Paloalto-Networks

Exam Questions PCNSE

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

NEW QUESTION 1
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 2
What are the two behavior differences between Highlight Unused Rules and the Rule Usage Hit counter when a firewall is rebooted? (Choose two.)

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

Answer: AB

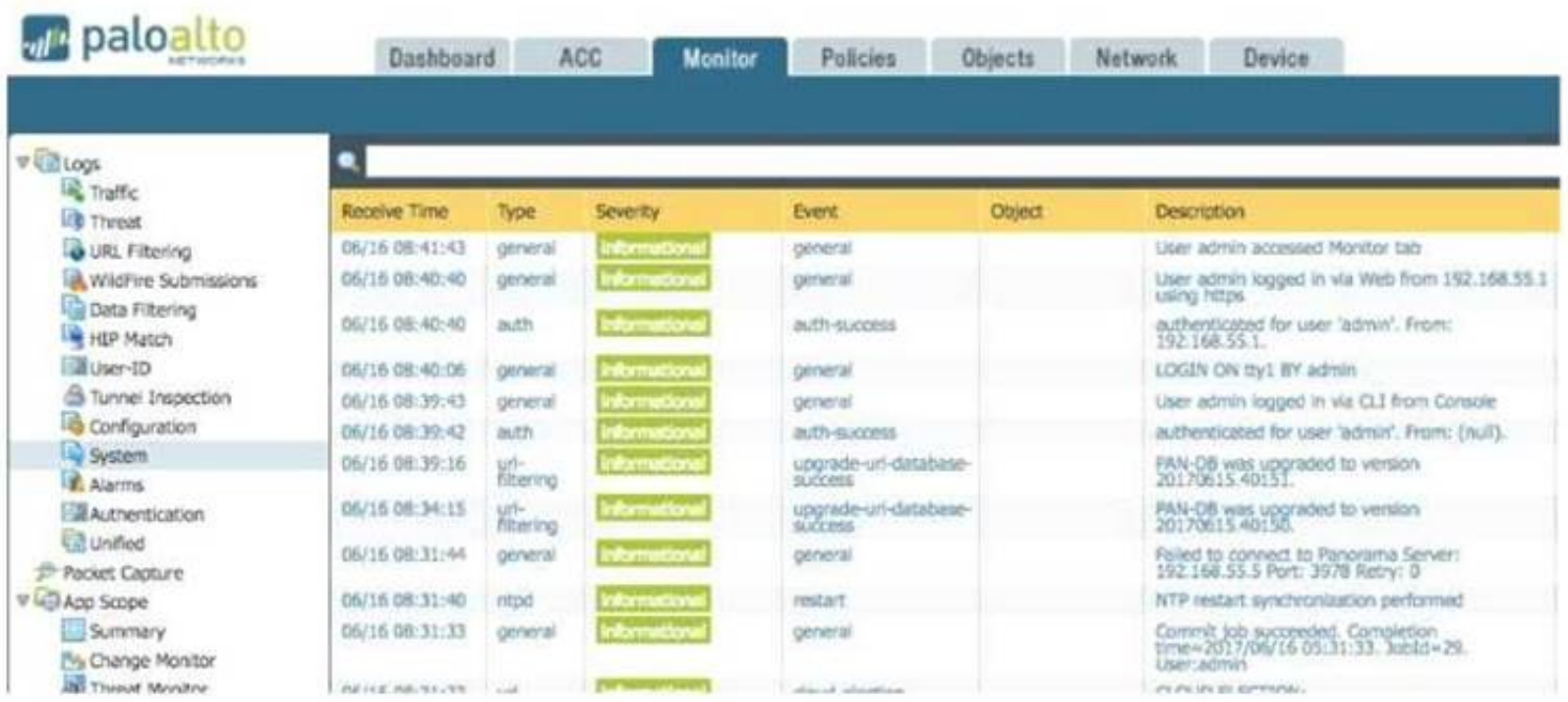
NEW QUESTION 3
How does Panorama prompt VMWare NSX to quarantine an infected VM?

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

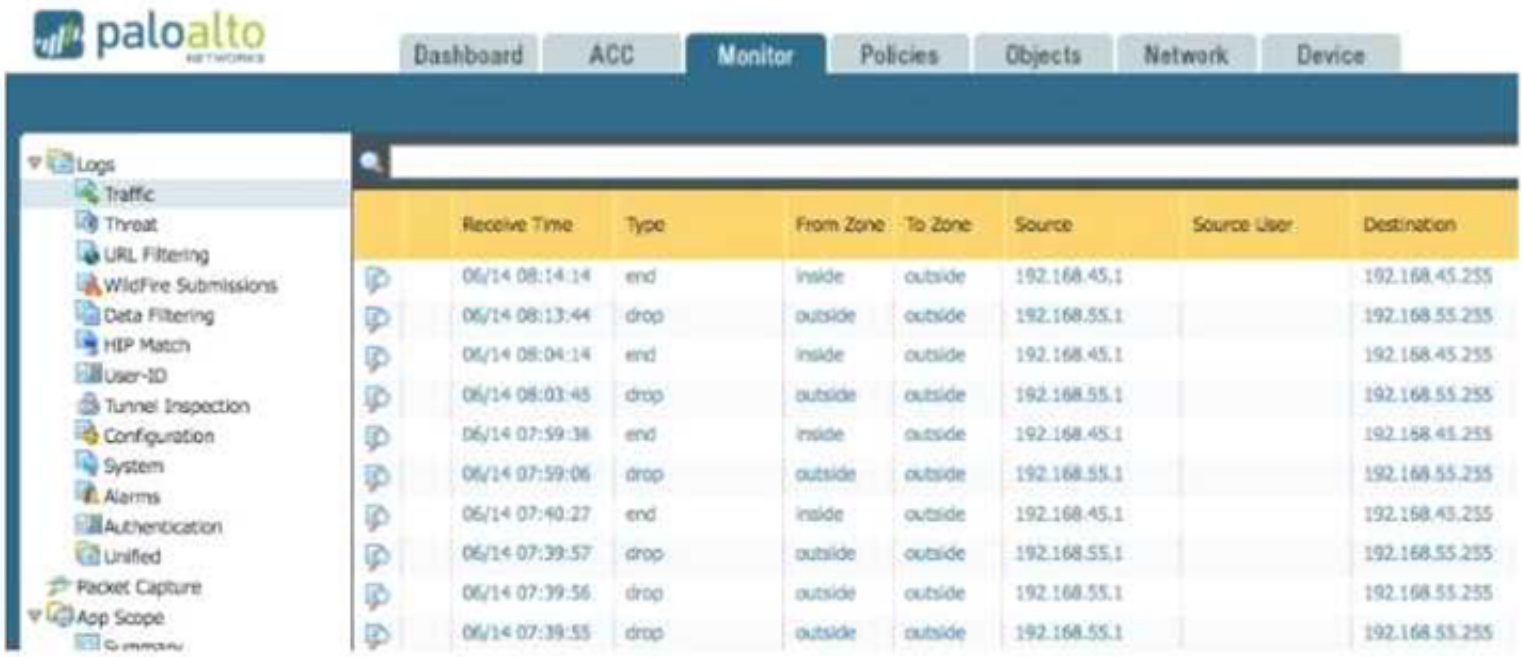
Answer: A

NEW QUESTION 4
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

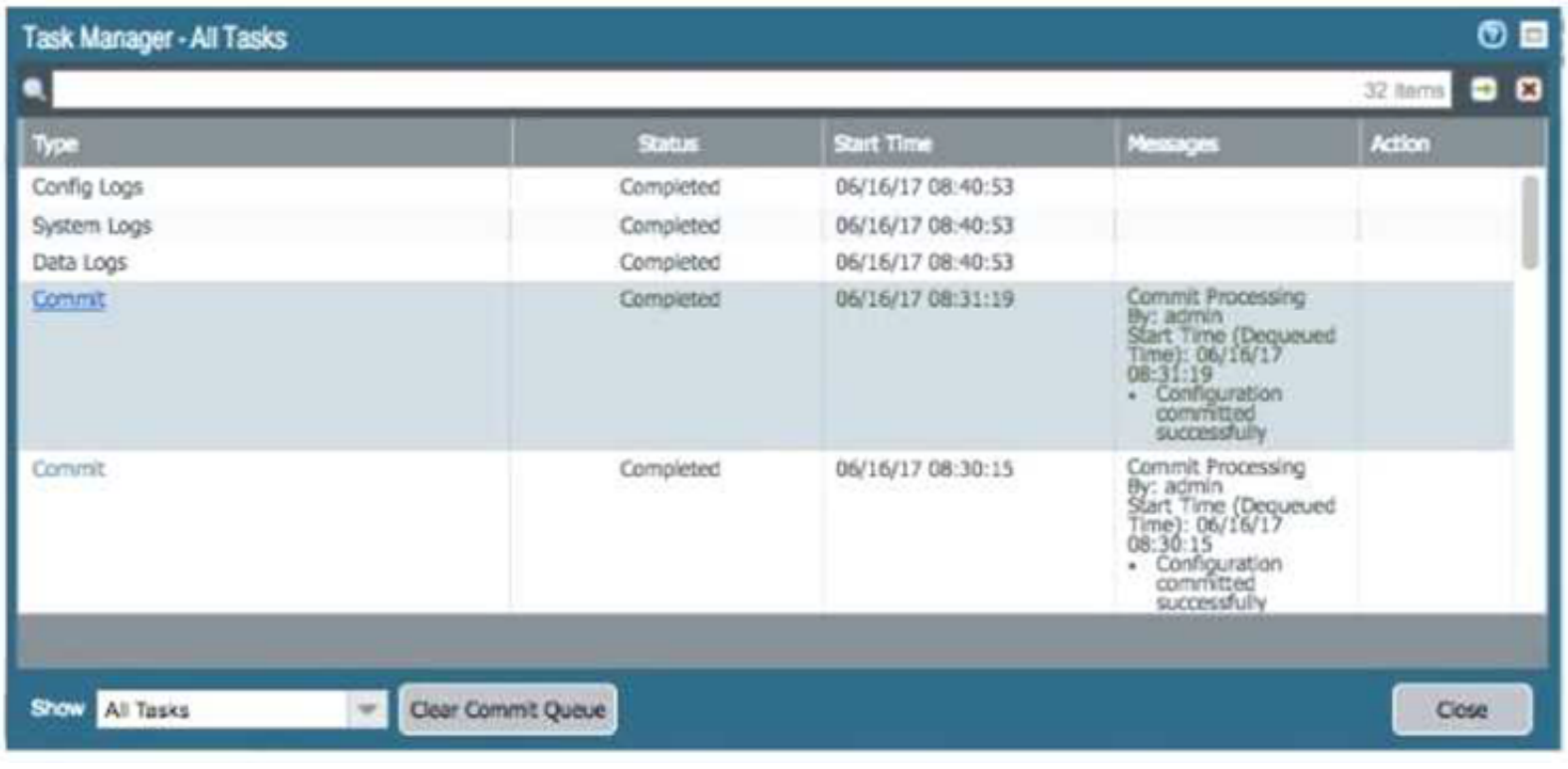


B



C

D



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

Answer: AD

NEW QUESTION 5
A customer wants to set up a VLAN interface for a Layer 2 Ethernet port.
Which two mandatory options are used to configure a VLAN interface? (Choose two.)

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

Answer: AB

Explanation:
Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/network/network-interfaces/pa-7000-series-layer-2-interface#idd2bcaacc-54b9-4ec9-a1dd- 8064499f5b9d

NEW QUESTION 6
A company needs to preconfigure firewalls to be sent to remote sites with the least amount of reconfiguration. Once deployed, each firewall must establish secure tunnels back to multiple regional data centers to include the future regional data centers.

Which VPN configuration would adapt to changes when deployed to the future site?

A. Preconfigured GlobalProtect satellite
B. Preconfigured GlobalProtect client
C. Preconfigured IPsec tunnels
D. Preconfigured PPTP Tunnels

Answer: A

NEW QUESTION 7
An administrator pushes a new configuration from Panorama to a pair of firewalls that are configured as an active/passive HA pair. Which NGFW receives the configuration from Panorama?

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

Answer: C

NEW QUESTION 8
When configuring a GlobalProtect Portal, what is the purpose of specifying an Authentication Profile?

A. To enable Gateway authentication to the Portal
B. To enable Portal authentication to the Gateway
C. To enable user authentication to the Portal
D. To enable client machine authentication to the Portal

Answer: C

Explanation:
The additional options of Browser and Satellite enable you to specify the authentication profile to use for specific scenarios. Select Browser to specify the authentication profile to use to authenticate a user accessing the portal from a web browser with the intent of downloading the GlobalProtect agent (Windows and Mac). Select Satellite to specify the authentication profile to use to authenticate the satellite.
Reference https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/globalprotect/network-globalprotect-portals

NEW QUESTION 9
How does an administrator schedule an Applications and Threats dynamic update while delaying installation of the update for a certain amount of time?

A. Configure the option for “Threshold”.
B. Disable automatic updates during weekdays.
C. Automatically “download only” and then install Applications and Threats later, after the administrator approves the update.
D. Automatically “download and install” but with the “disable new applications” option used.

Answer: A

NEW QUESTION 10
To connect the Palo Alto Networks firewall to AutoFocus, which setting must be enabled?

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

Answer: B

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

NEW QUESTION 10
Which User-ID method maps IP addresses to usernames for users connecting through an 802.1x- enabled wireless network device that has no native integration with PAN-OS® software?

A. XML API
B. Port Mapping
C. Client Probing
D. Server Monitoring

Answer: A

Explanation:
Captive Portal and the other standard user mapping methods might not work for certain types of user access. For example, the standard methods cannot add mappings of users connecting from a
third-party VPN solution or users connecting to a 802.1x-enabled wireless network. For such cases, you can use the PAN-OS XML API to capture login events and

send them to the PAN-OS integrated User-ID agent Reference: https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/user-id/user-id-concepts

NEW QUESTION 11
A Security policy rule is configured with a Vulnerability Protection Profile and an action of 'Deny". Which action will this cause configuration on the matched traffic?

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

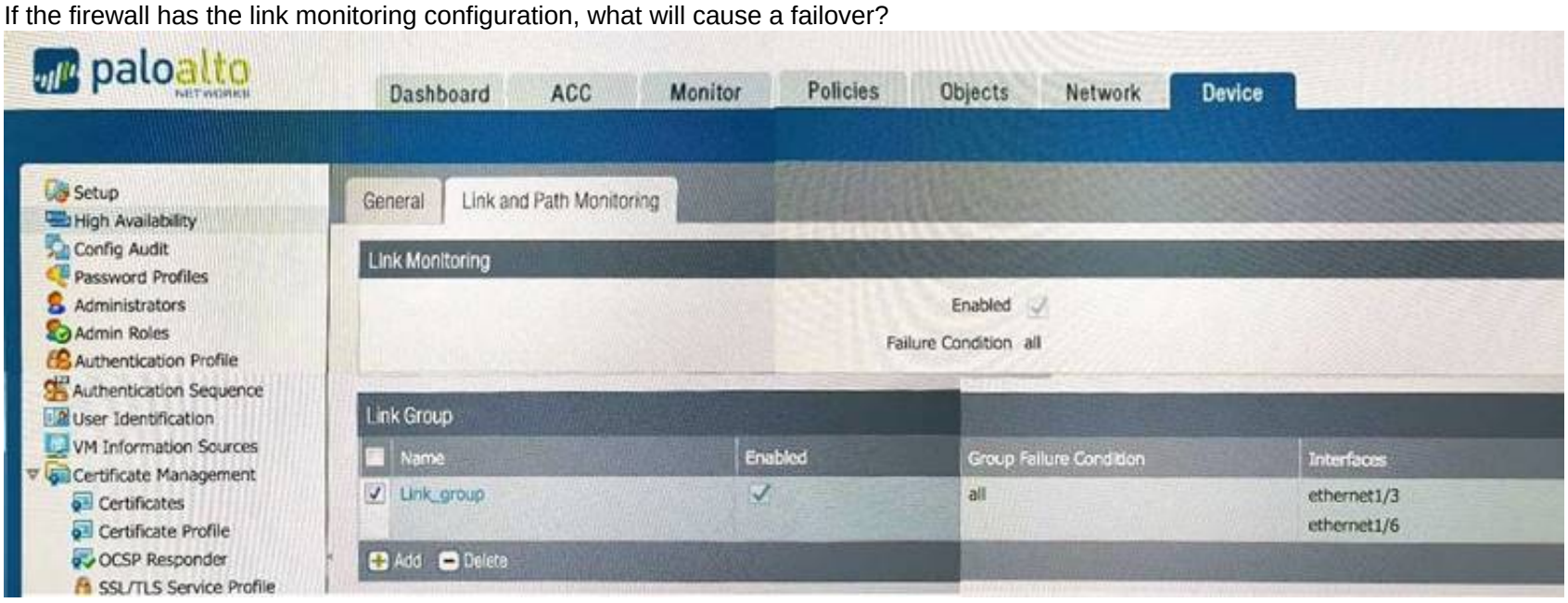
Answer: B

NEW QUESTION 15
A web server is hosted in the DMZ, and the server is configured to listen for incoming connections only on TCP port 8080. A Security policy rule allowing access from the Trust zone to the DMZ zone need to be configured to enable we browsing access to the server.
Which application and service need to be configured to allow only cleartext web-browsing traffic to thins server on tcp/8080.

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

Answer: A

NEW QUESTION 20
If the firewall has the link monitoring configuration, what will cause a failover?



A. ethernet1/3 and ethernet1/6 going down
B. ethernet1/3 going down
C. ethernet1/3 or Ethernet1/6 going down
D. ethernet1/6 going down

Answer: A

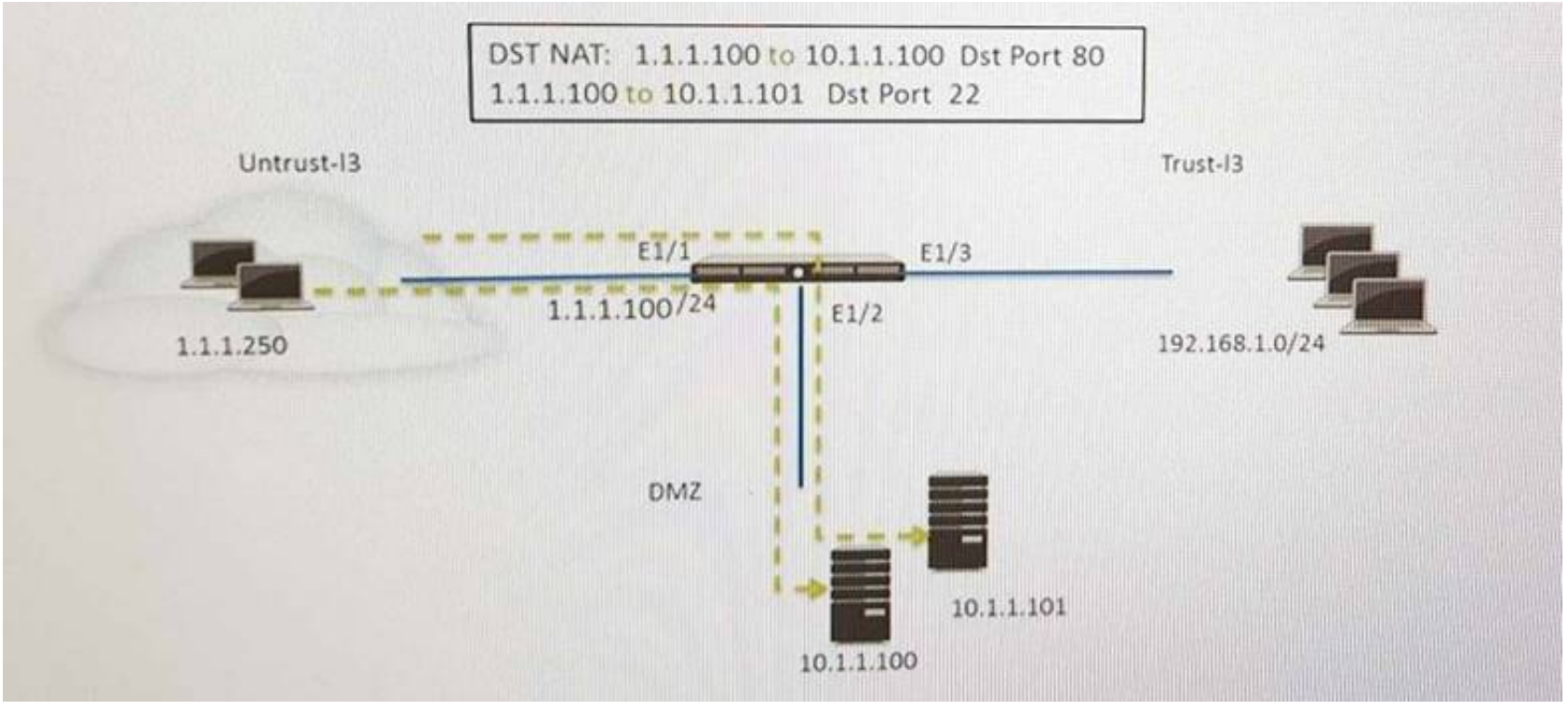
NEW QUESTION 22
An administrator needs to optimize traffic to prefer business-critical applications over non-critical applications. QoS natively integrates with which feature to provide service quality?

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-users

NEW QUESTION 26
Refer to the exhibit.



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

A. Untrust (Any) to Untrust (10.1.1.1), web-browsing -Allow
B. Untrust (Any) to Untrust (10.1.1.1), ssh -Allow
C. Untrust (Any) to DMZ (10.1.1.1), web-browsing -Allow
D. Untrust (Any) to DMZ (10.1.1.1), ssh –Allow
E. Untrust (Any) to DMZ (10.1.1.100.10.1.1.101), ssh, web-browsing -Allow

Answer: CD

NEW QUESTION 28
Which three settings are defined within the Templates object of Panorama? (Choose three.)

A. Setup
B. Virtual Routers
C. Interfaces
D. Security
E. Application Override

Answer: ADE

NEW QUESTION 33
An administrator has left a firewall to use the default port for all management services. Which three functions are performed by the dataplane? (Choose three.)

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

Answer: ABC

NEW QUESTION 37
An administrator is using Panorama and multiple Palo Alto Networks NGFWs. After upgrading all devices to the latest PAN-OS® software, the administrator enables log forwarding from the firewalls to Panorama. Pre-existing logs from the firewalls are not appearing in PanoramA.
Which action would enable the firewalls to send their pre-existing logs to Panorama?

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

Answer: B

NEW QUESTION 39
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: A

NEW QUESTION 43
Which event will happen if an administrator uses an Application Override Policy?

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 45
Which Security policy rule will allow an admin to block facebook chat but allow Facebook in general?

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

Answer: A

Explanation:
Reference: https://live.paloaltonetworks.com/t5/Configuration-Articles/Failed-to-Block-Facebook-Chat-Consistently/ta-p/115673

NEW QUESTION 48
If the firewall is configured for credential phishing prevention using the “Domain Credential Filter” method, which login will be detected as credential theft?

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 52
Which feature prevents the submission of corporate login information into website forms?

A. Data filtering
B. User-ID
C. File blocking
D. Credential phishing prevention

Answer: D

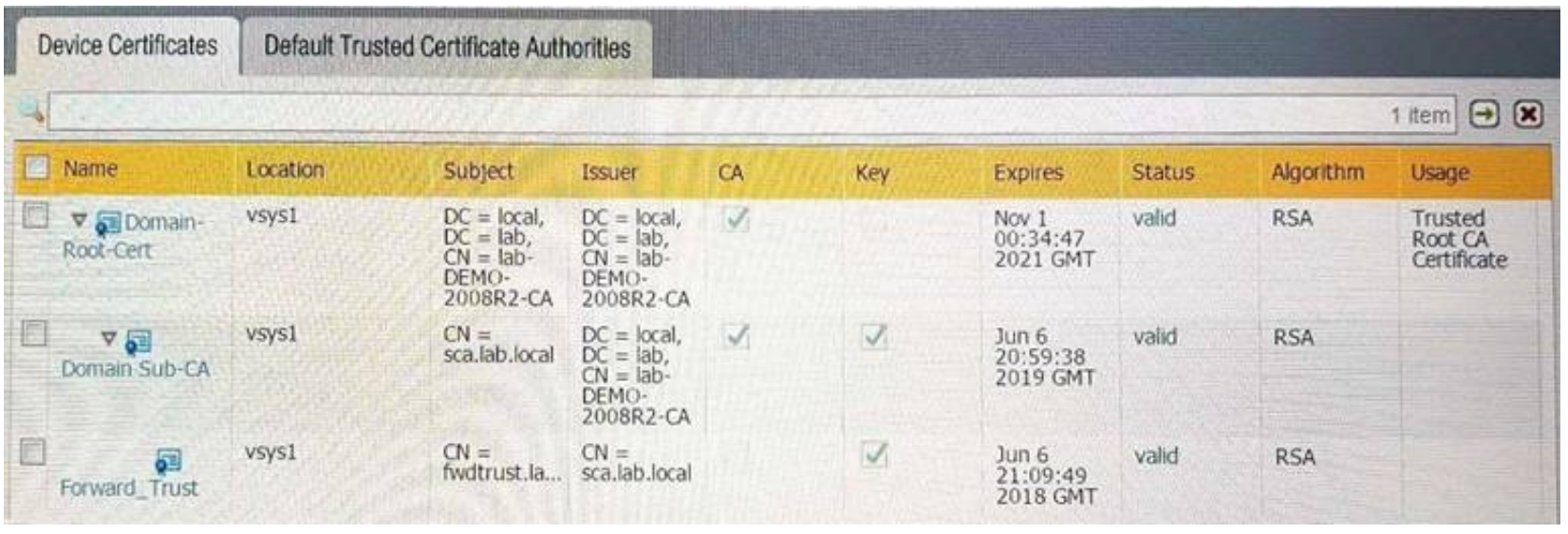
Explanation:
Reference: https://www.paloaltonetworks.com/cyberpedia/how-the-next-generation-security-platform-contributes-to-gdpr-compliance

NEW QUESTION 55
An administrator creates an SSL decryption rule decrypting traffic on all ports. The administrator also creates a Security policy rule allowing only the applications DNS, SSL, and web-browsing.
The administrator generates three encrypted BitTorrent connections and checks the Traffic logs. There are three entries. The first entry shows traffic dropped as application Unknown. The next two entries show traffic allowed as application SSL.
Which action will stop the second and subsequent encrypted BitTorrent connections from being allowed as SSL?

A. Create a decryption rule matching the encrypted BitTorrent traffic with action “No-Decrypt,” and place the rule at the top of the Decryption policy.
B. Create a Security policy rule that matches application “encrypted BitTorrent” and place the rule at the top of the Security policy.
C. Disable the exclude cache option for the firewall.
D. Create a Decryption Profile to block traffic using unsupported cyphers, and attach the profile to the decryption rule.

Answer: D

NEW QUESTION 59
Refer to the exhibit.



Which certificates can be used as a Forwarded Trust certificate?

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

Answer: A

NEW QUESTION 61
Which protection feature is available only in a Zone Protection Profile?

A. SYN Flood Protection using SYN Flood Cookies
B. ICMP Flood Protection
C. Port Scan Protection
D. UDP Flood Protections

Answer: A

NEW QUESTION 64
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: D

Explanation:
The firewall uses the service route to connect to the Update Server and checks for new content release versions and, if there are updates available, displays them at the top of the list.
Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/device/device-dynamic-updates

NEW QUESTION 65
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:
Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/device/device-high-availability/ha-lite

NEW QUESTION 67
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: CDE

NEW QUESTION 69
How can a candidate or running configuration be copied to a host external from Panorama?

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

Answer: D

Explanation:
Reference:
https://www.paloaltonetworks.com/documentation/71/panorama/panorama_adminguide/administ er-panorama/back-up-panorama-and-firewall-configurations

NEW QUESTION 74
An administrator sees several inbound sessions identified as unknown-tcp in the Traffic logs. The administrator determines that these sessions are form external users accessing the company's proprietary accounting application. The administrator wants to reliably identify this traffic as their accounting application and to scan this traffic for threats.
Which option would achieve this result?

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

Answer: A

NEW QUESTION 77
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

NEW QUESTION 80
An administrator has a requirement to export decrypted traffic from the Palo Alto Networks NGFW to a third-party, deep-level packet inspection appliance.
Which interface type and license feature are necessary to meet the requirement?

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

Answer: D

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

NEW QUESTION 81
Which processing order will be enabled when a Panorama administrator selects the setting "Objects defined in ancestors will take higher precedence?"

A. Descendant objects will take precedence over other descendant objects.
B. Descendant objects will take precedence over ancestor objects.
C. Ancestor objects will have precedence over descendant objects.
D. Ancestor objects will have precedence over other ancestor objects.

Answer: C

Explanation:
Reference: https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/device/device-setup-management

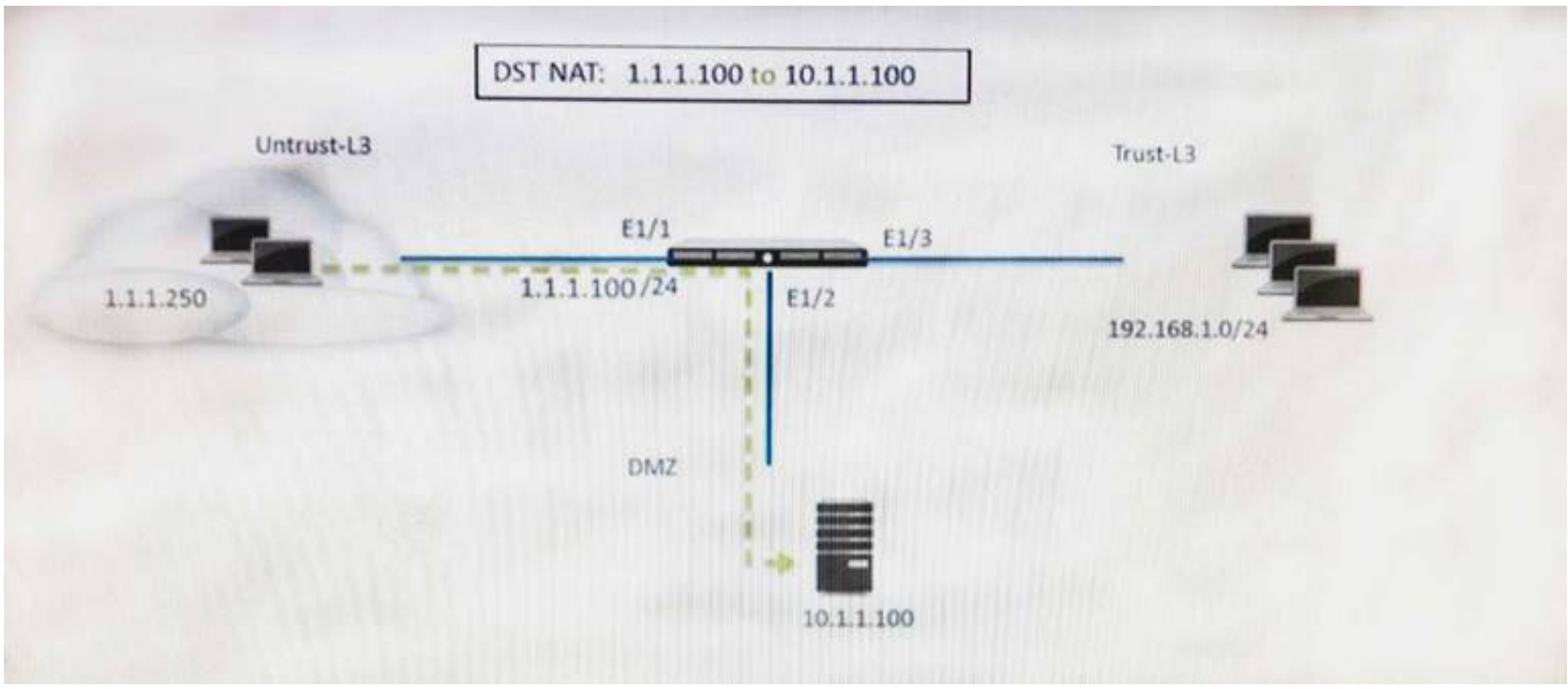
NEW QUESTION 86
An administrator using an enterprise PKI needs to establish a unique chain of trust to ensure mutual authentication between Panorama and the managed firewalls and Log Collectors.
How would the administrator establish the chain of trust?

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/plan-your-panorama-deployment

NEW QUESTION 87
Refer to the exhibit.



A web server in the DMZ is being mapped to a public address through DNAT. Which Security policy rule will allow traffic to flow to the web server?

A. Untrust (any) to Untrust (10. 1.1. 100), web browsing – Allow
B. Untrust (any) to Untrust (1. 1. 1. 100), web browsing – Allow
C. Untrust (any) to DMZ (1. 1. 1. 100), web browsing – Allow
D. Untrust (any) to DMZ (10. 1. 1. 100), web browsing – Allow

Answer: B

NEW QUESTION 90
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:
Reference: https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/user-id/configure-user-mapping-for-terminal-server-users

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

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

Answer: D

NEW QUESTION 94
In High Availability, which information is transferred via the HA data link?

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

Answer: A

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

NEW QUESTION 95
The firewall identifies a popular application as an unknown-tcp.
Which two options are available to identify the application? (Choose two.)

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

Answer: AB

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

NEW QUESTION 97
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. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 98
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. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 100
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

NEW QUESTION 105
Which three user authentication services can be modified to provide the Palo Alto Networks NGFW with both usernames and role names? (Choose three.)

A. TACACS+
B. Kerberos
C. PAP
D. LDAP
E. SAML
F. RADIUS

Answer: ADF

NEW QUESTION 108
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 113
An administrator sees several inbound sessions identified as unknown-tcp in the traffic logs. The administrator determines that these sessions are from external users accessing the company's proprietary accounting application. The administrator wants to reliably identify this as their accounting application and to scan this traffic for threats. Which option would achieve this result?

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

Answer: A

NEW QUESTION 116

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

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

Answer: C

NEW QUESTION 118
An administrator needs to upgrade an NGFW to the most current version of PAN-OS® software. The following is occurring:
•Firewall has Internet connectivity through e1/1.
•Default security rules and security rules allowing all SSL and web-browsing traffic to and from any zone.
•Service route is configured, sourcing update traffic from e1/1.
•A communication error appears in the System logs when updates are performed.
•Download does not complete.
What must be configured to enable the firewall to download the current version of PAN-OS software?

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

Answer: D

NEW QUESTION 119
An administrator wants a new Palo Alto Networks NGFW to obtain automatic application updates daily, so it is configured to use a scheduler for the application database. Unfortunately, they required the management network to be isolated so that it cannot reach the internet. Which configuration will enable the firewall to download and install application updates automatically?

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

Answer: B

NEW QUESTION 121
Which three firewall states are valid? (Choose three)

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

Answer: ABC

NEW QUESTION 124
Refer to the exhibit.

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

A. Untrust (Any) to Untrust (10.1.1.1) Ssh-Allow
B. Untrust (Any) to DMZ (1.1.1.100) Ssh-Allow

C. Untrust (Any) to DMZ (1.1.1.100) Web-browsing -Allow
D. Untrust (Any) to Untrust (10.1.1.1) Web-browsing -Allow

Answer: CD

NEW QUESTION 125
Which is the maximum number of samples that can be submitted to WildFire per day, based on wildfire subscription?

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

Answer: B

NEW QUESTION 130
Which operation will impact the performance of the management plane?

A. WildFire Submissions
B. DoS Protection
C. decrypting SSL Sessions
D. Generating a SaaS Application Report.

Answer: C

NEW QUESTION 133
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 137
A client has a sensitive application server in their data center and is particularly concerned about session flooding because of denial of-service attacks.
How can the Palo Alto Networks NGFW be configured to specifically protect this server against session floods originating from a single IP address?

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

Answer: C

NEW QUESTION 141
Which Panorama administrator types require the configuration of at least one access domain? (Choose two)

A. Dynamic
B. Custom Panorama Admin
C. Role Based
D. Device Group E.Template Admin

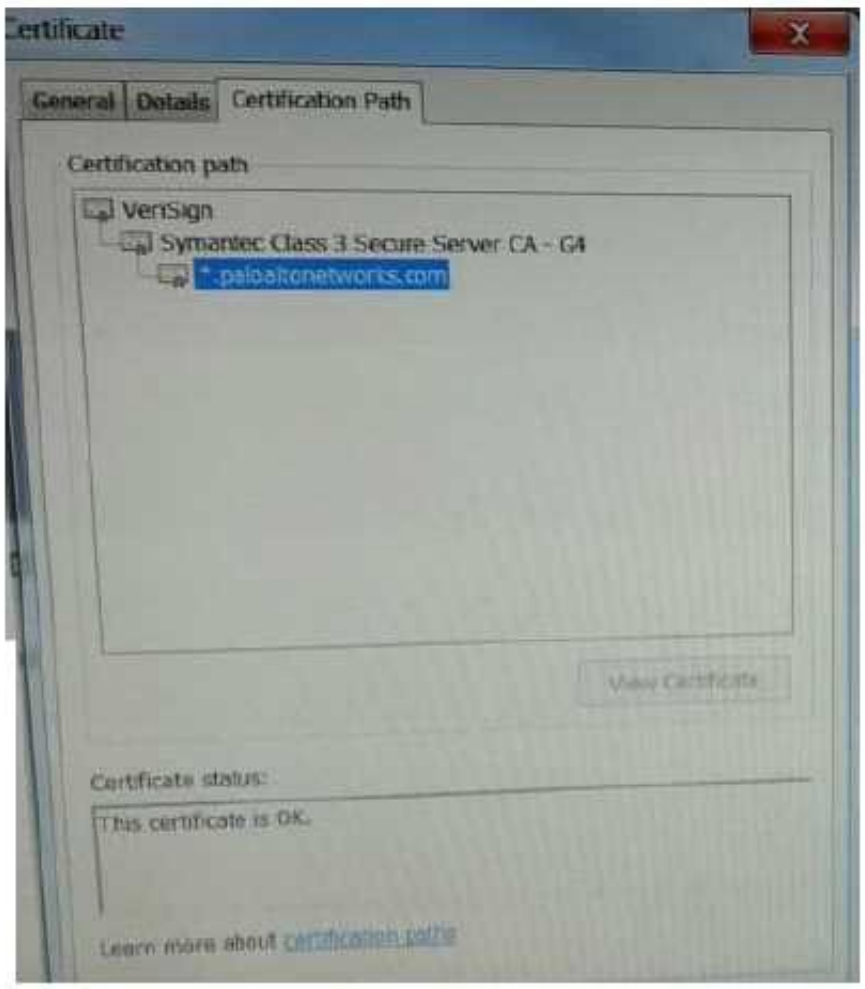
Answer: DE

NEW QUESTION 142
Which two settings can be configured only locally on the firewall and not pushed from a Panorama template or template stack? (Choose two)

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

Answer: AB

NEW QUESTION 146
Based on the following image,



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

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

Answer: D

NEW QUESTION 151
A host attached to Ethernet 1/4 cannot ping the default gateway. The widget on the dashboard shows Ethernet 1/1 and Ethernet 1/4 to be green. The IP address of Ethernet 1/1 is 192.168.1.7 and the IP address of Ethernet 1/4 is 10.1.1.7. The default gateway is attached to Ethernet 1/1. A default route is properly configured. What can be the cause of this problem?

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

Answer: A

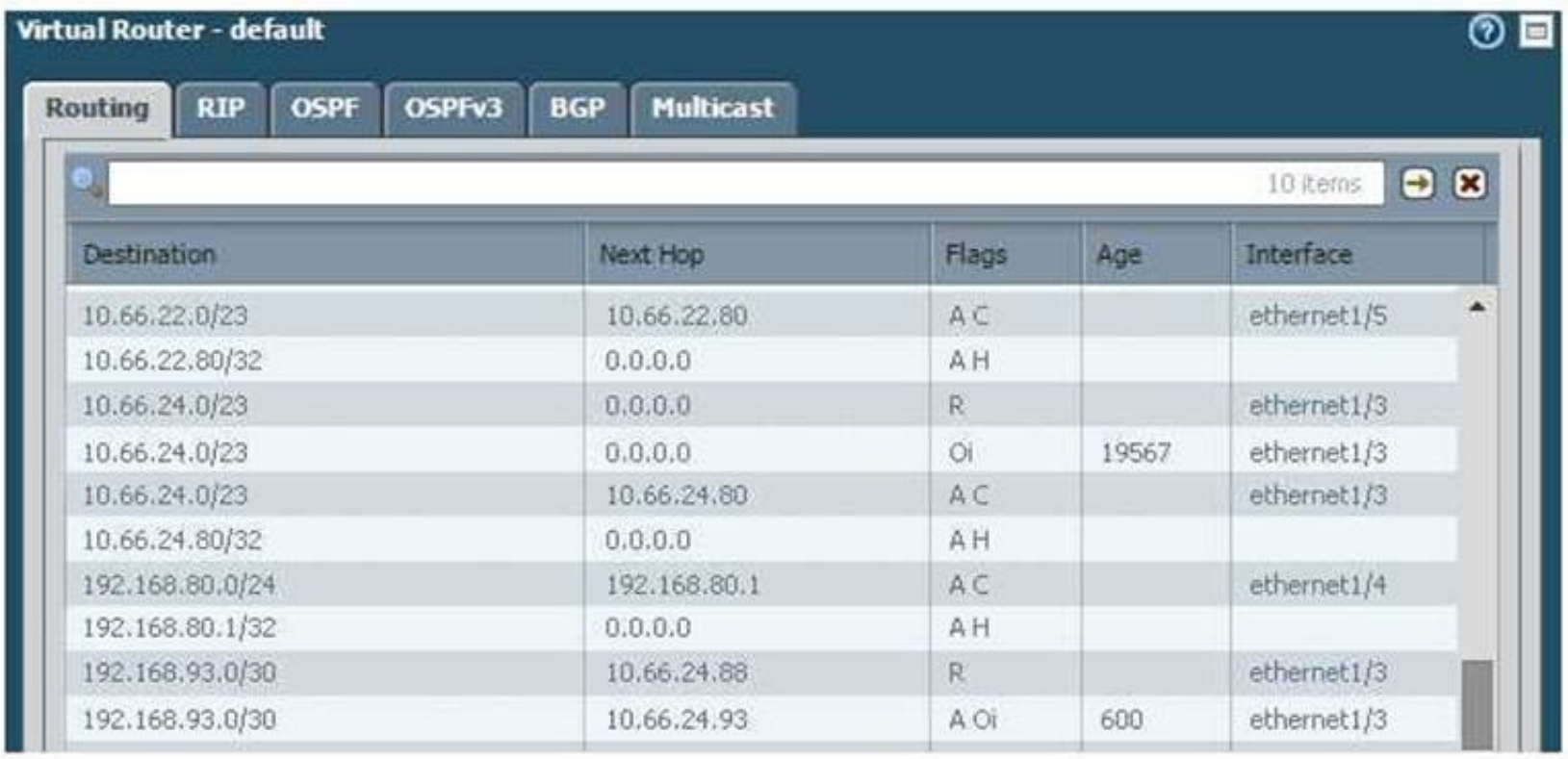
NEW QUESTION 152
Site-A and Site-B have a site-to-site VPN set up between them. OSPF is configured to dynamically create the routes between the sites. The OSPF configuration in Site-A is configured properly, but the route for the tunner is not being established. The Site-B interfaces in the graphic are 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 153
Given the following table.



Destination	Next Hop	Flags	Age	Interface
10.66.22.0/23	10.66.22.80	A C		ethernet1/5
10.66.22.80/32	0.0.0.0	A H		
10.66.24.0/23	0.0.0.0	R		ethernet1/3
10.66.24.0/23	0.0.0.0	Oi	19567	ethernet1/3
10.66.24.0/23	10.66.24.80	A C		ethernet1/3
10.66.24.80/32	0.0.0.0	A H		
192.168.80.0/24	192.168.80.1	A C		ethernet1/4
192.168.80.1/32	0.0.0.0	A H		
192.168.93.0/30	10.66.24.88	R		ethernet1/3
192.168.93.0/30	10.66.24.93	A Oi	600	ethernet1/3

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 155
A VPN connection is set up between Site-A and Site-B, but no traffic is passing in the system log of Site-A, there is an event logged as like-nego-p1-fail-psk.
What action will bring the VPN up and allow traffic to start passing between the sites?

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

Answer: D

NEW QUESTION 157
A company is upgrading its existing Palo Alto Networks firewall from version 7.0.1 to 7.0.4.
Which three methods can the firewall administrator use to install PAN-OS 8.0.4 across the enterprise?(Choose three)

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

Answer: ACF

NEW QUESTION 159
A logging infrastructure may need to handle more than 10,000 logs per second. Which two options support a dedicated log collector function? (Choose two)

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

Answer: BC

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

NEW QUESTION 161
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 166
A company hosts a publically accessible web server behind a Palo Alto Networks next generation firewall with the following configuration information.
Users outside the company are in the "Untrust-L3" zone The web server physically resides in the "Trust-L3" zone. Web server public IP address: 23.54.6.10
Web server private IP address: 192.168.1.10
Which two items must be NAT policy contain to allow users in the untrust-L3 zone to access the web server? (Choose two)

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

Answer: CD

NEW QUESTION 169
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 172
What are three valid actions in a File Blocking Profile? (Choose three)

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

Answer: ABC

Explanation:
https://live.paloaltonetworksHYPERLINK "https://live.paloaltonetworks.com/t5/Configuration-Articles/File-Blocking-Rulebase-and-Action-Precedence/ta-p/53623".com/t5/Configuration- ArticHYPERLINK "https://live.paloaltonetworks.com/t5/Configuration-Articles/File-Blocking-Rulebase-and-Action-Precedence/ta-p/53623"les/File-Blocking-RulebHYPERLINK "https://live.paloaltonetworks.com/t5/Configuration-Articles/File-Blocking-Rulebase-and-Action-Precedence/ta-p/53623"ase-and-Action-Precedence/ta-p/53623

NEW QUESTION 175
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 179
Which three log-forwarding destinations require a server profile to be configured? (Choose three)

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

Answer: ABF

NEW QUESTION 181
An Administrator is configuring an IPSec VPN to a Cisco ASA at the administrator's home and experiencing issues completing the connection. The following is th output from the command:

less mp-log ikemgr.log:

```
less mp-log ikemgr.log:

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

What could be the cause of this problem?

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

Answer: B

NEW QUESTION 183
How does Panorama handle incoming logs when it reaches the maximum storage capacity?

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

Answer: D

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

NEW QUESTION 185
Which client software can be used to connect remote Linux client into a Palo Alto Networks Infrastructure without sacrificing the ability to scan traffic and protect against threats?

A. X-Auth IPsec VPN
B. GlobalProtect Apple IOS
C. GlobalProtect SSL
D. GlobalProtect Linux

Answer: A

Explanation:
(http://blog.webernetz.net/2014/03/31/palo-alto-globalprotect-for-linux-with-vpnc/)

NEW QUESTION 188
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 190
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 193
A network security engineer has been asked to analyze Wildfire activity. However, the Wildfire Submissions item is not visible form the Monitor tab.
What could cause this condition?

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

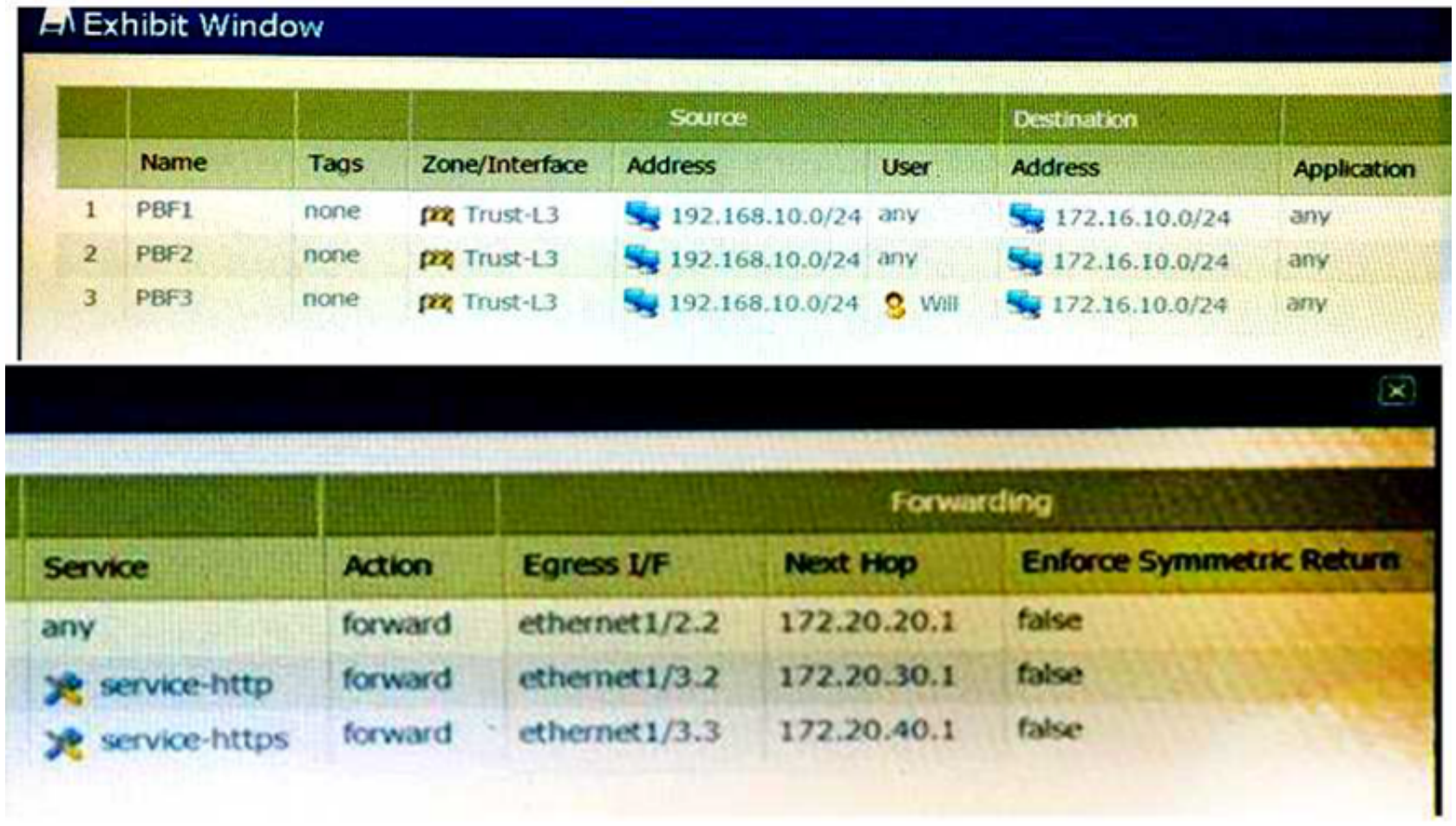
Answer: B

NEW QUESTION 196
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 198
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 200
Which three function are found on the dataplane of a PA-5050? (Choose three)

A. Protocol Decoder
B. Dynamic routing
C. Management
D. Network Processing
E. Signature Match

Answer: BDE

NEW QUESTION 205
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 208
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 212
Which interface configuration will accept specific VLAN IDs?

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

Answer: B

NEW QUESTION 214
Support for which authentication method was added in PAN-OS 8.0?

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

Answer: D

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

NEW QUESTION 217
A company.com wants to enable Application Override. Given the following screenshot:

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

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

Answer: AC

NEW QUESTION 221
A network design calls for a "router on a stick" implementation with a PA-5060 performing inter- VLAN routing All VLAN-tagged traffic will be forwarded to the PA-5060 through a single dot1q trunk interface
Which interface type and configuration setting will support this design?

A. Trunk interface type with specified tag
B. Layer 3 interface type with specified tag
C. Layer 2 interface type with a VLAN assigned
D. Layer 3 subinterface type with specified tag

Answer: D

NEW QUESTION 226
A Network Administrator wants to deploy a Large Scale VPN solution. The Network Administrator has chosen a GlobalProtect Satellite solution. This configuration needs to be deployed to multiple remote offices and the Network Administrator decides to use Panorama to deploy the configurations.
How should this be accomplished?

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

Answer: B

NEW QUESTION 228
Which option is an IPv6 routing protocol?

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

Answer: B

NEW QUESTION 231
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 234
Which URL Filtering Security Profile action togs the URL Filtering category to the URL Filtering log?

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

Answer: B

NEW QUESTION 235
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 237
Several offices are connected with VPNs using static IPV4 routes. An administrator has been tasked with implementing OSPF to replace static routing.
Which step is required to accoumplish this goal?

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

Answer: C

NEW QUESTION 242
Which Panorama feature allows for logs generated by Panorama to be forwarded to an external Security Information and Event Management(SIEM) system?

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

D. Collector Log Forwarding for Collector Groups

Answer: A

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

NEW QUESTION 246
A file sharing application is being permitted and no one knows what this application is used for. How should this application be blocked?

A. Block all unauthorized applications using a security policy
B. Block all known internal custom applications
C. Create a WildFire Analysis Profile that blocks Layer 4 and Layer 7 attacks
D. Create a File blocking profile that blocks Layer 4 and Layer 7 attacks

Answer: D

NEW QUESTION 248
Which CLI command displays the current management plane memory utilization?

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

Answer: D

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

NEW QUESTION 252
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 257
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 258
Which field is optional when creating a new Security Policy rule?

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

Answer: B

NEW QUESTION 259

.....

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