Paloalto-Networks

Exam Questions PCNSE

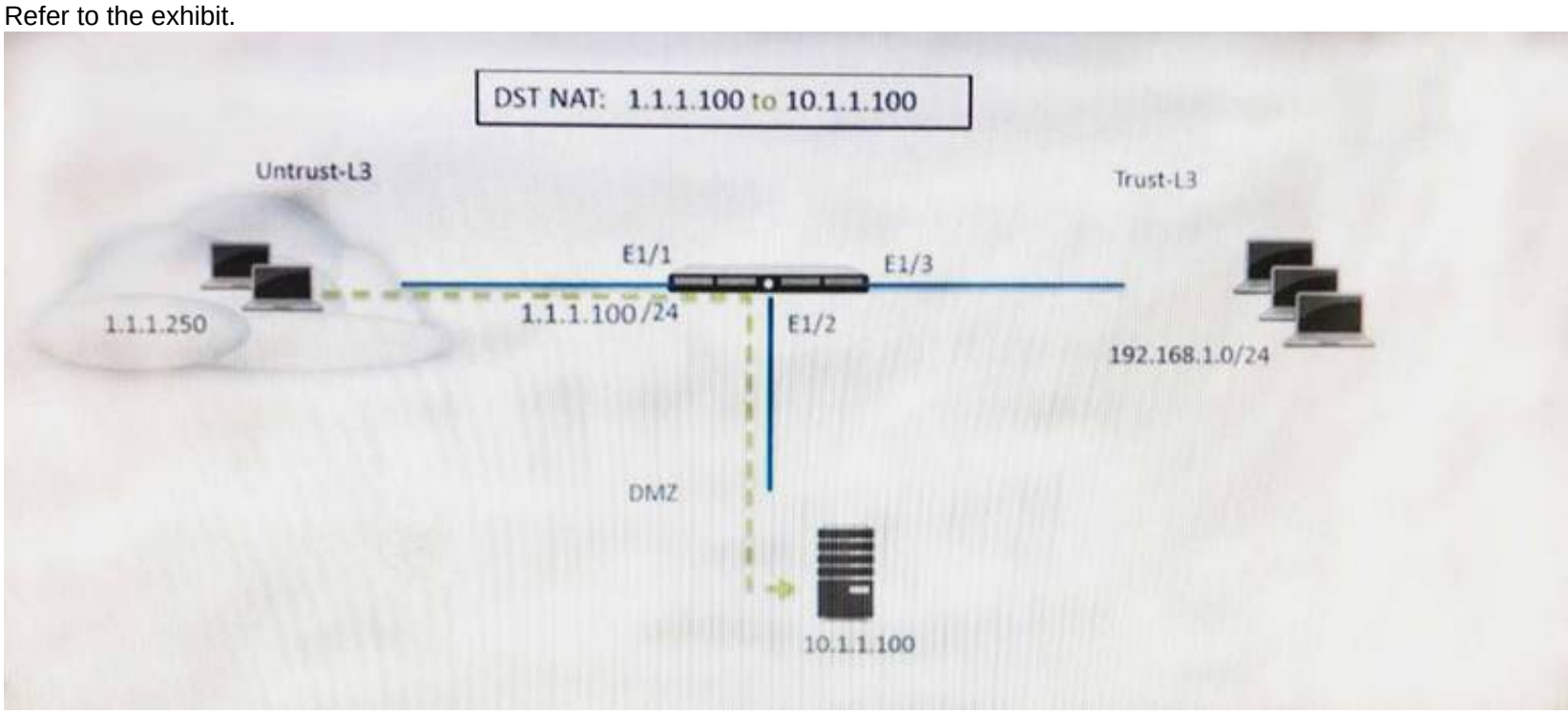
Palo Alto Networks Certified Security Engineer (PCNSE)PAN-OS 9.0

NEW QUESTION 1
- (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 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)
A global corporate office has a large-scale network with only one User-ID agent, which creates a bottleneck near the User-ID agent server. Which solution in PAN-OS® software would help in this case?

A. Application override
B. Redistribution of user mappings
C. Virtual Wire mode
D. Content inspection

Answer: B

Explanation:
https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/user-id/deploy-user-id-in-a-large-scale-network.ht

NEW QUESTION 4
- (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 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)
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 8
- (Exam Topic 2)
Which DoS protection mechanism detects and prevents session exhaustion attacks?

A. Packet Based Attack Protection
B. Flood Protection
C. Resource Protection
D. TCP Port Scan Protection

Answer: C

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

NEW QUESTION 9
- (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)
Which protection feature is available only in a Zone Protection Profile?

A. SYN Flood Protection using SYN Flood Cookies
B. ICMP Flood Protection

C. Port Scan Protection
D. UDP Flood Protections

Answer: A

Explanation:
https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-web-interface-help/network/network-network-profiles-zon

NEW QUESTION 10
- (Exam Topic 2)
To connect the Palo Alto Networks firewall to AutoFocus, which setting must be enabled?

A. Device>Setup>Services>AutoFocus
B. Device> Setup>Management >AutoFocus
C. AutoFocus is enabled by default on the Palo Alto Networks NGFW
D. Device>Setup>WildFire>AutoFocus
E. Device>Setup> Management> Logging and Reporting Settings

Answer: B

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

NEW QUESTION 12
- (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 15
- (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 20
- (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 25
- (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 29
- (Exam Topic 2)
Which item enables a firewall administrator to see details about traffic that is currently active through the NGFW?

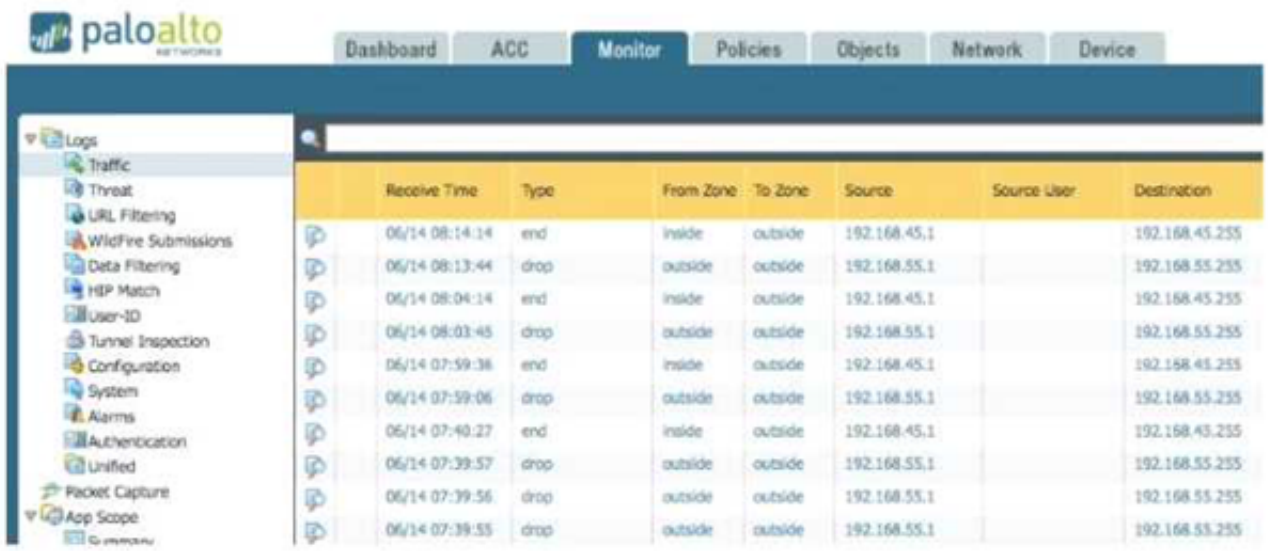
A. ACC
B. System Logs
C. App Scope
D. Session Browser

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)
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 37
- (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 42
- (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 44
- (Exam Topic 2)
SAML SLO is supported for which two firewall features? (Choose two.)

A. GlobalProtect Portal
B. CaptivePortal
C. WebUI
D. CLI

Answer: AB

NEW QUESTION 46
- (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)
How does Panorama prompt VMWare NSX to quarantine an infected VM?

A. HTTP Server Profile
B. Syslog Server Profile
C. Email Server Profile
D. SNMP Server Profile

Answer: A

NEW QUESTION 54
- (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 57
- (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 59
- (Exam Topic 2)
An administrator logs in to the Palo Alto Networks NGFW and reports that the WebUI is missing the Policies tab. Which profile is the cause of the missing Policies tab?

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

Answer: A

NEW QUESTION 61
- (Exam Topic 2)
A Palo Alto Networks NGFW just submitted a file to WildFire for analysis. Assume a 5-minute window for analysis. The firewall is configured to check for verdicts every 5 minutes.
How quickly will the firewall receive back a verdict?

A. More than 15 minutes
B. 5 minutes
C. 10 to 15 minutes
D. 5 to 10 minutes

Answer: D

NEW QUESTION 64
- (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 65
- (Exam Topic 2)
Which three options are supported in HA Lite? (Choose three.)

A. Virtual link
B. Active/passive deployment
C. Synchronization of IPsec security associations
D. Configuration synchronization
E. Session synchronization

Answer: BCD

Explanation:
“The PA-200 firewall supports HA Lite only. HA Lite is an active/passive deployment that provides configuration synchronization and some runtime data synchronization such as IPSec security associations. It does not support any session synchronization (HA2), and therefore does not offer stateful failover.”
Reference:
https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/device/device-high-availability

NEW QUESTION 70
- (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 73
- (Exam Topic 2)
The firewall determines if a packet is the first packet of a new session or if a packet is part of an existing session using which kind of match?

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

Answer: A

Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClVECA0

NEW QUESTION 74
- (Exam Topic 2)
A Security policy rule is configured with a Vulnerability Protection Profile and an action of ‘Deny”. Which action will this cause configuration on the matched traffic?

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

Answer: D

Explanation:
“Security profiles are not used in the match criteria of a traffic flow. The security profile is applied to scan traffic after the application or category is allowed by the security policy.”
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/policy/security-profiles.html#

NEW QUESTION 79
- (Exam Topic 2)
When is the content inspection performed in the packet flow process?

A. after the application has been identified
B. before session lookup
C. before the packet forwarding process

D. after the SSL Proxy re-encrypts the packet

Answer: A

Explanation:
Reference:
https://live.paloaltonetworks.com/t5/Learning-Articles/Packet-Flow-Sequence-in-PAN-OS/ta-p/56081

NEW QUESTION 84
- (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 88
- (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 93
- (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 95
- (Exam Topic 2)
ESTION NO: 94
If an administrator wants to decrypt SMTP traffic and possesses the server’s certificate, which SSL decryption mode will allow the Palo Alto Networks NGFW to inspect traffic to the server?

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

Answer: B

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

NEW QUESTION 97
- (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 102
- (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 104
- (Exam Topic 2)
Which option enables a Palo Alto Networks NGFW administrator to schedule Application and Threat updates while applying only new content-IDs to traffic?

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

Answer: C

NEW QUESTION 108
- (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 111
- (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 113
- (Exam Topic 2)
Which three split tunnel methods are supported by a globalProtect gateway? (Choose three.)

A. video streaming application

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

Answer: ABC

NEW QUESTION 116
- (Exam Topic 2)
In a virtual router, which object contains all potential routes?

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

Answer: B

Explanation:
https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/networking/virtual-routers

NEW QUESTION 117
- (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 121
- (Exam Topic 2)
Which three file types can be forwarded to WildFire for analysis as a part of the basic WildFire service? (Choose three.)

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

Answer: DEF

Explanation:
https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-admin/getting-started/enable-basic-wildfire-forwarding

NEW QUESTION 125
- (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 127
- (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 128
- (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 131
- (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

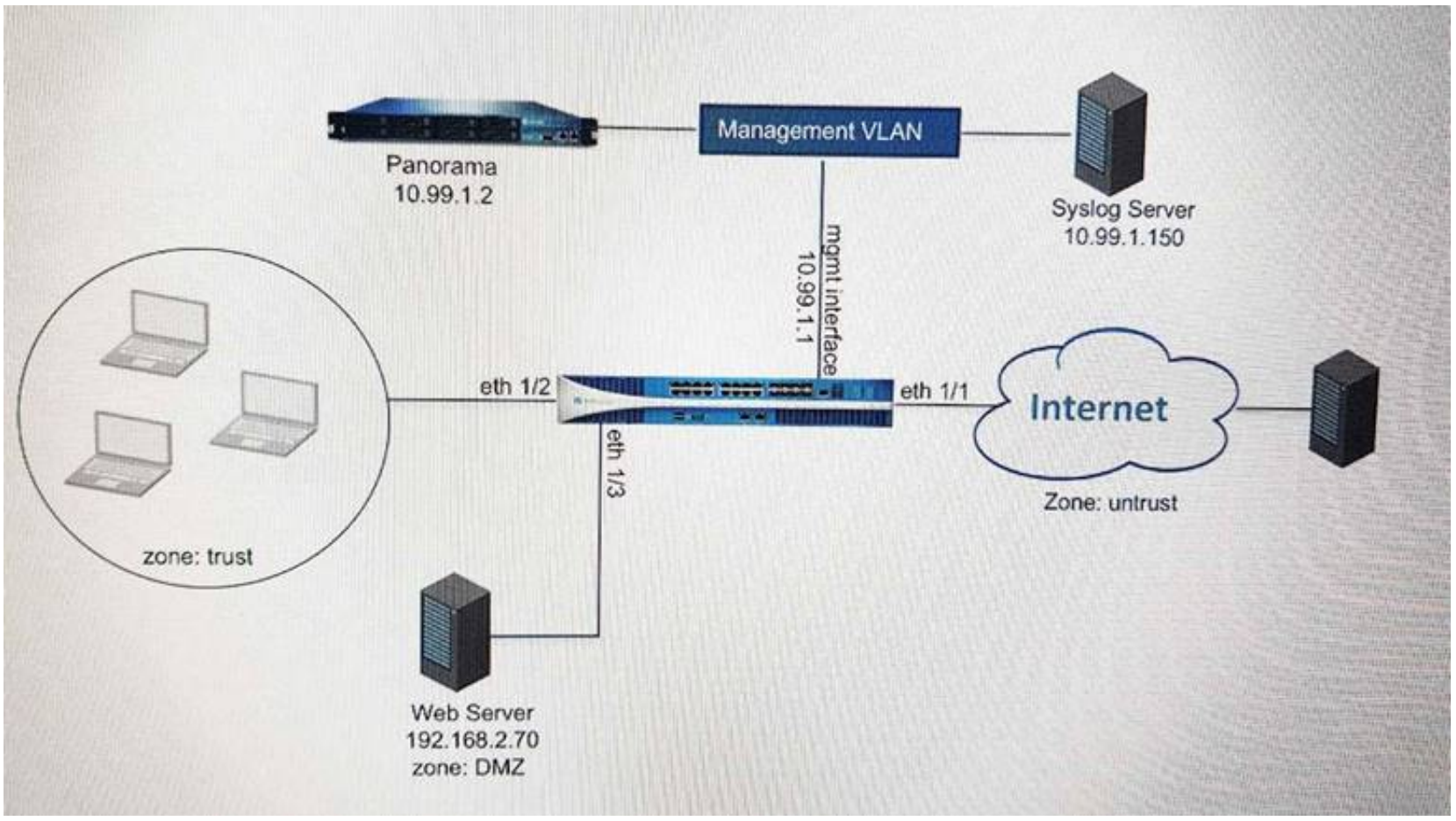
NEW QUESTION 134
- (Exam Topic 2)
When configuring a GlobalProtect Portal, what is the purpose of specifying an Authentication Profile?

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

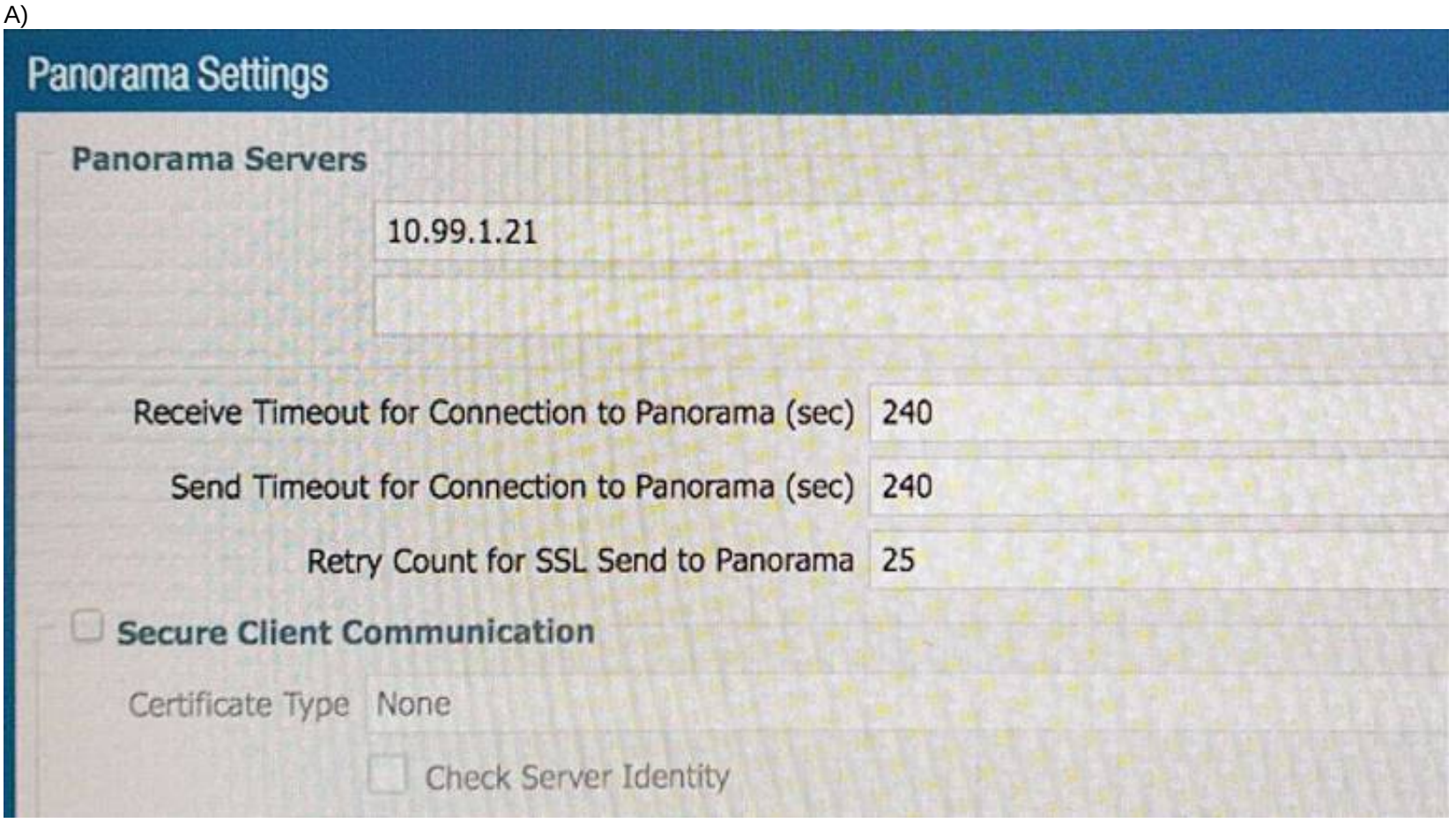
Explanation:
The additional options of Browser and Satellite enable you to specify the authentication profile to use for specific scenarios. Select Browser to specify the authentication profile to use to authenticate a user accessing the portal from a web browser with the intent of downloading the GlobalProtect 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 139
- (Exam Topic 2)
Refer to the exhibit.

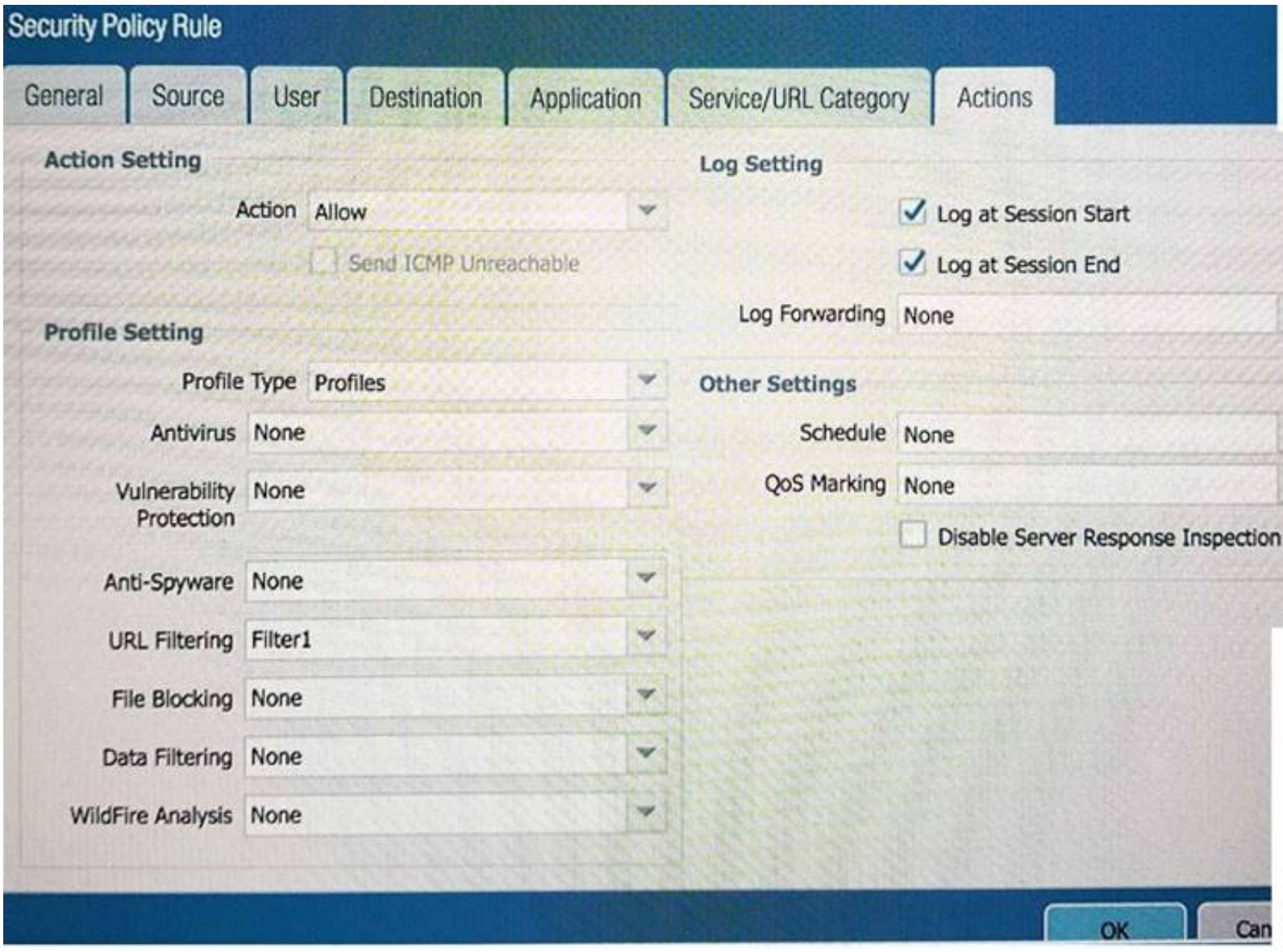


An administrator cannot see any of the Traffic logs from the Palo Alto Networks NGFW on Panorama. The configuration problem seems to be on the firewall side. Where is the best place on the Palo Alto Networks NGFW to check whether the configuration is correct?

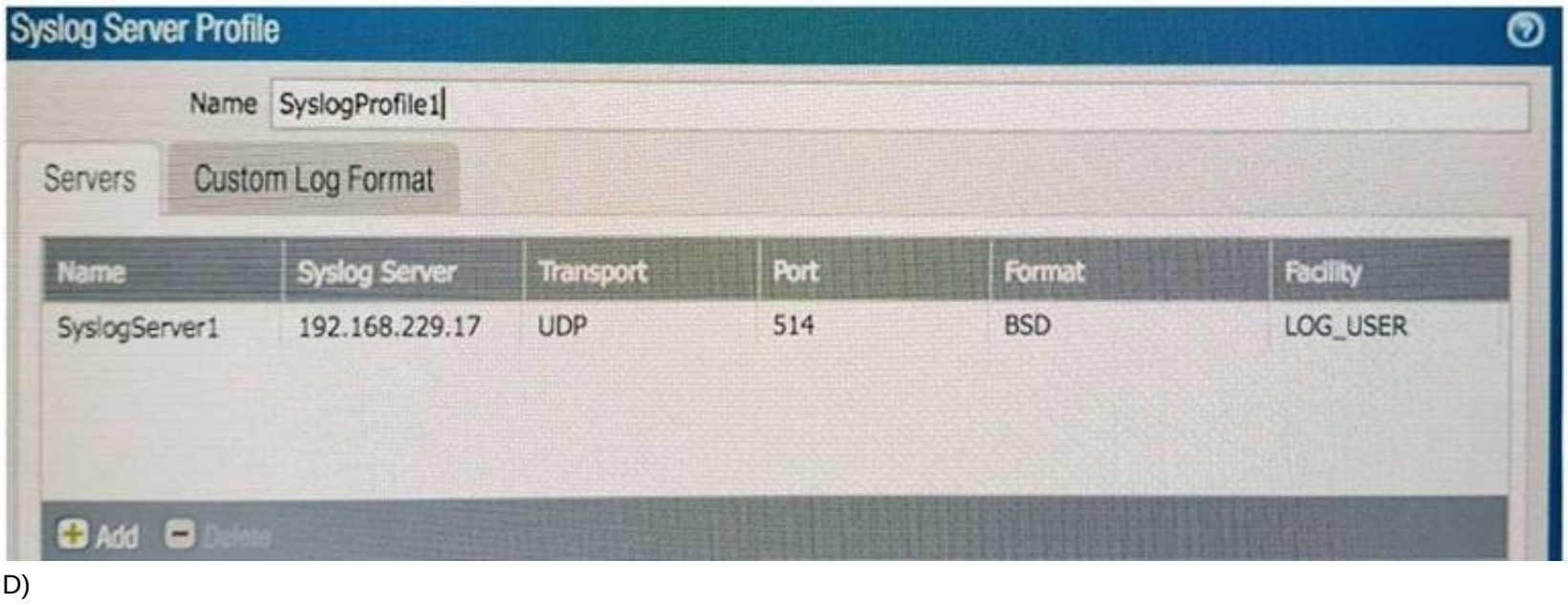
A)



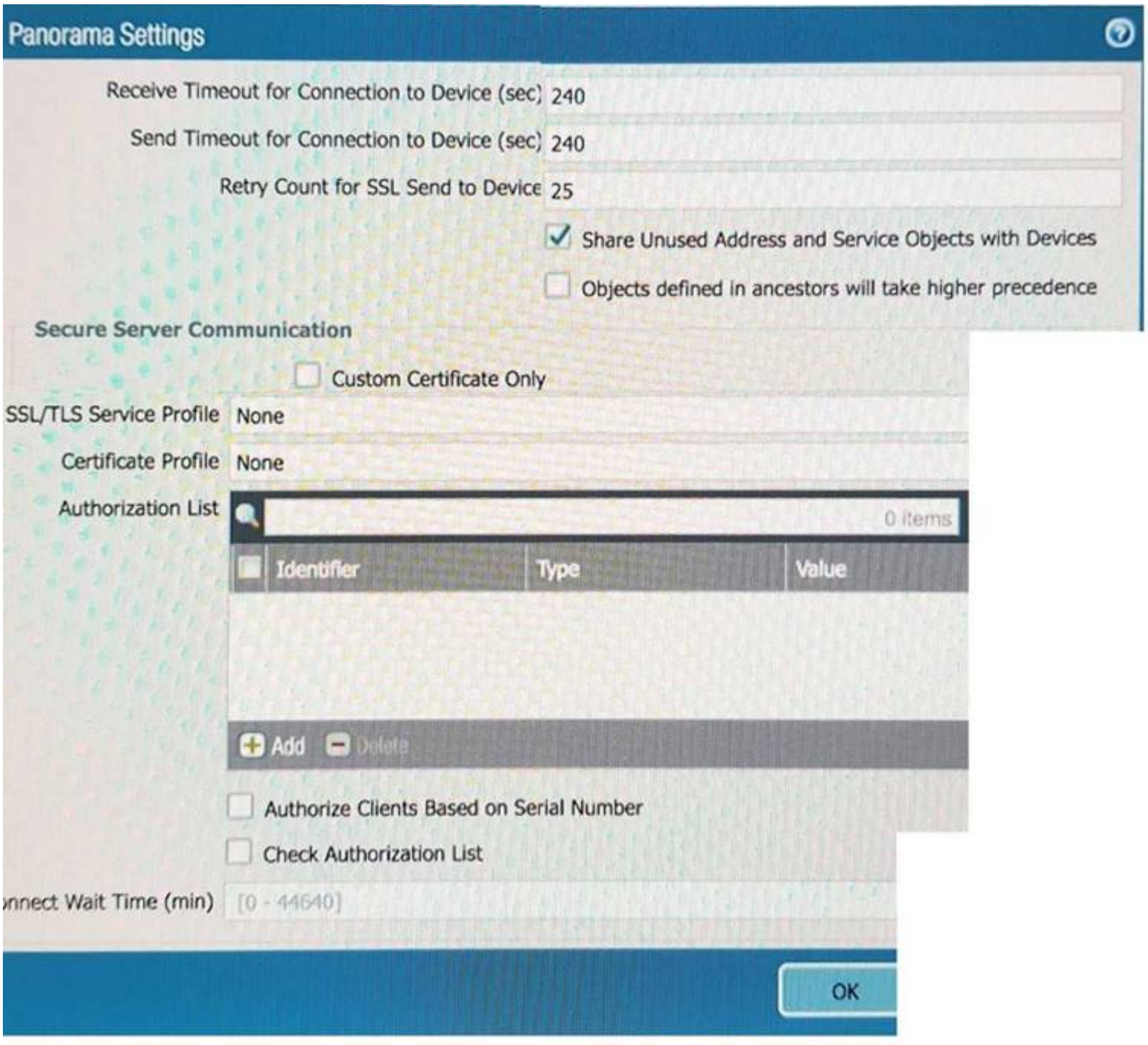
B)


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 144
- (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 147
- (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 148
- (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

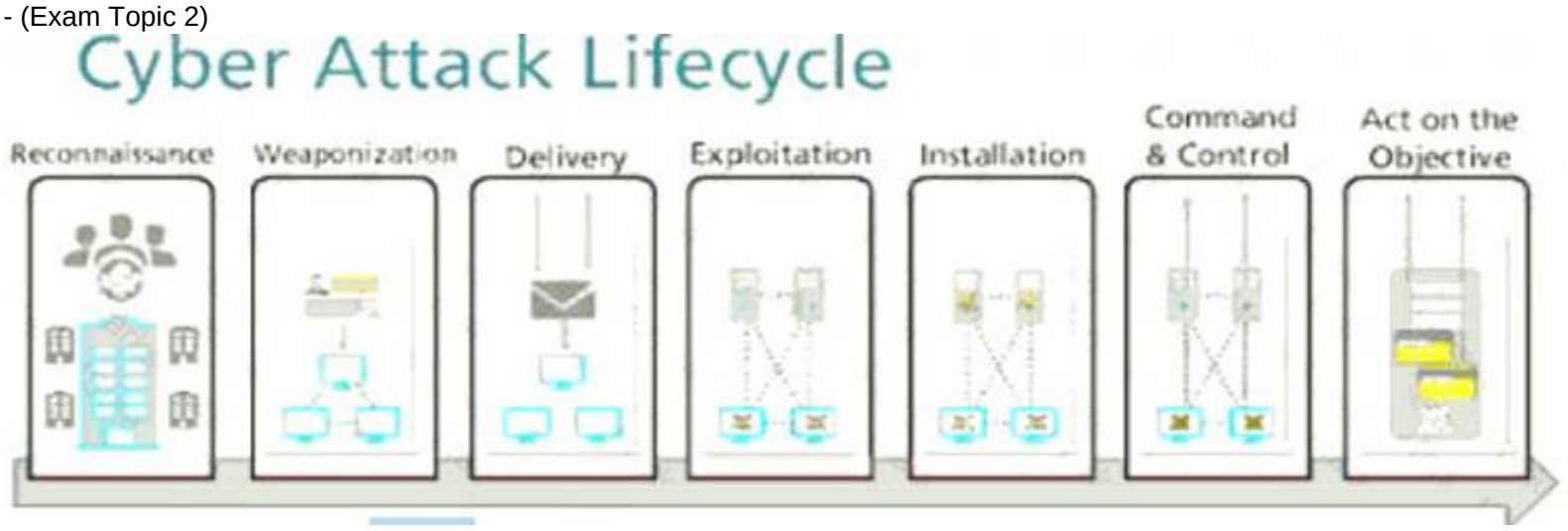
NEW QUESTION 151
- (Exam Topic 2)
Decrypted packets from the website https://www.microsoft.com will appear as which application and service within the Traffic log?

A. web-browsing and 443
B. SSL and 80
C. SSL and 443
D. web-browsing and 80

Answer: A

Explanation:
We know that SSL decryption is supposed to give us visibility of traffic that would otherwise be encrypted. Therefore, we'd expect decrypted traffic to be identified as the underlying applications, such as web-browsing, facebook-base or other, but not as SSL.
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CmdLCAS

NEW QUESTION 153
- (Exam Topic 2)



At which stage of the cyber-attack lifecycle would the attacker attach an infected PDF file to an email?

A. exploitation
B. IP command and control
C. delivery
D. reconnaissance

Answer: D

NEW QUESTION 154
- (Exam Topic 2)
Which feature can provide NGFWs with User-ID mapping information?

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

Answer: A

NEW QUESTION 159

- (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 161
- (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 165
- (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 167
- (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 168
- (Exam Topic 2)
An administrator using an enterprise PKI needs to establish a unique chain of trust to ensure mutual authentication between Panorama and the managed firewalls and Log Collectors.
How would the administrator establish the chain of trust?

A. Use custom certificates
B. Enable LDAP or RADIUS integration
C. Set up multi-factor authentication
D. Configure strong password authentication

Answer: A

Explanation:
Reference:
https://www.paloaltonetworks.com/documentation/80/panorama/panorama_adminguide/panorama-overview/pla panorama-deployment

NEW QUESTION 172
- (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 175
- (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 180
- (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 183
- (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

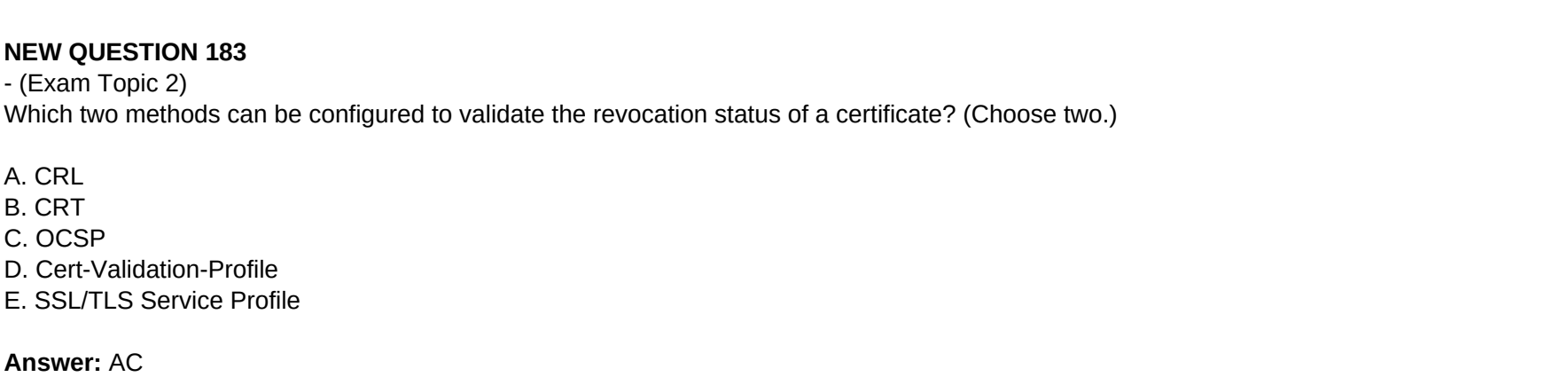
Answer: AC

NEW QUESTION 188
- (Exam Topic 1)
An administrator needs to gather information about the CPU utilization on both the management plane and the data plane
Where does the administrator view the desired data?

A. Monitor > Utilization
B. Resources Widget on the Dashboard
C. Support > Resources
D. Application Command and Control Center

Answer: A

NEW QUESTION 189
- (Exam Topic 1)
Refer to the exhibit.

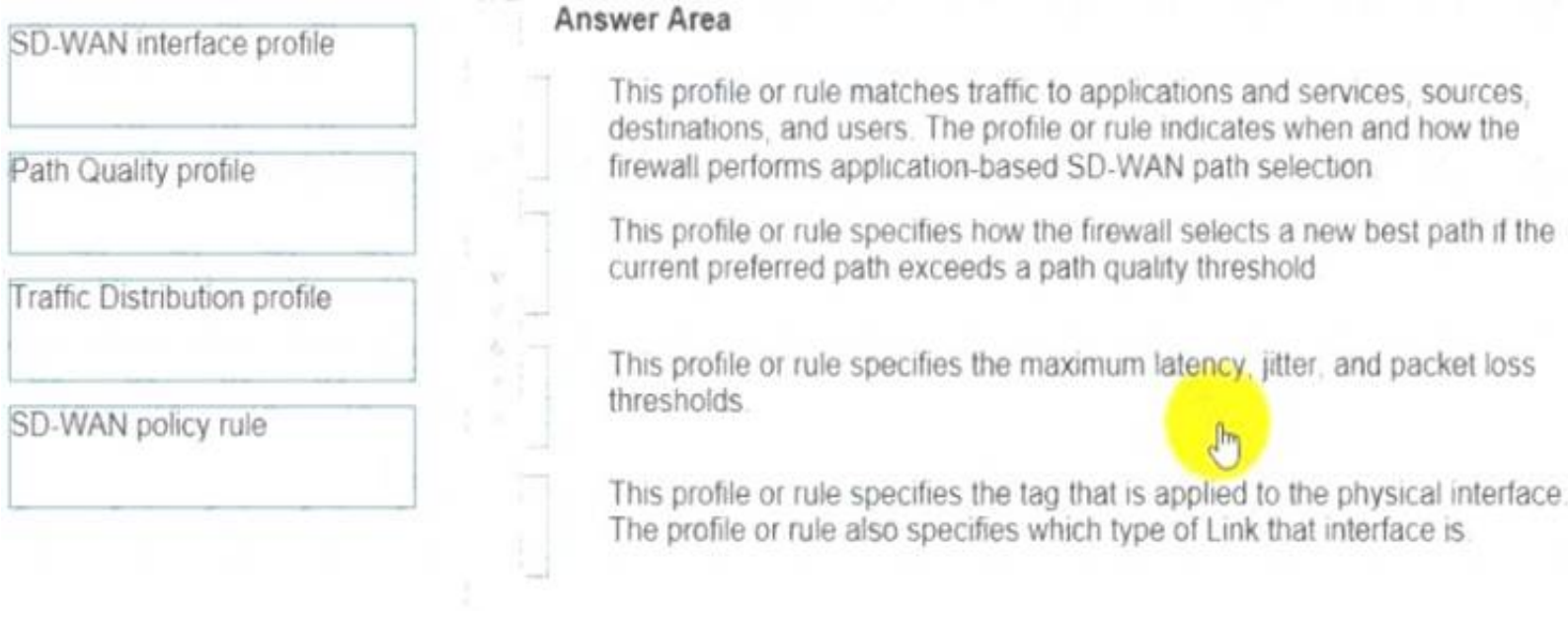


Which certificate can be used as the Forward Trust certificate?

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

Answer: D

NEW QUESTION 191
- (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

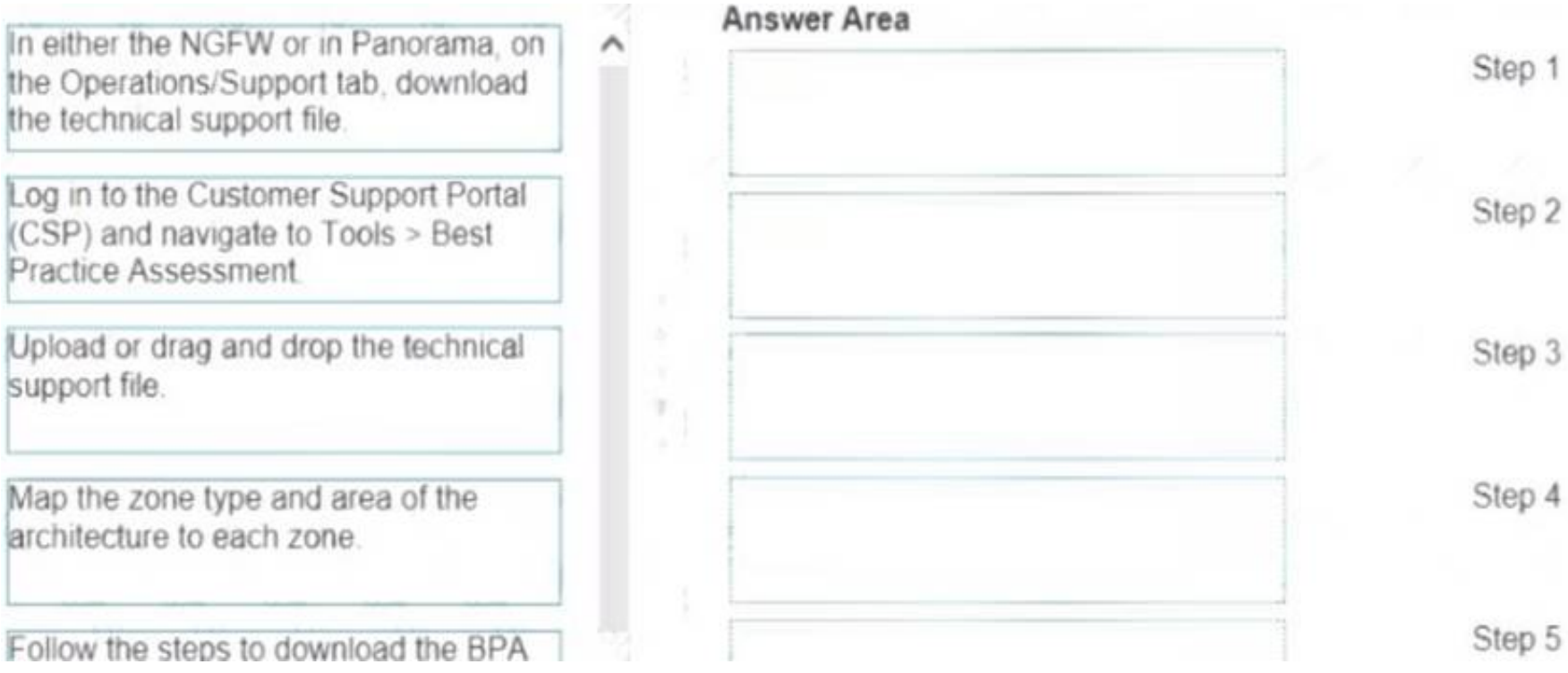
NEW QUESTION 193
- (Exam Topic 1)
A variable name must start with which symbol?

A. $
B. &
C. !
D. #

Answer: A

Explanation:
https://docs.paloaltonetworks.com/panorama/8-1/panorama-admin/manage-firewalls/manage-templates-and-tem

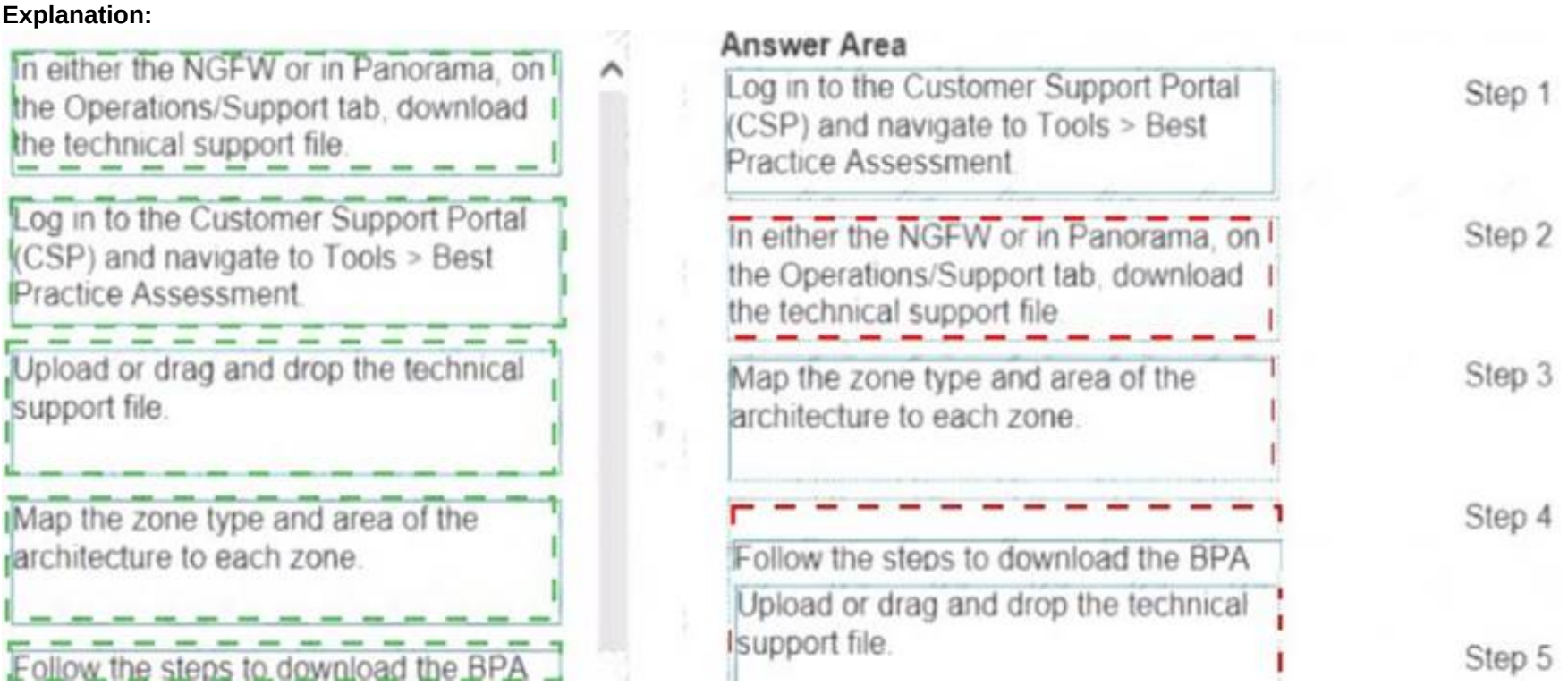
NEW QUESTION 196
- (Exam Topic 1)
Below are the steps in the workflow for creating a Best Practice Assessment in a firewall and Panorama configuration Place the steps in order.



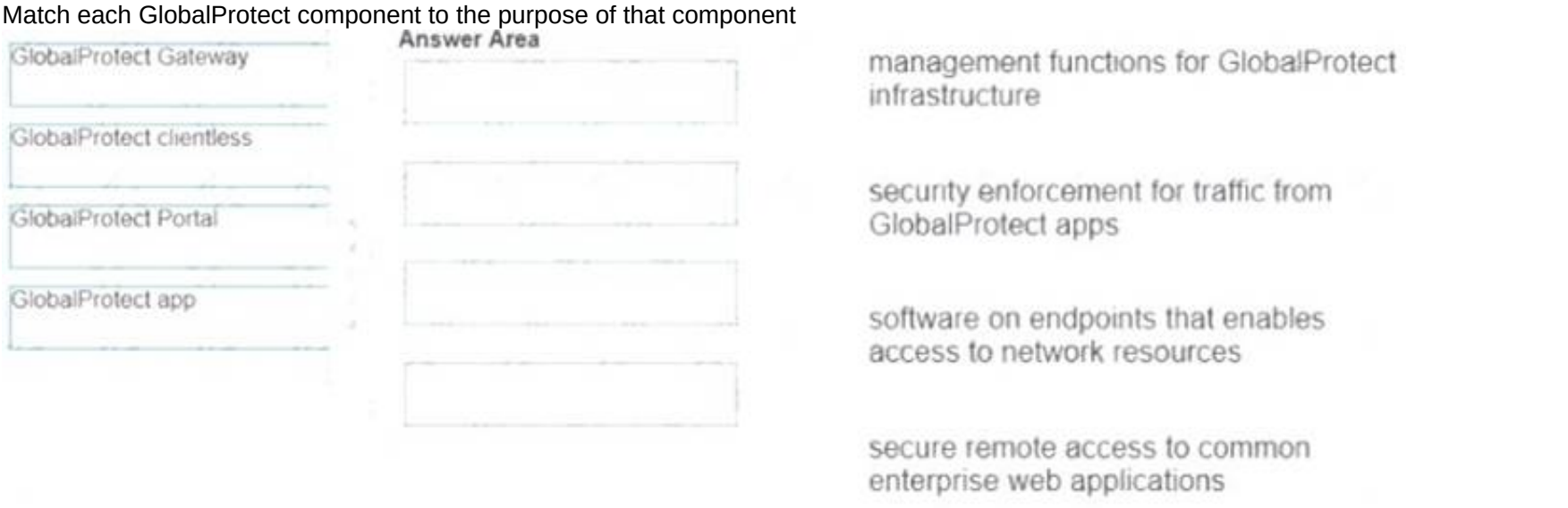
A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 199
- (Exam Topic 1)
Match each GlobalProtect component to the purpose of that component



A. Mastered
B. Not Mastered

Answer: A

Explanation:
The GlobalProtect portal provides the management functions for your GlobalProtect infrastructure The GlobalProtect gateways provide security enforcement for traffic from GlobalProtect apps
The GlobalProtect app software runs on endpoints and enables access to your network resources

NEW QUESTION 203
- (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 205
- (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 207
- (Exam Topic 1)
An organization is building a Bootstrap Package to deploy Palo Alto Networks VM-Series firewalls into their AWS tenant Which two statements are correct regarding the bootstrap package contents? (Choose two)

A. The /config /content and /software folders are mandatory while the /license and /plugin folders are optional
B. The bootstrap package is stored on an AFS share or a discrete container file bucket
C. The directory structure must include a /config /content, /software and /license folders
D. The init-cfg txt and bootstrap.xml files are both optional configuration items for the /config folder
E. The bootstrap xml file allows for automated deployment of VM-Senes firewalls with full network and policy configurations.

Answer: DE

NEW QUESTION 210
- (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 213
- (Exam Topic 1)
During SSL decryption which three factors affect resource consumption1? (Choose three)

A. TLS protocol version
B. transaction size
C. key exchange algorithm
D. applications that use non-standard ports
E. certificate issuer

Answer: ABC

Explanation:
https://docs.paloaltonetworks.com/best-practices/8-1/decryption-best-practices/decryption-best-practices/plan-ss

NEW QUESTION 216
- (Exam Topic 1)
Which User-ID mapping method should be used in a high-security environment where all IP address-to-user mappings should always be explicitly known?

A. PAN-OS integrated User-ID agent
B. LDAP Server Profile configuration
C. GlobalProtect
D. Windows-based User-ID agent

Answer: A

NEW QUESTION 219
- (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 223
- (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 227
- (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 231
- (Exam Topic 1)
What are two characteristic types that can be defined for a variable? (Choose two)

A. zone
B. FQDN
C. path group
D. IP netmask

Answer: BD

Explanation:
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface-help/panorama-web-interface/panorama-tem

NEW QUESTION 232
- (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 236

- (Exam Topic 1)
The UDP-4501 protocol-port is used between which two GlobalProtect components?

A. GlobalProtect app and GlobalProtect gateway
B. GlobalProtect portal and GlobalProtect gateway
C. GlobalProtect app and GlobalProtect satellite
D. GlobalProtect app and GlobalProtect portal

Answer: A

NEW QUESTION 237
- (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 239
- (Exam Topic 1)
In a security-first network what is the recommended threshold value for content updates to be dynamically updated?

A. 1 to 4 hours
B. 6 to 12 hours
C. 24 hours
D. 36 hours

Answer: B

Explanation:
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/threat-prevention/best-practices-for-content-and-thr

NEW QUESTION 242
- (Exam Topic 1)
What are three valid qualifiers for a Decryption Policy Rule match? (Choose three)

A. Destination Zone
B. App-ID
C. Custom URL Category
D. User-ID
E. Source Interface

Answer: ADE

NEW QUESTION 243
- (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 244
- (Exam Topic 1)
An engineer is planning an SSL decryption implementation
Which of the following statements is a best practice for SSL decryption?

A. Obtain an enterprise CA-signed certificate for the Forward Trust certificate
B. Obtain a certificate from a publicly trusted root CA for the Forward Trust certificate
C. Use an enterprise CA-signed certificate for the Forward Untrust certificate
D. Use the same Forward Trust certificate on all firewalls in the network

Answer: D

NEW QUESTION 246
- (Exam Topic 1)
Which rule type controls end user SSL traffic to external websites?

A. SSL Outbound Proxyless Inspection
B. SSL Forward Proxy
C. SSL Inbound Inspection
D. SSH Proxy

Answer: C

NEW QUESTION 251
- (Exam Topic 1)
When you import the configuration of an HA pair into Panorama, how do you prevent the import from affecting ongoing traffic?

A. Disable HA
B. Disable the HA2 link
C. Disable config sync
D. Set the passive link state to 'shutdown.

Answer: C

NEW QUESTION 255
- (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

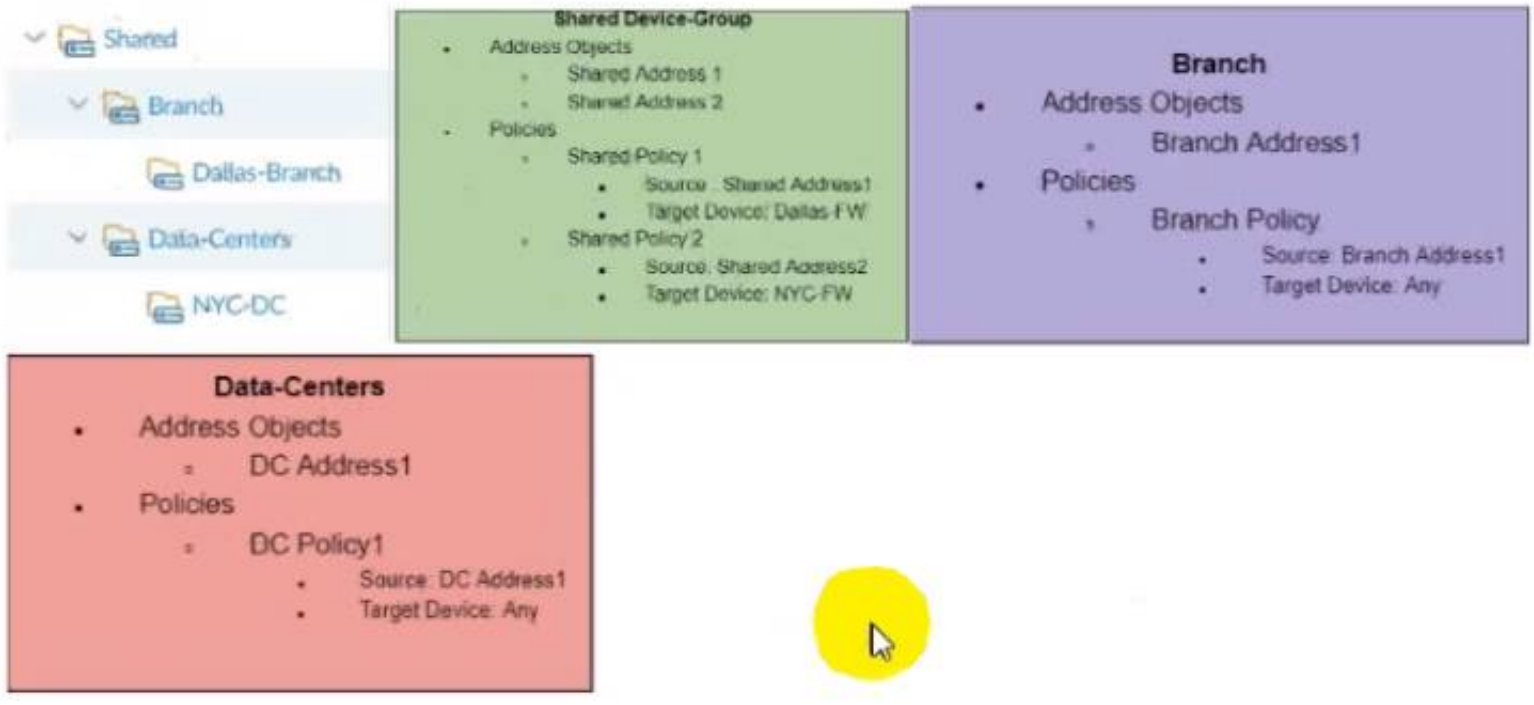
NEW QUESTION 260
- (Exam Topic 1)
Which value in the Application column indicates UDP traffic that did not match an App-ID signature?

A. not-applicable
B. incomplete
C. unknown-ip
D. unknown-udp

Answer: D

Explanation:
To safely enable applications you must classify all traffic, across all ports, all the time. With App-ID, the only applications that are typically classified as unknown traffic—tcp, udp or non-syn-tcp—in the ACC and the Traffic logs are commercially available applications that have not yet been added to App-ID, internal or custom applications on your network, or potential threats.
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/app-id/use-application-objects-in-policy/create-a-cu

NEW QUESTION 264
- (Exam Topic 1)
The following objects and policies are defined in a device group hierarchy



Dallas-Branch has **Dallas-FW** as a member of the **Dallas-Branch device-group**
NYC-DC has **NYC-FW** as a member of the **NYC-DC device-group**
What objects and policies will the **Dallas-FW** receive if "Share Unused Address and Service Objects" is enabled in Panorama?

A)
Address Objects
-Shared Address1
-Shared Address2
-Branch Address1
Policies
-Shared Policy1
-Branch Policy1

B)

Address Objects
-Shared Address1
-Shared Address2
-Branch Address1
-DC Address1
Policies
-Shared Policy1
-Shared Policy2
-Branch Policy1

C)
Address Objects
-Shared Address 1
-Branch Address2 Policies -Shared Polic1 l -Branch Policyl
D)
Address Objects -Shared Addressl -Shared Address2 -Branch Addressl Policies -Shared Policyl -Shared Policy2 -Branch Policyl

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

Answer: A

NEW QUESTION 265
- (Exam Topic 1)
Which three statements accurately describe Decryption Mirror? (Choose three.)

A. Decryption Mirror requires a tap interface on the firewall
B. Decryption, storage, inspection and use of SSL traffic are regulated in certain countries
C. Only management consent is required to use the Decryption Mirror feature
D. You should consult with your corporate counsel before activating and using Decryption Mirror in a production environment
E. Use of Decryption Mirror might enable malicious users with administrative access to the firewall to harvest sensitive information that is submitted via an encrypted channel

Answer: ABC

NEW QUESTION 269
- (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 271
- (Exam Topic 1)
Which action disables Zero Touch Provisioning (ZTP) functionality on a ZTP firewall during the onboarding process?

A. performing a local firewall commit
B. removing the firewall as a managed device in Panorama
C. performing a factory reset of the firewall
D. removing the Panorama serial number from the ZTP service

Answer: D

NEW QUESTION 272
- (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

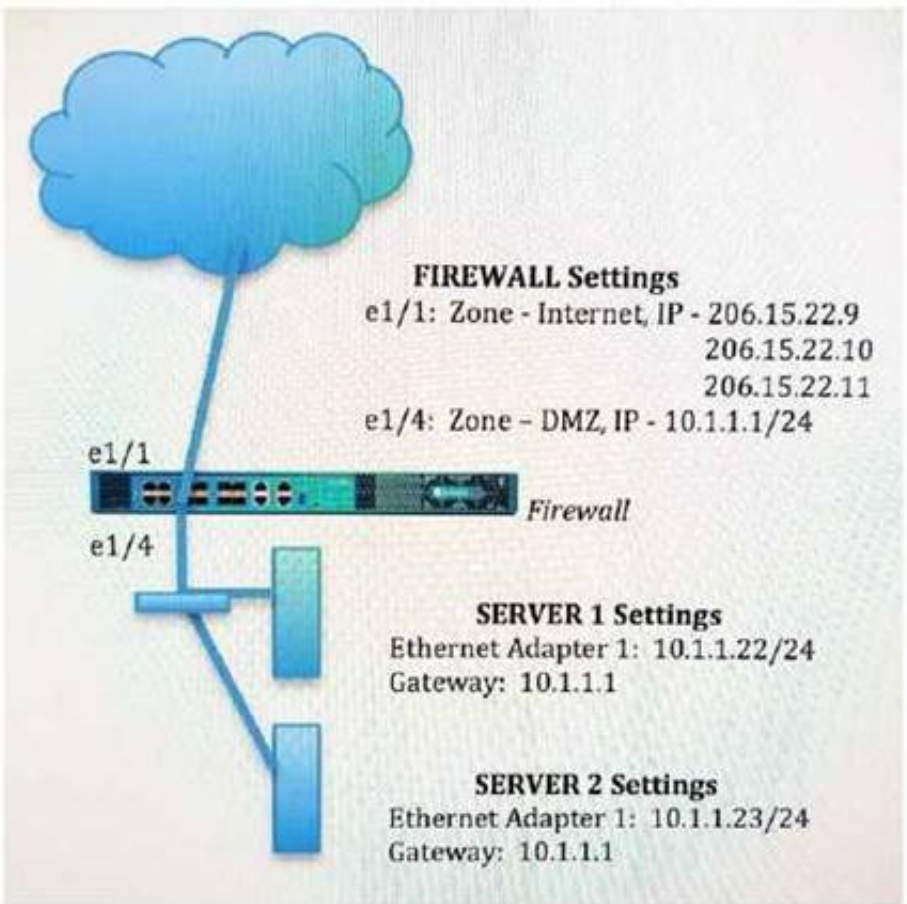
NEW QUESTION 275
- (Exam Topic 2)
Which four NGFW multi-factor authentication factors are supported by PAN-OS? (Choose four.)

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 278
- (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 279
- (Exam Topic 2)
For which two reasons would a firewall discard a packet as part of the packet flow sequence? (Choose two)

A. equal-cost multipath
B. ingress processing errors
C. rule match with action "allow"
D. rule match with action "deny"

Answer: BD

NEW QUESTION 282
- (Exam Topic 2)
Which tool provides an administrator the ability to see trends in traffic over periods of time, such as threats detected in the last 30 days?

A. Session Browser
B. Application Command Center
C. TCP Dump
D. Packet Capture

Answer: B

Explanation:
Reference:
https://live.paloaltonetworks.com/t5/Management-Articles/Tips-amp-Tricks-How-to-Use-the-Application-Comm ACC/ta-p/67342

NEW QUESTION 287
- (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 289
- (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 290
- (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 294
- (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 297
- (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 301
- (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 305
- (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 308

- (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 309
- (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 311
- (Exam Topic 2)
What are two benefits of nested device groups in Panorama? (Choose two.)

A. Reuse of the existing Security policy rules and objects
B. Requires configuring both function and location for every device
C. All device groups inherit settings form the Shared group
D. Overwrites local firewall configuration

Answer: AC

Explanation:
Creation of a device group hierarchy enables you to organize firewalls based on common policy requirements without redundant configuration. When you create objects for use in shared or device group policy once and use them many times, you reduce administrative overhead and ensure consistency across firewall policies.

NEW QUESTION 315
- (Exam Topic 2)
An administrator pushes a new configuration from Panorama to a pair of firewalls that are configured as an active/passive HA pair. Which NGFW receives the configuration from Panorama?

A. The Passive firewall, which then synchronizes to the active firewall
B. The active firewall, which then synchronizes to the passive firewall
C. Both the active and passive firewalls, which then synchronize with each other
D. Both the active and passive firewalls independently, with no synchronization afterward

Answer: D

Explanation:
Palo Alto NetworksPanorama 7.0 Administrator's Guide •77Manage FirewallsManage Device GroupsManage Device GroupsAdd a Device GroupCreate a Device Group HierarchyCreate Objects for Use in Shared or Device Group PolicyRevert to Inherited Object ValuesManage Unused Shared ObjectsManage Precedence of Inherited ObjectsMove or Clone a Policy Rule or Object to a Different Device GroupSelect a URL Filtering Vendor on PanoramaPush a Policy Rule to a Subset of FirewallsManage the Rule HierarchyAdd a Device GroupAfter adding firewalls (see Add a Firewall as a Managed Device), you can group them into Device Groups (up to 256), as follows. Be sure to assign both firewalls in an active-passive high availability (HA) configuration to the same device group so that Panorama will push the same policy rules and objects to those firewalls. ##############PAN-OS doesn't synchronize pushed rules across HA peers.########## To manage rules and objects at different administrative levels in your organization, Create a Device Group Hierarchy.
https://docs.paloaltonetworks.com/panorama/8-0/panorama-admin/manage-firewalls/transition-a-firewall-to-pan
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CleOCAS

NEW QUESTION 316
- (Exam Topic 2)
Which Security policy rule will allow an admin to block facebook chat but allow Facebook in general?

A. Deny application facebook-chat before allowing application facebook
B. Deny application facebook on top
C. Allow application facebook on top
D. Allow application facebook before denying application facebook-chat

Answer: A

Explanation:

Reference:
https://live.paloaltonetworks.com/t5/Configuration-Articles/Failed-to-Block-Facebook-Chat-Consistently/ta-p/1

NEW QUESTION 317
- (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

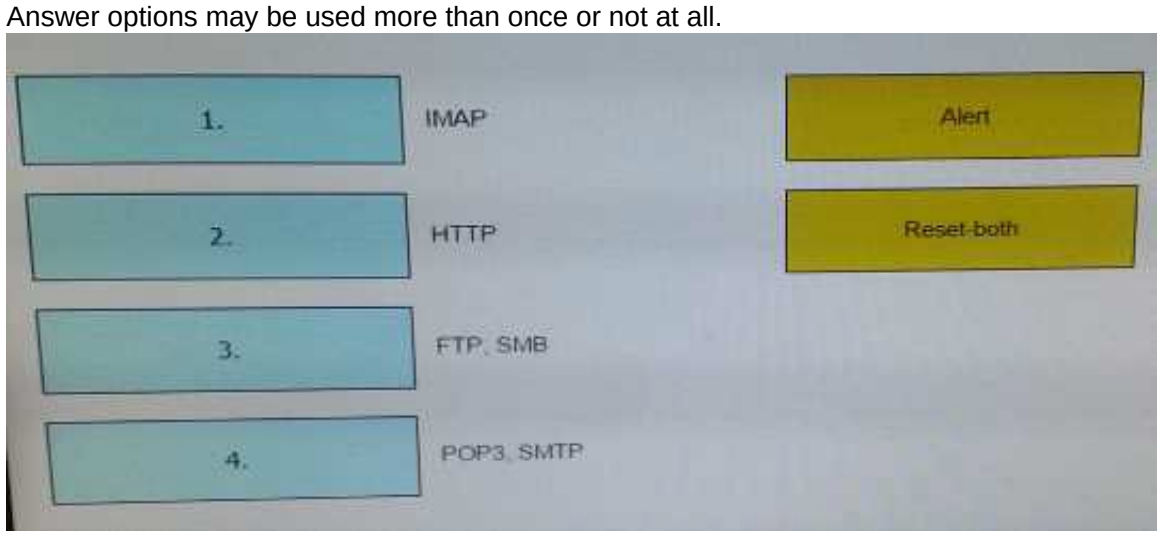
Explanation:
(https://live.paloaltonetworks.com/t5/Featured-Articles/Getting-Started-Packet-Capture/ta-p/72069)

NEW QUESTION 318
- (Exam Topic 3)
Which two actions are required to make Microsoft Active Directory users appear in a firewall traffic log? (Choose two.)

A. Run the User-ID Agent using an Active Directory account that has "event log viewer" permissions
B. Enable User-ID on the zone object for the destination zone
C. Run the User-ID Agent using an Active Directory account that has "domain administrator" permissions
D. Enable User-ID on the zone object for the source zone
E. Configure a RADIUS server profile to point to a domain controller

Answer: AD

NEW QUESTION 320
- (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 322
- (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

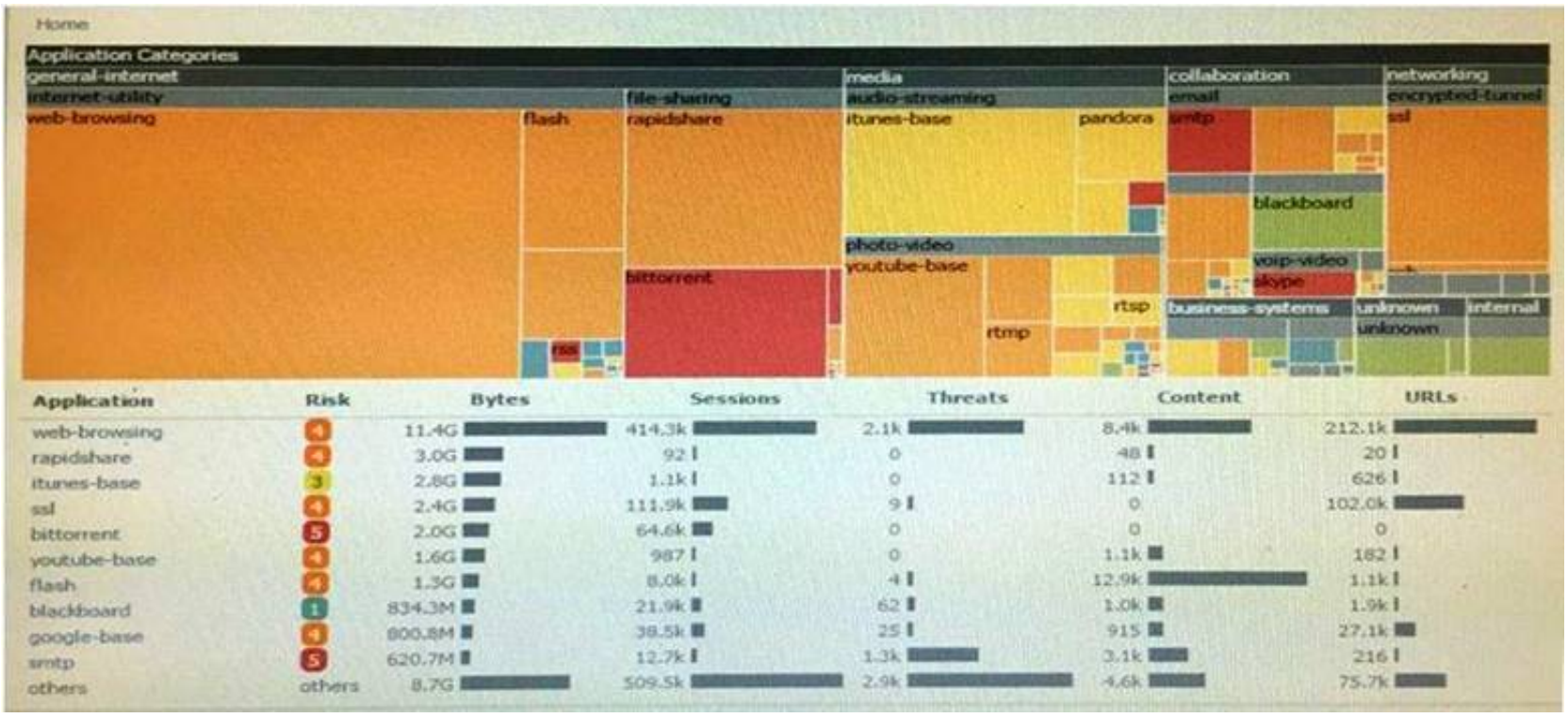
NEW QUESTION 323
- (Exam Topic 3)
Which two methods can be used to mitigate resource exhaustion of an application server? (Choose two)

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

D. Zone Protection Profile

Answer: BD

NEW QUESTION 327
- (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 332
- (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 336
- (Exam Topic 3)
Site-A and Site-B need to use IKEv2 to establish a VPN connection. Site A connects directly to the internet using a public IP address. Site-B uses a private IP address behind an ISP router to connect to the internet.
How should NAT Traversal be implemented for the VPN connection to be established between Site-A and Site-B?

A. Enable on Site-A only
B. Enable on Site-B only
C. Enable on Site-B only with passive mode
D. Enable on Site-A and Site-B

Answer: D

NEW QUESTION 338
- (Exam Topic 3)
Which three options does the WF-500 appliance support for local analysis? (Choose three)

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

Answer: ACE

NEW QUESTION 339
- (Exam Topic 3)

A network Administrator needs to view the default action for a specific spyware signature. The administrator follows the tabs and menus through Objects> Security Profiles> Anti-Spyware and select default profile.
What should be done next?

A. Click the simple-critical rule and then click the Action drop-down list.
B. Click the Exceptions tab and then click show all signatures.
C. View the default actions displayed in the Action column.
D. Click the Rules tab and then look for rules with "default" in the Action column.

Answer: B

NEW QUESTION 340
- (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 342
- (Exam Topic 3)
Which Palo Alto Networks VM-Series firewall is supported for VMware NSX?

A. VM-100
B. VM-200
C. VM-1000-HV
D. VM-300

Answer: C

NEW QUESTION 345
- (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 347
- (Exam Topic 3)
Company.com has an in-house application that the Palo Alto Networks device doesn't identify correctly. A Threat Management Team member has mentioned that this in-house application is very sensitive and all traffic being identified needs to be inspected by the Content-ID engine.
Which method should company.com use to immediately address this traffic on a Palo Alto Networks device?

A. Create a custom Application without signatures, then create an Application Override policy that includes the source, Destination, Destination Port/Protocol and Custom Application of the traffic.
B. Wait until an official Application signature is provided from Palo Alto Networks.
C. Modify the session timer settings on the closest referanced application to meet the needs of the in-house application
D. Create a Custom Application with signatures matching unique identifiers of the in-house application traffic

Answer: D

NEW QUESTION 352
- (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 356
- (Exam Topic 3)
A firewall administrator has been asked to configure a Palo Alto Networks NGFW to prevent against compromised hosts trying to phone-home or beacon out to external command-and-control (C2) servers.
Which security Profile type will prevent these behaviors?

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

Answer: D

NEW QUESTION 360
- (Exam Topic 3)
Which CLI command displays the current management plane memory utilization?

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

Answer: D

Explanation:
https://live.paloaltonetworks.com/t5/Learning-Articles/How-to-Interpret-show-system-resources/ta-p/59364 "The command show system resources gives a snapshot of Management Plane (MP) resource utilization
including memory and CPU. This is similar to the ‘top’ command in Linux."https://live.paloaltonetworks.com/t5/Learning-Articles/How-to-Interpret-show-system-resources/ta-p/59

NEW QUESTION 365
- (Exam Topic 3)
A firewall administrator is troubleshooting problems with traffic passing through the Palo Alto Networks firewall. Which method shows the global counters associated with the traffic after configuring the appropriate packet filters?

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

Answer: B

NEW QUESTION 370
- (Exam Topic 3)
Which two statements are correct for the out-of-box configuration for Palo Alto Networks NGFWs? (Choose two)

A. The devices are pre-configured with a virtual wire pair out the first two interfaces.
B. The devices are licensed and ready for deployment.
C. The management interface has an IP address of 192.168.1.1 and allows SSH and HTTPS connections.
D. A default bidirectional rule is configured that allows Untrust zone traffic to go to the Trust zone.
E. The interface are pingable.

Answer: BC

NEW QUESTION 373
- (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 378
- (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 383
- (Exam Topic 3)
The GlobalProtect Portal interface and IP address have been configured. Which other value needs to be defined to complete the network settings configuration of GlobalPortect Portal?

A. Server Certificate
B. Client Certificate
C. Authentication Profile
D. Certificate Profile

Answer: A

Explanation:
(https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Configure-GlobalProtect/ta-p/58351)

NEW QUESTION 386
- (Exam Topic 3)
Which three options are available when creating a security profile? (Choose three)

A. Anti-Malware
B. File Blocking
C. Url Filtering
D. IDS/ISP
E. Threat Prevention
F. Antivirus

Answer: ABF

NEW QUESTION 389
- (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 393
- (Exam Topic 3)
After pushing a security policy from Panorama to a PA-3020 firwall, the firewall administrator notices that traffic logs from the PA-3020 are not appearing in Panorama's traffic logs. What could be the problem?

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

Answer: D

NEW QUESTION 395
- (Exam Topic 3)
What are two prerequisites for configuring a pair of Palo Alto Networks firewalls in an active/passive High Availability (HA) pair? (Choose two.)

A. The firewalls must have the same set of licenses.
B. The management interfaces must to be on the same network.
C. The peer HA1 IP address must be the same on both firewalls.
D. HA1 should be connected to HA1. Either directly or with an intermediate Layer 2 device.

Answer: AD

NEW QUESTION 397
- (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 401
- (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.

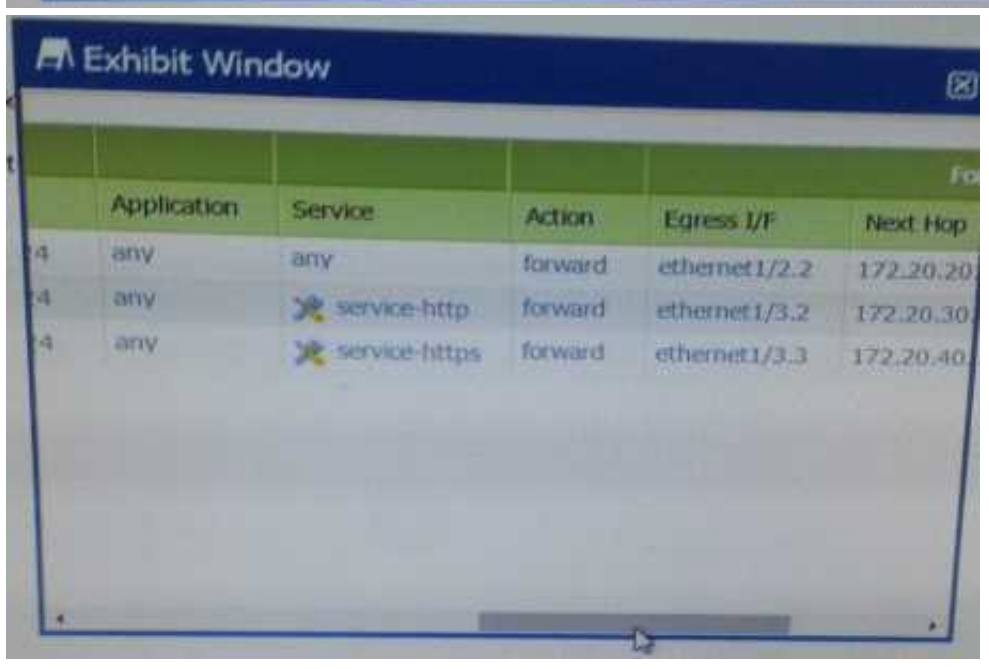
Answer: BD

NEW QUESTION 404
- (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 405
- (Exam Topic 3)
Refer to Exhibit:



A firewall has three PDF rules and a default route with a next hop of 172.29.19.1 that is configured in the default VR. A user named XX-bes a PC with a 192.168.101.10 IP address.
He makes an HTTPS connection to 172.16.10.29.
What is the next hop IP address for the HTTPS traffic from Wills PC.

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

Answer: B

NEW QUESTION 408
- (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 410
- (Exam Topic 3)
YouTube videos are consuming too much bandwidth on the network, causing delays in mission-critical traffic. The administrator wants to throttle YouTube traffic.
The following interfaces and zones are in use on the firewall:
* ethernet1/1, Zone: Untrust (Internet-facing)
* ethernet1/2, Zone: Trust (client-facing)
A QoS profile has been created, and QoS has been enabled on both interfaces. A QoS rule exists to put the YouTube application into QoS class 6. Interface Ethernet1/1 has a QoS profile called Outbound, and interface Ethernet1/2 has a QoS profile called Inbound.
Which setting for class 6 with throttle YouTube traffic?

A. Outbound profile with Guaranteed Ingress
B. Outbound profile with Maximum Ingress
C. Inbound profile with Guaranteed Egress
D. Inbound profile with Maximum Egress

Answer: D

NEW QUESTION 413

- (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 418
- (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

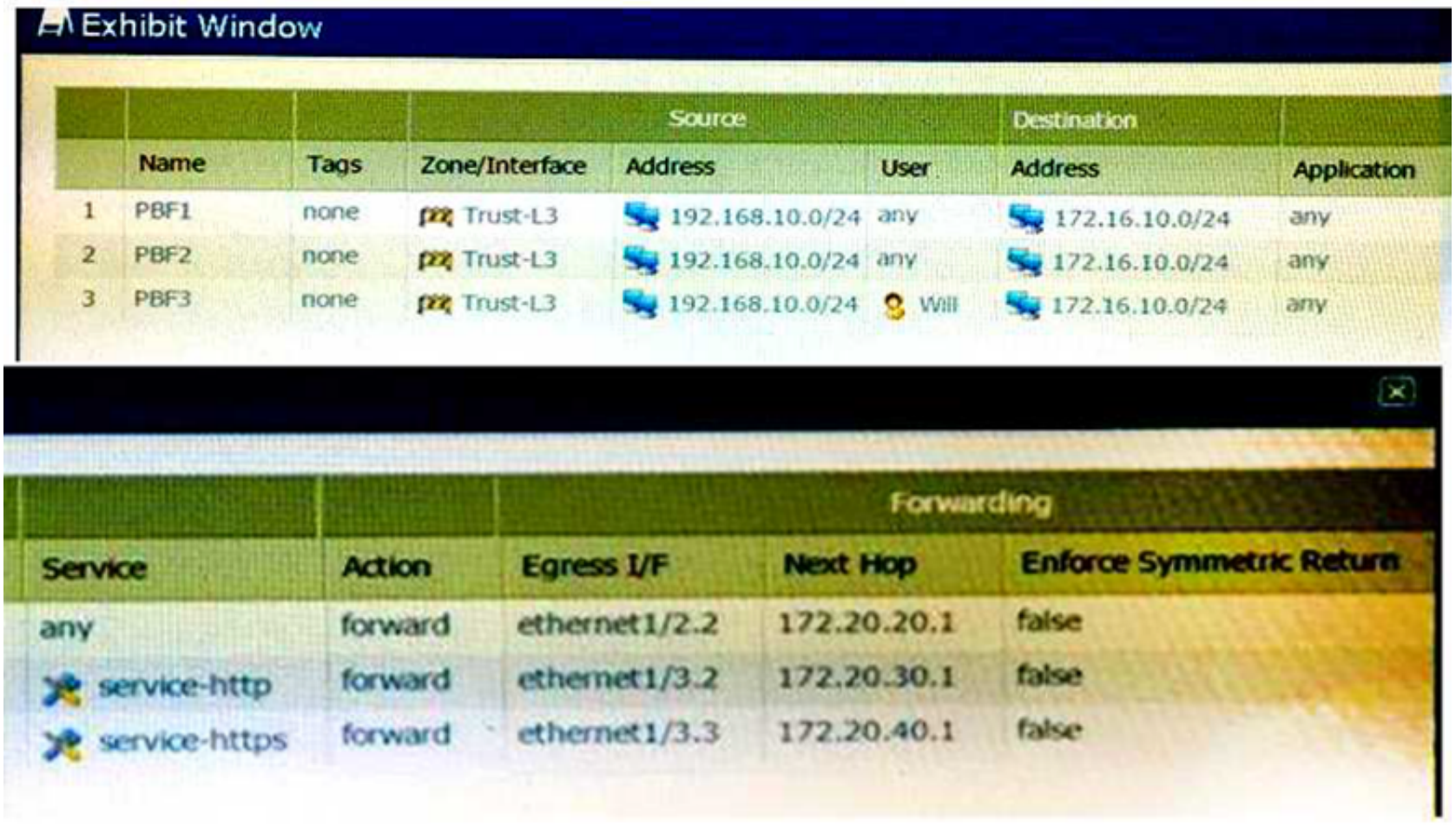
Answer: A

NEW QUESTION 421
- (Exam Topic 3)
How can a Palo Alto Networks firewall be configured to send syslog messages in a format compatible with non-standard syslog servers?

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

Answer: D

NEW QUESTION 425
- (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 426
- (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 428
- (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 429
- (Exam Topic 3)
Starting with PAN-OS version 9.1, application dependency information is now reported in which new locations? (Choose two.)

A. On the App Dependency tab in the Commit Status window
B. On the Application tab in the Security Policy Rule creation window
C. On the Objects > Applications browsers pages
D. On the Policy Optimizer's Rule Usage page

Answer: AB

NEW QUESTION 431
- (Exam Topic 3)
Which interface configuration will accept specific VLAN IDs?

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

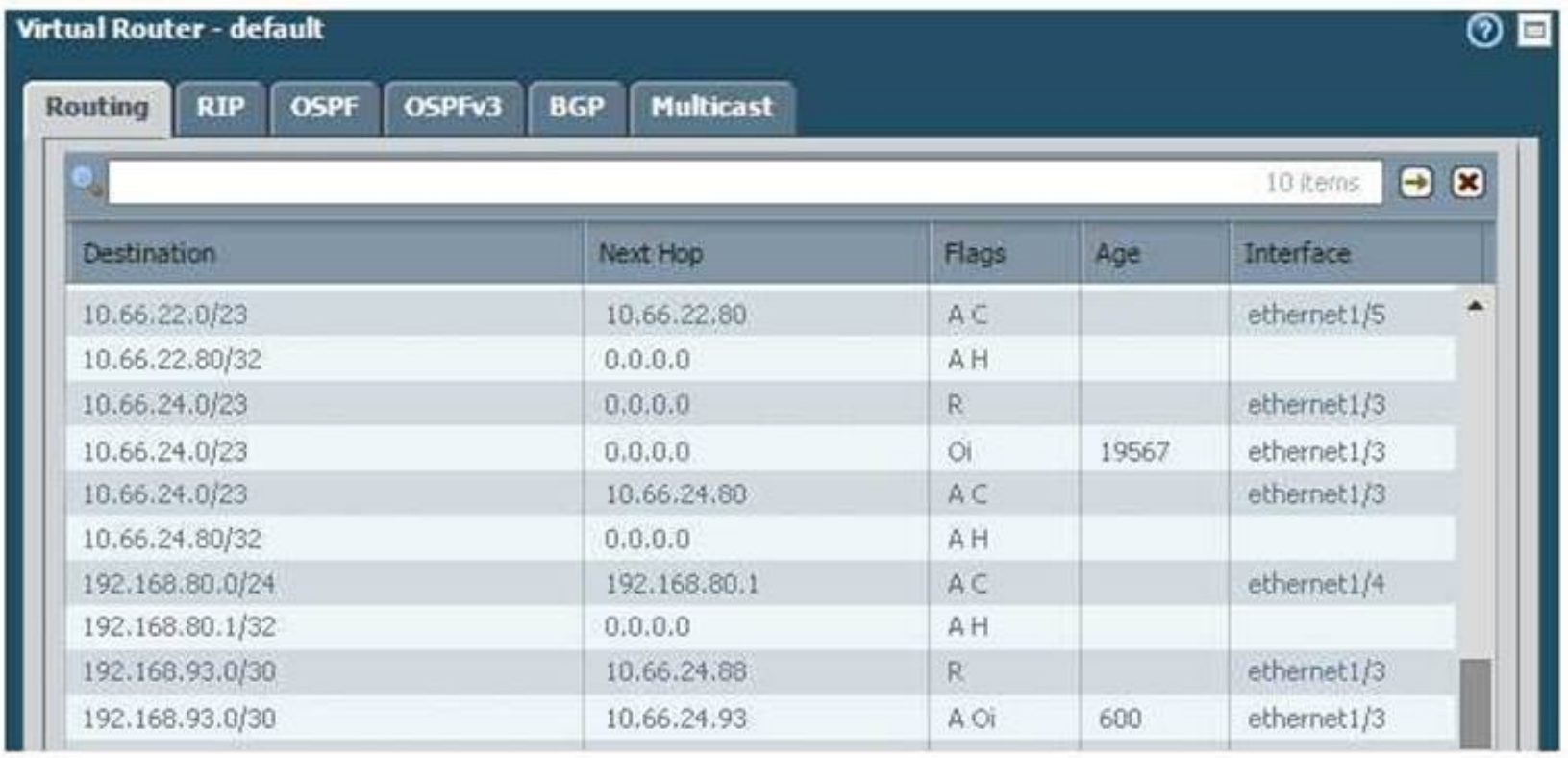
Answer: B

NEW QUESTION 434
- (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 437
- (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 442
- (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 447
- (Exam Topic 3)
A logging infrastructure may need to handle more than 10,000 logs per second. Which two options support a dedicated log collector function? (Choose two)

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

Answer: BC

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

NEW QUESTION 449
- (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 452
- (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 453
- (Exam Topic 3)
Which URL Filtering Security Profile action logs the URL Filtering category to the URL Filtering log?

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

Answer: B

Explanation:
https://www.paloaltonetworks.com/documentation/70/pan-os/pan-os/url-filtering/url-filtering-profile-actions

NEW QUESTION 456
- (Exam Topic 3)
A Palo Alto Networks firewall is being targeted by an NTP Amplification attack and is being flooded with tens thousands of bogus UDP connections per second to a single destination IP address and post.
Which option when enabled with the correction threshold would mitigate this attack without dropping legitirnate traffic to other hosts insides the network?

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

Answer: D

NEW QUESTION 459
- (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 464
- (Exam Topic 3)
Which two virtualized environments support Active/Active High Availability (HA) in PAN-OS 8.0? (Choose two.)

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

Answer: AB

NEW QUESTION 468
- (Exam Topic 3)
Which option is an IPv6 routing protocol?

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

Answer: B

NEW QUESTION 472
- (Exam Topic 3)
A company has a pair of Palo Alto Networks firewalls configured as an Acitve/Passive High Availability (HA) pair.
What allows the firewall administrator to determine the last date a failover event occurred?

A. From the CLI issue use the show System log
B. Apply the filter subtype eq ha to the System log
C. Apply the filter subtype eq ha to the configuration log
D. Check the status of the High Availability widget on the Dashboard of the GUI

Answer: B

NEW QUESTION 474
- (Exam Topic 3)
A network administrator uses Panorama to push security polices to managed firewalls at branch offices. Which policy type should be configured on Panorama if the administrators at the branch office sites to override these products?

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

Answer: A

NEW QUESTION 475
- (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 480
.....

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