer: A

NEW QUESTION 320
- (Exam Topic 3)
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/deter

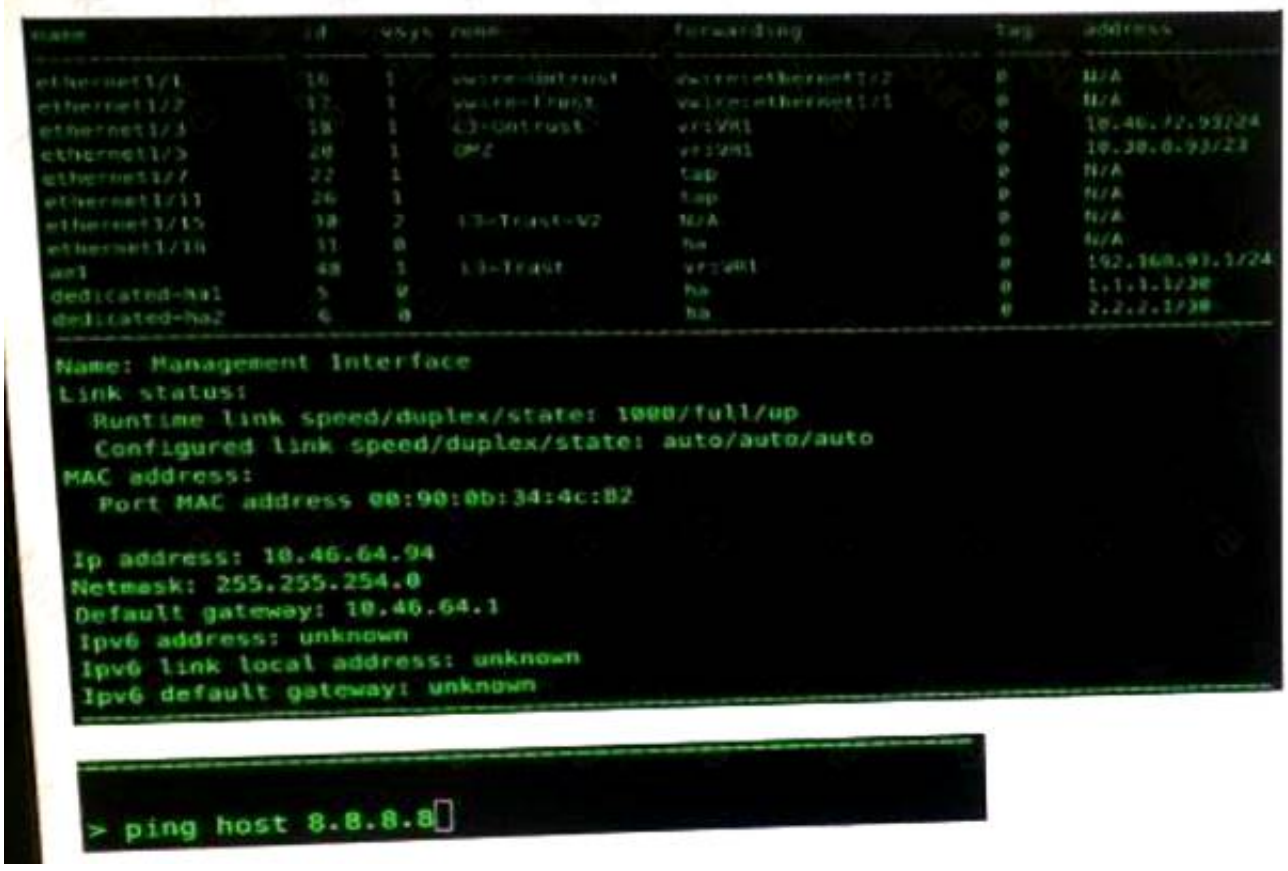
NEW QUESTION 322
- (Exam Topic 3)
In an enterprise deployment, a network security engineer wants to assign to a group of administrators without creating local administrator accounts on the firewall.
Which authentication method must be used?

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

Answer: D

NEW QUESTION 326
- (Exam Topic 3)

When performing the "ping" test shown in this CLI output



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 331
- (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 accoumplish 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 332
- (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 337
- (Exam Topic 3)
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 341
- (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 344
- (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 347
- (Exam Topic 3)
What can missing SSL packets when performing a packet capture on dataplane interfaces?

A. The packets are hardware offloaded to the offloaded processor on the dataplane
B. The missing packets are offloaded to the management plane CPU
C. The packets are not captured because they are encrypted
D. There is a hardware problem with offloading FPGA on the management plane

Answer: A

NEW QUESTION 349
- (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 353
- (Exam Topic 3)
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 355
- (Exam Topic 3)
Which operation will impact performance of the management plane?

A. DoS protection
B. WildFire submissions

C. generating a SaaS Application report
D. decrypting SSL sessions

Answer: C

NEW QUESTION 358
- (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 362
- (Exam Topic 3)
Which interface configuration will accept specific VLAN IDs?

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

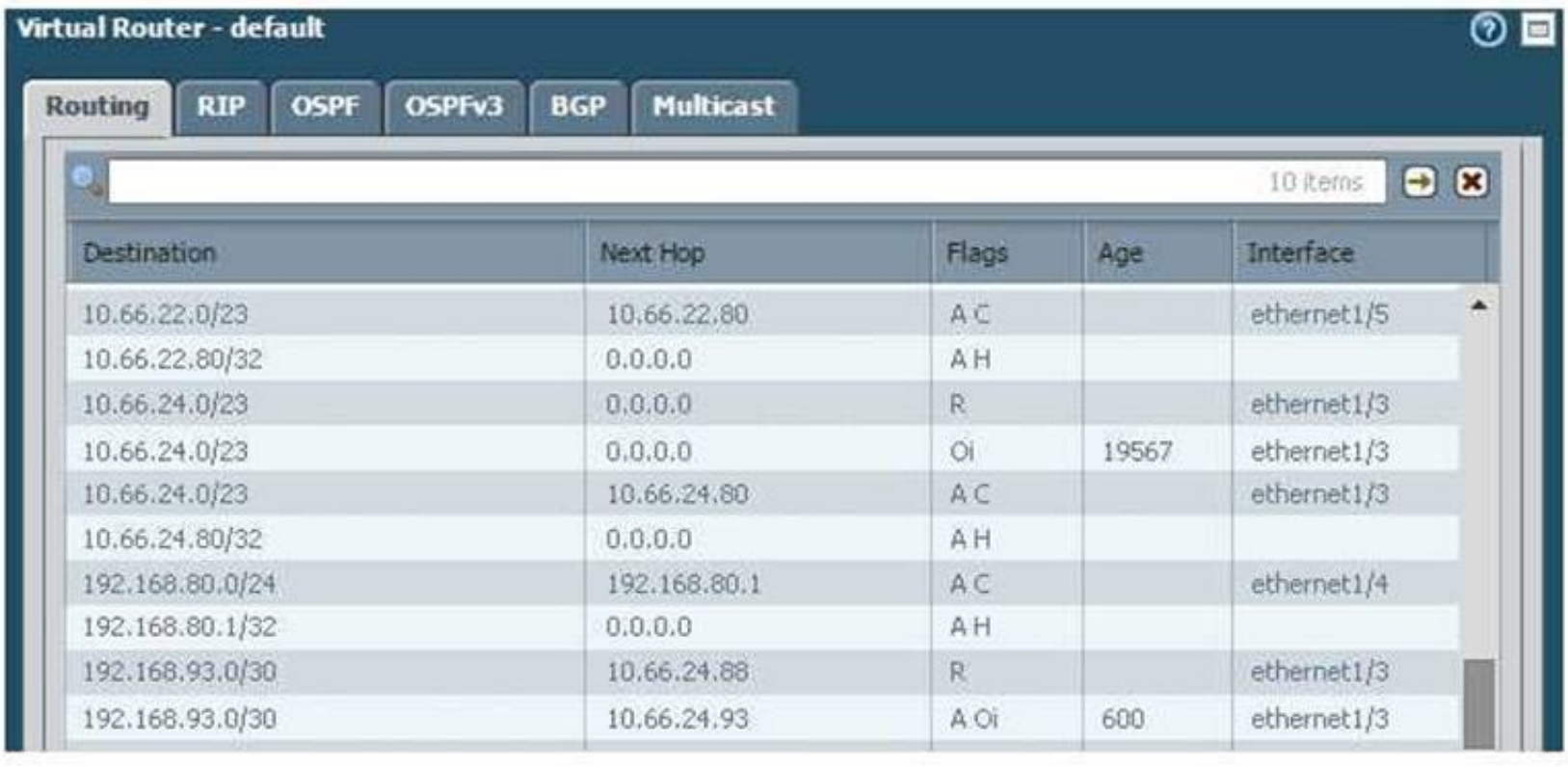
Answer: B

NEW QUESTION 363
- (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 367
- (Exam Topic 3)
Given the following table.



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

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

Answer: A

NEW QUESTION 372
- (Exam Topic 3)

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

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

Answer: ABE

NEW QUESTION 377
- (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 381
- (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 385
- (Exam Topic 3)
A company hosts a publicly accessible web server behind a Palo Alto Networks next-generation firewall with the following configuration information:
* Users outside the company are in the "Untrust-L3" zone.
* The web server physically resides in the "Trust-L3" zone.
* Web server public IP address: 23.54.6.10
* Web server private IP address: 192.168.1.10
Which two items must the NAT policy contain to allow users in the Untrust-L3 zone to access the web server? (Choose two.)

A. Destination IPof 23.54.6.10
B. UntrustL3 for both Source and Destination Zone
C. Destination IP of 192.168.1.10
D. UntrustL3 for Source Zone and Trust-L3 for Destination Zone

Answer: AB

NEW QUESTION 389
- (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 394
- (Exam Topic 3)
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 398
- (Exam Topic 3)
Which option is an IPv6 routing protocol?

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

Answer: B

NEW QUESTION 399
- (Exam Topic 3)
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 403
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

PCNSE Practice Exam Features:

* PCNSE Questions and Answers Updated Frequently

* PCNSE Practice Questions Verified by Expert Senior Certified Staff

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

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