# Paloalto-Networks

## Exam Questions PCNSE

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

**NEW QUESTION 1**
- (Exam Topic 2)
An Administrator is configuring Authentication Enforcement and they would like to create an exemption rule to exempt a specific group from authentication. Which authentication enforcement object should they select?

A. default-browser-challenge
B. default-authentication-bypass
C. default-web-format
D. default-no-captive-portal

**Answer:** D

**NEW QUESTION 2**
- (Exam Topic 2)
Which option is part of the content inspection process?

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

**Answer:** B

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

**NEW QUESTION 3**
- (Exam Topic 2)
An administrator has been asked to configure active/active HA for a pair of Palo Alto Networks NGFWs. The firewall use Layer 3 interfaces to send traffic to a single gateway IP for the pair.
Which configuration will enable this HA scenario?

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

**Answer:** A

**NEW QUESTION 4**
- (Exam Topic 2)
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 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)
An administrator has users accessing network resources through Citrix XenApp 7 x. Which User-ID mapping solution will map multiple users who are using Citrix to connect to the network and access resources?

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

**Answer:**

C

**NEW QUESTION 7**
- (Exam Topic 2)
Which menu item enables a firewall administrator to see details about traffic that is currently active through the NGFW?

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

**Answer:** C

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

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

**Answer:** AC

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

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

**Answer:** D

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

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

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

**Answer:** C

**NEW QUESTION 14**
- (Exam Topic 2)
An administrator needs to upgrade a Palo Alto Networks NGFW to the most current version of PAN-OS® software. The firewall has internet connectivity through an Ethernet interface, but no internet connectivity from the management interface. The Security policy has the default security rules and a rule that allows all web-browsing traffic from any to any zone. What must the administrator configure so that the PAN-OS® software can be upgraded?

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

D. Scheduler

**Answer:** A

**NEW QUESTION 16**
- (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. Virtual Wire mode
C. content inspection
D. redistribution of user mappings

**Answer:** D

**Explanation:**
Reference:
https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/user-id/deploy-user-id-in-a-large-scale-net

**NEW QUESTION 17**
- (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 18**
- (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 22**
- (Exam Topic 2)
Refer to the exhibit.

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

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

**Answer:** CD

**NEW QUESTION 23**
- (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 28**
- (Exam Topic 2)
An administrator has been asked to create 100 virtual firewalls in a local, on-premise lab environment (not in “the cloud”). Bootstrapping is the most expedient way to perform this task.
Which option describes deployment of a bootstrap package in an on-premise virtual environment?

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

**Answer:** D

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

**NEW QUESTION 32**
- (Exam Topic 2)
Which two features does PAN-OS® software use to identify applications? (Choose two)

A. port number
B. session number
C. transaction characteristics
D. application layer payload

**Answer:** AD

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

**NEW QUESTION 33**
- (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 34**
- (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 35**
- (Exam Topic 2)
A bootstrap USB flash drive has been prepared using a Windows workstation to load the initial configuration of a Palo Alto Networks firewall that was previously being used in a lab. The USB flash drive was formatted using file system FAT32 and the initial configuration is stored in a file named init-cfg txt. The firewall is currently running PAN-OS 10.0 and using a lab config The contents of init-cfg txi in the USB flash drive are as follows:

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 39**
- (Exam Topic 2)
Which option would an administrator choose to define the certificate and protocol that Panorama and its managed devices use for SSL/TLS services?

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

**Answer:** D

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

**NEW QUESTION 43**
- (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 47**
- (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 51**
- (Exam Topic 2)
The firewall is not downloading IP addresses from MineMeld. Based, on the image, what most likely is wrong?

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

**Answer:** D

**NEW QUESTION 54**
- (Exam Topic 2)
A company wants to install a PA-3060 firewall between two core switches on a VLAN trunk link. They need to assign each VLAN to its own zone and to assign untagged (native) traffic to its own zone which options differentiates multiple VLAN into separate zones?

A. Create V-Wire objects with two V-Wire interfaces and define a range of "0-4096 in the "Tag Allowed" field of the V-Wire object.
B. Create V-Wire objects with two V-Wire subinterfaces and assign only a single VLAN ID to the Tag Allowed" field of the V-Wire objec
C. Repeat for every additional VLAN and use a VLAN ID of 0 for untagged traffi
D. Assign each iinterface/sub interface to a unique zone.
E. Create Layer 3 subinterfaces that are each assigned t
F. single VLAN ID and a common virtual router.The physical Layer 3 interface would handle untagged traffi

G. Assign each interface/subinterface t
H. unique zon
I. Do not assign any interface an IP address.
J. Create VLAN objects for each VLAN and assign VLAN interfaces matching each VLAN I
K. Repeat for every additional VLAN and use a VLAN ID of 0 for untagged traffi
L. Assign each interface/sub interface to a unique zone.

**Answer:** B

**Explanation:**
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/networking/configure-interfaces/virtual-wire-interfa Virtual wire interfaces by default allow all untagged traffic. You can, however, use a virtual wire to connect
two interfaces and configure either interface to block or allow traffic based on the virtual LAN (VLAN) tags. VLAN tag 0 indicates untagged traffic.You can also create multiple subinterfaces, add them into different
zones, and then classify traffic according to a VLAN tag or a combination of a VLAN tag with IP classifiers (address, range, or subnet) to apply granular policy control for specific VLAN tags or for VLAN tags from a specific source IP address, range, or subnet.

**NEW QUESTION 59**
- (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 64**
- (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 67**
- (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 69**
- (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 74**
- (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 79**
- (Exam Topic 2)
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:** B

**NEW QUESTION 83**
- (Exam Topic 2)
Updates to dynamic user group membership are automatic therefore using dynamic user groups instead of static group objects allows you to:

A. respond to changes in user behavior or potential threats using manual policy changes
B. respond to changes in user behavior or potential threats without automatic policy changes
C. respond to changes in user behavior and confirmed threats with manual policy changes
D. respond to changes in user behavior or potential threats without manual policy changes

**Answer:** D

**Explanation:**
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/user-id-features/dynamic-user-groups#:~:tex

**NEW QUESTION 87**
- (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 89**
- (Exam Topic 2)
A customer wants to set up a VLAN interface for a Layer 2 Ethernet port.
Which two mandatory options are used to configure a VLAN interface? (Choose two.)

A. Virtual router

B. Security zone
C. ARP entries
D. Netflow Profile

**Answer:** AB

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

**NEW QUESTION 90**
- (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 95**
- (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 97**
- (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 102**
- (Exam Topic 2)
An administrator needs to upgrade an NGFW to the most current version of PAN-OS® software. The following is occurring:
•Firewall has Internet connectivity through e1/1.
•Default security rules and security rules allowing all SSL and web-browsing traffic to and from any zone.
•Service route is configured, sourcing update traffic from e1/1.
•A communication error appears in the System logs when updates are performed.
•Download does not complete.
What must be configured to enable the firewall to download the current version of PAN-OS software?

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

**Answer:** D

**NEW QUESTION 107**
- (Exam Topic 2)
Which data flow describes redistribution of user mappings?

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

**Answer:** B

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

**NEW QUESTION 111**
- (Exam Topic 2)
If a template stack is assigned to a device and the stack includes three templates with overlapping settings, which settings are published to the device when the template stack is pushed?

A. The settings assigned to the template that is on top of the stack.
B. The administrator will be promoted to choose the settings for that chosen firewall.
C. All the settings configured in all templates.
D. Depending on the firewall location, Panorama decides with settings to send.

**Answer:** A

**Explanation:**
Reference:
https://www.paloaltonetworks.com/documentation/80/panorama/panorama_adminguide/manage-firewalls/mana templates-and-template-stacks/configure-a-template-stack

**NEW QUESTION 114**
- (Exam Topic 2)
Based on the following image,

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

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

**Answer:** B

**NEW QUESTION 115**
- (Exam Topic 2)
If the firewall is configured for credential phishing prevention using the “Domain Credential Filter” method, which login will be detected as credential theft?

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

**Answer:** A

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

**NEW QUESTION 120**
- (Exam Topic 2)
Which PAN-OS® policy must you configure to force a user to provide additional credentials before he is allowed to access an internal application that contains highly-sensitive business data?

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

**Answer:** C

**NEW QUESTION 121**
- (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 124**
- (Exam Topic 2)
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 127**
- (Exam Topic 2)
An administrator sees several inbound sessions identified as unknown-tcp in the Traffic logs. The administrator determines that these sessions are form external users accessing the company's proprietary accounting application. The administrator wants to reliably identify this traffic as their accounting application and to scan this traffic for threats.
Which option would achieve this result?

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

**Answer:** A

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

**NEW QUESTION 131**
- (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 133**
- (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 137**
- (Exam Topic 2)
Which User-ID method maps IP address to usernames for users connecting through a web proxy that has already authenticated the user?

A. Client Probing
B. Port mapping
C. Server monitoring
D. Syslog listening

**Answer:** D

**Explanation:**
To obtain user mappings from existing network services that authenticate users—such as wireless controllers, 802.1x devices, Apple Open Directory servers, proxy servers, or other Network Access Control (NAC) mechanisms—Configure User-ID to Monitor Syslog Senders for User Mapping.While you can configure either the Windows agent or the PAN-OS integrated User-ID agent on the firewall to listen for authentication syslog messages from the network services, because only the PAN-OS integrated agent supports syslog listening over TLS, it is the preferred configuration.

**NEW QUESTION 142**
- (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 143**
- (Exam Topic 2)
In High Availability, which information is transferred via the HA data link?

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

**Answer:** A

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

**NEW QUESTION 144**
- (Exam Topic 2)
Exhibit:

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 146**
- (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 147**
- (Exam Topic 2)
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:**
https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/user-id/user-id-concepts/user-mapping/xml-api.ht

**NEW QUESTION 151**
- (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 152**
- (Exam Topic 1)
Which CLI command displays the physical media that are connected to ethernetl/8?

A. > show system state filter-pretty sys.si.p8.stats
B. > show interface ethernetl/8
C. > show system state filter-pretty sys.sl.p8.phy
D. > show system state filter-pretty sys.si.p8.med

**Answer:** D

**NEW QUESTION 156**
- (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 159**
- (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 163**
- (Exam Topic 1)
In a firewall, which three decryption methods are valid? (Choose three )

A. SSL Inbound Inspection
B. SSL Outbound Proxyless Inspection
C. SSL Inbound Proxy
D. Decryption Mirror
E. SSH Proxy

**Answer:** ADE

**NEW QUESTION 166**
- (Exam Topic 1)
Given the following snippet of a WildFire submission log. did the end-user get access to the requested information and why or why not?

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

**Answer:** B

**NEW QUESTION 167**
- (Exam Topic 1)
PBF can address which two scenarios? (Select Two)

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

**Answer:** AC

**NEW QUESTION 169**
- (Exam Topic 1)
Match each type of DoS attack to an example of that type of attack

A. Mastered
B. Not Mastered

**Answer:** A

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

Application-Based Attacks
—Target weaknesses in a particular application and try to exhaust its resources so legitimate users can't use it. An example of this is the Slowloris attack.
Protocol-Based Attacks
—Also known as state-exhaustion attacks, these attacks target protocol weaknesses. A common example is a SYN flood attack.
Volumetric Attacks
—High-volume attacks that attempt to overwhelm the available network resources, especially bandwidth, and bring down the target to prevent legitimate users from accessing those resources. An example of this is a UDP flood attack.
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/zone-protection-and-dos-protection/zone-defense.ht

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

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

**Answer:** B

**NEW QUESTION 175**
- (Exam Topic 1)
When overriding a template configuration locally on a firewall, what should you consider?

A. Only Panorama can revert the override
B. Panorama will lose visibility into the overridden configuration
C. Panorama will update the template with the overridden value
D. The firewall template will show that it is out of sync within Panorama

**Answer:** B

**NEW QUESTION 179**
- (Exam Topic 1)
An internal system is not functioning The firewall administrator has determined that the incorrect egress interface is being used After looking at the configuration, the administrator believes that the firewall is not using a static route
What are two reasons why the firewall might not use a static route"? (Choose two.)

A. no install on the route
B. duplicate static route
C. path monitoring on the static route
D. disabling of the static route

**Answer:** C

**NEW QUESTION 184**

- (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 187**
- (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 188**
- (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-lntermediate-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-lntermediate-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 191**
- (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 193**
- (Exam Topic 1)
An administrator cannot see any Traffic logs from the Palo Alto Networks NGFW in Panorama reports. The configuration problem seems to be on the firewall Which settings, if configured incorrectly, most likely would stop only Traffic logs from being sent from the NGFW to Panorama?
A)

B)

C)

D)

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

**Answer:** B

**NEW QUESTION 194**
- (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 196**
- (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 197**
- (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 201**
- (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 203**
- (Exam Topic 1)
An administrator needs to troubleshoot a User-ID deployment The administrator believes that there is an issue related to LDAP authentication The administrator wants to create a packet capture on the management plane
Which CLI command should the administrator use to obtain the packet capture for validating the configuration^

A. > ftp export mgmt-pcap from mgmt.pcap to <FTP host>
B. > scp export mgmt-pcap from mgmt.pcap to {usernameQhost:path>
C. > scp export pcap-mgmt from pcap.mgiat to (username@host:path)
D. > scp export pcap from pcap to (usernameQhost:path)

**Answer:** C

**NEW QUESTION 208**
- (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 209**
- (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 212**
- (Exam Topic 1)
An administrator is considering upgrading the Palo Alto Networks NGFW and central management Panorama version
What is considered best practice for this scenario?

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

**Answer:** A

**NEW QUESTION 213**
- (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 218**
- (Exam Topic 1)
Given the following configuration, which route is used for destination 10.10.0.4?

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

**Answer:** A

**NEW QUESTION 221**
- (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 224**
- (Exam Topic 1)
An administrator has 750 firewalls The administrator's central-management Panorama instance deploys dynamic updates to the firewalls
The administrator notices that the dynamic updates from Panorama do not appear on some of the firewalls If Panorama pushes the configuration of a dynamic update schedule to managed firewalls, but the
configuration does not appear what is the root cause?

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

**Answer:** D

**NEW QUESTION 228**
- (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 233**
- (Exam Topic 2)
Which two settings can be configured only locally on the firewall and not pushed from a Panorama template or template stack? (Choose two)

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

**Answer:** AC

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

**NEW QUESTION 237**
- (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 239**
- (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 240**
- (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 244**
- (Exam Topic 2)
An administrator wants a new Palo Alto Networks NGFW to obtain automatic application updates daily, so it is configured to use a scheduler for the application database. Unfortunately, they required the management network to be isolated so that it cannot reach the internet. Which configuration will enable the firewall to download and install application updates automatically?

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

**Answer:** D

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

**NEW QUESTION 245**
- (Exam Topic 2)
Refer to the exhibit.

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

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

**Answer:** BE

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

**NEW QUESTION 248**
- (Exam Topic 2)
A web server is hosted in the DMZ, and the server is configured to listen for incoming connections only on TCP port 8080. A Security policy rule allowing access from the Trust zone to the DMZ zone need to be configured to enable we browsing access to the server.
Which application and service need to be configured to allow only cleartext web-browsing traffic to thins server on tcp/8080.

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

**Answer:** D

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

**NEW QUESTION 251**
- (Exam Topic 2)
How does an administrator schedule an Applications and Threats dynamic update while delaying installation of the update for a certain amount of time?

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

**Answer:** A

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

**NEW QUESTION 252**
- (Exam Topic 2)
An administrator has been asked to configure a Palo Alto Networks NGFW to provide protection against external hosts attempting to exploit a flaw in an operating system on an internal system.
Which Security Profile type will prevent this attack?

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

**Answer:** A

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

**NEW QUESTION 253**
- (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 256**
- (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 260**
- (Exam Topic 2)
Which method does an administrator use to integrate all non-native MFA platforms in PAN-OS® software?

A. Okta
B. DUO

C. RADIUS
D. PingID

**Answer:** C

**Explanation:**
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/authentication/authentication-types/multi-factor-aut

**NEW QUESTION 265**
- (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 266**
- (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 267**
- (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 268**
- (Exam Topic 3)
A network security engineer is asked to provide a report on bandwidth usage. Which tab in the ACC provides the information needed to create the report?

A. Blocked Activity
B. Bandwidth Activity
C. Threat Activity
D. Network Activity

**Answer:** D

**NEW QUESTION 271**
- (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 276**
- (Exam Topic 3)
Which three function are found on the dataplane of a PA-5050? (Choose three)

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

**Answer:** BDE

**NEW QUESTION 281**
- (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 284**
- (Exam Topic 3)
Which Device Group option is assigned by default in Panorama whenever a new device group is created to manage a Firewall?

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

**Answer:** C

**NEW QUESTION 286**
- (Exam Topic 3)
During the packet flow process, which two processes are performed in application identification? (Choose two.)

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

**Answer:** AD

**NEW QUESTION 289**
- (Exam Topic 3)
A network security engineer has been asked to analyze Wildfire activity. However, the Wildfire Submissions item is not visible form the Monitor tab.
What could cause this condition?

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

**Answer:** B

**NEW QUESTION 291**
- (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 295**
- (Exam Topic 3)
How are IPV6 DNS queries configured to user interface ethernet1/3?

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

**Answer:** D

**NEW QUESTION 300**
- (Exam Topic 3)
Which command can be used to validate a Captive Portal policy?

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

**Answer:** C

**NEW QUESTION 301**
- (Exam Topic 3)
A network security engineer needs to configure a virtual router using IPv6 addresses. Which two routing options support these addresses? (Choose two)

A. BGP not sure
B. OSPFv3
C. RIP
D. Static Route

**Answer:** BD

**Explanation:**
https://live.paloaltonetworks.com/t5/Management-Articles/Does-PAN-OS-Support-Dynamic-Routing-Protocols

**NEW QUESTION 306**
- (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 311**
- (Exam Topic 3)
Which two interface types can be used when configuring GlobalProtect Portal?(Choose two)

A. Virtual Wire
B. Loopback
C. Layer 3
D. Tunnel

**Answer:** BC

**NEW QUESTION 316**
- (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 320**
- (Exam Topic 3)
Which three rule types are available when defining policies in Panorama? (Choose three.)

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

**Answer:** ABC

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

**NEW QUESTION 321**
- (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 325**
- (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 328**
- (Exam Topic 3)
An Administrator is configuring an IPSec VPN toa Cisco ASA at the administrator's home and experiencing issues completing the connection. The following is th output from the command:
less mp-log ikemgr.log:

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 330**
- (Exam Topic 3)
How does Panorama handle incoming logs when it reaches the maximum storage capacity?

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

**Answer:** D

**Explanation:**

(https://www.paloaltonetworks.com/documentation/60/panorama/panorama_adminguide/set-up-panorama/deter

**NEW QUESTION 334**
- (Exam Topic 3)
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 338**
- (Exam Topic 3)

What will be the source address in the ICMP packet?

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

**Answer:** C

**NEW QUESTION 341**
- (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 346**
- (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 347**
- (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 351**

- (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.

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 354**
- (Exam Topic 3) A
users traffic traversing a Palo Alto networks NGFW sometimes can reach http //www company com At other times the session times out. At other times the session times out The NGFW has been configured with a PBF rule that the user traffic matches when it goes to http://www.company.com goes to http://www company com
How can the firewall be configured to automatically disable the PBF rule if the next hop goes down?

A. Create and add a monitor profile with an action of fail over in the PBF rule in question
B. Create and add a monitor profile with an action of wait recover in the PBF rule in question
C. Configure path monitoring for the next hop gateway on the default route in the virtual router
D. Enable and configure a link monitoring profile for the external interface of the firewall

**Answer:** C

**NEW QUESTION 357**
- (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 359**
- (Exam Topic 3)
An administrator has left a firewall to use the data of port for all management service which there functions are performed by the data face? (Choose three.)

A. NTP

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

**Answer:** ACD

**NEW QUESTION 360**
- (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 364**
- (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 367**
- (Exam Topic 3)
Which CLI command displays the current management plan memory utilization?

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

**Answer:** B

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

**NEW QUESTION 372**
- (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 377**
- (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 378**
- (Exam Topic 3)
People are having intermittent quality issues during a live meeting via web application.

A. Use QoS profile to define QoS Classes
B. Use QoS Classes to define QoS Profile
C. Use QoS Profile to define QoS Classes and a QoS Policy
D. Use QoS Classes to define QoS Profile and a QoS Policy

**Answer:** C

**NEW QUESTION 379**
- (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 381**
- (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 383**
- (Exam Topic 3)
What are three possible verdicts that WildFire can provide for an analyzed sample? (Choose three)

A. Clean
B. Bengin
C. Adware
D. Suspicious
E. Grayware
F. Malware

**Answer:** BEF

**Explanation:**
https://www.paloaltonetworks.com/documentation/70/pan-os/newfeaturesguide/wildfire-features/wildfire-grayw

**NEW QUESTION 384**
- (Exam Topic 3)
A company hosts a publicly accessible web server behind a Palo Alto Networks next-generation firewall with the following configuration information:
* Users outside the company are in the "Untrust-L3" zone.
* The web server physically resides in the "Trust-L3" zone.
* Web server public IP address: 23.54.6.10
* Web server private IP address: 192.168.1.10
Which two items must the NAT policy contain to allow users in the Untrust-L3 zone to access the web server? (Choose two.)

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

**Answer:** AB

**NEW QUESTION 387**
- (Exam Topic 3)
A company hosts a publically accessible web server behind a Palo Alto Networks next generation firewall with the following configuration information.
Users outside the company are in the "Untrust-L3" zone
The web server physically resides in the "Trust-L3" zone.
Web server public IP address: 23.54.6.10
Web server private IP address: 192.168.1.10
Which two items must be NAT policy contain to allow users in the untrust-L3 zone to access the web server? (Choose two)

A. Untrust-L3 for both Source and Destination zone

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

**Answer:** CD

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

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

**Answer:** B

**NEW QUESTION 394**
- (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 396**
- (Exam Topic 3)
A network security engineer has a requirement to allow an external server to access an internal web server. The internal web server must also initiate connections with the external server.
What can be done to simplify the NAT policy?

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

**Answer:** C

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

**NEW QUESTION 397**
- (Exam Topic 3)
Palo Alto Networks maintains a dynamic database of malicious domains.
Which two Security Platform components use this database to prevent threats? (Choose two)

A. Brute-force signatures
B. BrightCloud Url Filtering
C. PAN-DB URL Filtering
D. DNS-based command-and-control signatures

**Answer:** CD

**NEW QUESTION 398**
- (Exam Topic 3)
Which Security Policy Rule configuration option disables antivirus and anti-spyware scanning of server-to-client flows only?

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

**Answer:** A

**NEW QUESTION 403**
......