# Exam Questions PCNSE

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

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

**NEW QUESTION 1**
- (Exam Topic 2)
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)
A global corporate office has a large-scale network with only one User-ID agent, which creates a bottleneck near the User-ID agent server. Which solution in PAN-OS® software would help in this case?

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

**Answer:** B

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

**NEW QUESTION 4**
- (Exam Topic 2)
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 5**
- (Exam Topic 2)
During the packet flow process, which two processes are performed in application identification? (Choose two.)

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

**Answer:** AB

**Explanation:**

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

**NEW QUESTION 6**
- (Exam Topic 2)
Which version of GlobalProtect supports split tunneling based on destination domain, client process, and HTTP/HTTPS video streaming application?

A. GlobalProtect version 4.0 with PAN-OS 8.1
B. GlobalProtect version 4.1 with PAN-OS 8.1
C. GlobalProtect version 4.1 with PAN-OS 8.0

D. GlobalProtect version 4.0 with PAN-OS 8.0

**Answer:** B

**NEW QUESTION 7**
- (Exam Topic 2)
Which log file can be used to identify SSL decryption failures?

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

**Answer:** D

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

**NEW QUESTION 8**
- (Exam Topic 2)
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 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 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 10**
- (Exam Topic 2)
Which protection feature is available only in a Zone Protection Profile?

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

C. Port Scan Protection
D. UDP Flood Protections

**Answer:** A

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

**NEW QUESTION 12**
- (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 14**
- (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 18**
- (Exam Topic 2)
How can a candidate or running configuration be copied to a host external from Panorama?

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

**Answer:** D

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

**NEW QUESTION 19**
- (Exam Topic 2)
Starling with PAN-OS version 9.1, GlobalProtect logging information is now recorded in which firewall log?

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

**Answer:** C

**NEW QUESTION 24**
- (Exam Topic 2)
What are the differences between using a service versus using an application for Security Policy match?

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

**Answer:** B

**NEW QUESTION 26**
- (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 27**
- (Exam Topic 2)
What should an administrator consider when planning to revert Panorama to a pre-PAN-OS 8.1 version?

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

**Answer:** A

**NEW QUESTION 28**
- (Exam Topic 2)
An administrator has enabled OSPF on a virtual router on the NGFW. OSPF is not adding new routes to the virtual router. Which two options enable the administrator to troubleshoot this issue? (Choose two.)

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

**Answer:** AB

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

**NEW QUESTION 29**
- (Exam Topic 2)
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. Exhibit A
B. Exhibit B
C. Exhibit C
D. Exhibit D

**Answer:** AD

**NEW QUESTION 33**
- (Exam Topic 2)
An administrator sees several inbound sessions identified as unknown-tcp in the traffic logs. The administrator determines that these sessions are from external users accessing the company's proprietary accounting application. The administrator wants to reliably identify this as their accounting application and to scan this traffic for threats. Which option would achieve this result?

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

**Answer:** D

**NEW QUESTION 36**
- (Exam Topic 2)
An administrator is using Panorama and multiple Palo Alto Networks NGFWs. After upgrading all devices to the latest PAN-OS® software, the administrator enables log forwarding from the firewalls to PanoramA.
Pre-existing logs from the firewalls are not appearing in PanoramA.
Which action would enable the firewalls to send their pre-existing logs to Panorama?

A. Use the import option to pull logs into Panorama.
B. A CLI command will forward the pre-existing logs to Panorama.

C. Use the ACC to consolidate pre-existing logs.
D. The log database will need to exported form the firewalls and manually imported into Panorama.

**Answer:** B

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

**NEW QUESTION 38**
- (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 40**
- (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 42**
- (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 43**
- (Exam Topic 2)
The firewall is not downloading IP addresses from MineMeld. Based, on the image, what most likely is wrong?

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

**Answer:** D

**NEW QUESTION 47**
- (Exam Topic 2)
An administrator 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. Configuration Logs
B. System Logs
C. Task Manager
D. Traffic Logs

**Answer:** BC

**NEW QUESTION 51**
- (Exam Topic 2)
SD-WAN is designed to support which two network topology types? (Choose two.)

A. ring
B. point-to-point
C. hub-and-spoke
D. full-mesh

**Answer:** CD

**NEW QUESTION 52**
- (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 55**
- (Exam Topic 2)
To more easily reuse templates and template slacks , you can create term plate variables in place of firewall-specific and appliance-specific IP literals in your configurations
Which one is the correct configuration?

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

**Answer:** D

**NEW QUESTION 56**
- (Exam Topic 2)
Which Palo Alto Networks VM-Series firewall is valid?

A. VM-25
B. VM-800
C. VM-50
D. VM-400

**Answer:** C

**Explanation:**
Reference:
https://www.paloaltonetworks.com/products/secure-the-network/virtualized-next-generation-firewall/vm-series
https://docs.paloaltonetworks.com/vm-series/9-0/vm-series-deployment/about-the-vm-series-firewall/vm-series

**NEW QUESTION 61**
- (Exam Topic 2)
An administrator creates a custom application containing Layer 7 signatures. The latest application and threat dynamic update is downloaded to the same NGFW. The update contains an application that matches the same traffic signatures as the custom application. Which application should be used to identify traffic traversing the NGFW?

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

**Answer:** C

**NEW QUESTION 65**
- (Exam Topic 2)
An administrator is defining protection settings on the Palo Alto Networks NGFW to guard against resource exhaustion. When platform utilization is considered, which steps must the administrator take to configure and apply packet buffer protection?

A. Enable and configure the Packet Buffer protection thresholds.Enable Packet Buffer Protection per ingress zone.
B. Enable and then configure Packet Buffer thresholdsEnable Interface Buffer protection.
C. Create and Apply Zone Protection Profiles in all ingress zones.Enable Packet Buffer Protection per ingress zone.
D. Configure and apply Zone Protection Profiles for all egress zones.Enable Packet Buffer Protection pre egress zone.
E. Enable per-vsys Session Threshold alerts and triggers for Packet Buffer Limits.Enable Zone Buffer Protection per zone.

**Answer:** A

**NEW QUESTION 70**
- (Exam Topic 2)

If an administrator does not possess a website's certificate, which SSL decryption mode will allow the Palo Alto networks NGFW to inspect when users browse to HTTP(S) websites?

A. SSL Forward Proxy
B. SSL Inbound Inspection
C. TLS Bidirectional proxy
D. SSL Outbound Inspection

**Answer:** A

**Explanation:**
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClV8CAK

**NEW QUESTION 74**
- (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 76**
- (Exam Topic 2)
Which three options are supported in HA Lite? (Choose three.)

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

**Answer:** BCD

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

**NEW QUESTION 78**
- (Exam Topic 2)
An administrator needs to implement an NGFW between their DMZ and Core network. EIGRP Routing between the two environments is required. Which interface type would support this business requirement?

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

**Answer:** A

**NEW QUESTION 81**
- (Exam Topic 2)
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 85**
- (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 90**
- (Exam Topic 2)
The firewall identifies a popular application as an unknown-tcp.
Which two options are available to identify the application? (Choose two.)

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

**Answer:** AD

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

**NEW QUESTION 92**
- (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 96**
- (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 99**
- (Exam Topic 2)
ESTION NO: 94
If an administrator wants to decrypt SMTP traffic and possesses the server's certificate, which SSL decryption mode will allow the Palo Alto Networks NGFW to inspect traffic to the server?

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

**Answer:** B

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

**NEW QUESTION 104**
- (Exam Topic 2)
Which CLI command can be used to export the tcpdump capture?

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

**Answer:** C

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

**NEW QUESTION 105**
- (Exam Topic 2)
Which event will happen if an administrator uses an Application Override Policy?

A. Threat-ID processing time is decreased.
B. The Palo Alto Networks NGFW stops App-ID processing at Layer 4.
C. The application name assigned to the traffic by the security rule is written to the Traffic log.
D. App-ID processing time is increased.

**Answer:** B

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

**NEW QUESTION 109**
- (Exam Topic 2)
Which Zone Pair and Rule Type will allow a successful connection for a user on the internet zone to a web server hosted in the DMZ zone? The web server is reachable using a destination Nat policy in the Palo Alto Networks firewall.

A. Zone Pair:Source Zone: Internet Destination Zone: DMZ Rule Type:“intrazone”
B. Zone Pair:Source Zone: Internet Destination Zone: DMZ Rule Type:“intrazone” or “universal”
C. Zone Pair:Source Zone: Internet Destination Zone: Internet Rule Type:“intrazone” or “universal”
D. Zone Pair:Source Zone: Internet Destination Zone: Internet Rule Type:“intrazone”

**Answer:** B

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

**NEW QUESTION 110**
- (Exam Topic 2)
Which three split tunnel methods are supported by a globalProtect gateway? (Choose three.)

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

**Answer:** ABC

**NEW QUESTION 113**
- (Exam Topic 2)
Refer to exhibit.

An organization has Palo Alto Networks NGFWs that send logs to remote monitoring and security management platforms. The network team has reported excessive traffic on the corporate WAN.
How could the Palo Alto Networks NGFW administrator reduce WAN traffic while maintaining support for all existing monitoring/ security platforms?

A. Forward logs from firewalls only to Panorama and have Panorama forward logs to other external services.
B. Forward logs from external sources to Panorama for correlation, and from Panorama send them to the NGFW.
C. Configure log compression and optimization features on all remote firewalls.
D. Any configuration on an M-500 would address the insufficient bandwidth concerns.

**Answer:** A

**Explanation:**
https://docs.paloaltonetworks.com/panorama/8-1/panorama-admin/panorama-overview/centralized-logging-and

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

**NEW QUESTION 118**
- (Exam Topic 2)
An administrator has configured the Palo Alto Networks NGFW's management interface to connect to the internet through a dedicated path that does not traverse back through the NGFW itself.
Which configuration setting or step will allow the firewall to get automatic application signature updates?

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

**Answer:** A

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

**NEW QUESTION 121**
- (Exam Topic 2)
Which 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-c
"Credential phishing prevention works by scanning username and password submissions to websites and comparing those submissions against valid corporate credentials. You can choose what websites you want to either allow, alert on, or block corporate credential submissions to based on the URL category of the website. Alternatively, you can present a page that warns users against submitting credentials to sites classified in certain URL categories. This gives you the opportunity to educate users against reusing corporate credentials, even on legitimate, non-phishing sites. In the event that corporate credentials are compromised, this feature allows you to identify the user who submitted credentials so that you can remediate."

**NEW QUESTION 123**
- (Exam Topic 2)
A user's traffic traversing a Palo Alto Networks NGFW sometimes can reach http://www.company.com. At other times the session times out. The NGFW has been configured with a PBF rule that the user's traffic matches when it goes to http://www.company.com.
How can the firewall be configured automatically disable the PBF rule if the next hop goes down?

A. Create and add a Monitor Profile with an action of Wait Recover in the PBF rule in question:.
B. Create and add a Monitor Profile with an action of Fail Over in the PBF rule in question.
C. Enable and configure a Link Monitoring Profile for the external interface of the firewall.
D. Configure path monitoring for the next hop gateway on the default route in the virtual router.

**Answer:** B

**Explanation:**
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClFiCAK

**NEW QUESTION 128**
- (Exam Topic 2)
Which CLI command is used to simulate traffic going through the firewall and determine which Security policy rule, NAT translation, static route, or PBF rule will be triggered by the traffic?

A. check
B. find
C. test
D. sim

**Answer:** C

**Explanation:**
Reference: http://www.shanekillen.com/2014/02/palo-alto-useful-cli-commands.html
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClQSCA0

**NEW QUESTION 130**
- (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 133**
- (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 138**
- (Exam Topic 2)
Where can an administrator see both the management plane and data plane CPU utilization in the WebUI?

A. System log
B. CPU Utilization widget
C. Resources widget
D. System Utilization log

**Answer:** C

**Explanation:**
System Resources (widget)Displays the Management CPU usage, Data Plane usage, and the Session Count (the number of sessions established through the firewall or
Panorama).https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-web-interface-help/dashboard/dashboard-widg

**NEW QUESTION 140**
- (Exam Topic 2)
VPN traffic intended for an administrator’s Palo Alto Networks NGFW is being maliciously intercepted and retransmitted by the interceptor. When creating a VPN tunnel, which protection profile can be enabled to prevent this malicious behavior?

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

**Answer:** D

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

**NEW QUESTION 145**
- (Exam Topic 2)
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

**Explanation:**
https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/large-scale-vpn-lsvpn/configure-the-globalprotect

**NEW QUESTION 148**
- (Exam Topic 2)
Which GlobalProtect Client connect method requires the distribution and use of machine certificates?

A. User-logon (Always on)

B. At-boot
C. On-demand
D. Pre-logon

**Answer:** D

**NEW QUESTION 153**
- (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 158**
- (Exam Topic 2)
When configuring a GlobalProtect Portal, what is the purpose of specifying an Authentication Profile?

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

**Answer:** C

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

**NEW QUESTION 163**
- (Exam Topic 2)
Refer to the exhibit.

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

B)

C)

D)

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

**Answer:** A

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

**NEW QUESTION 168**
- (Exam Topic 2)
Which three settings are defined within the Templates object of Panorama? (Choose three.)

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

**Answer:** ABC

**NEW QUESTION 171**
- (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 172**
- (Exam Topic 2)
Which feature can provide NGFWs with User-ID mapping information?

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

**Answer:** A

**NEW QUESTION 174**
- (Exam Topic 2)
An administrator has configured a QoS policy rule and a QoS profile that limits the maximum allowable bandwidth for the YouTube application. However , YouTube is consuming more than the maximum bandwidth allotment configured.
Which configuration step needs to be configured to enable QoS?

A. Enable QoS Data Filtering Profile
B. Enable QoS monitor
C. Enable Qos interface
D. Enable Qos in the interface Management Profile.

**Answer:** C

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

**NEW QUESTION 176**
- (Exam Topic 2)
Which three steps will reduce the CPU utilization on the management plane? (Choose three.)

A. Disable SNMP on the management interface.
B. Application override of SSL application.
C. Disable logging at session start in Security policies.
D. Disable predefined reports.
E. Reduce the traffic being decrypted by the firewall.

**Answer:** ACD

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

**NEW QUESTION 178**
- (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 182**
- (Exam Topic 2)
An administrator using an enterprise PKI needs to establish a unique chain of trust to ensure mutual authentication between Panorama and the managed firewalls and Log Collectors.
How would the administrator establish the chain of trust?

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

**Answer:** A

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

**NEW QUESTION 184**
- (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 185**
- (Exam Topic 2)
Which two subscriptions are available when configuring panorama to push dynamic updates to connected devices? (Choose two.)

A. Content-ID
B. User-ID
C. Applications and Threats
D. Antivirus

**Answer:** CD

**Explanation:**
Reference:
https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/device/device-dynamic-update

**NEW QUESTION 190**
- (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 191**
- (Exam Topic 2)
Which two methods can be configured to validate the revocation status of a certificate? (Choose two.)

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

**Answer:** AC

**NEW QUESTION 192**
- (Exam Topic 1)
An administrator needs to gather information about the CPU utilization on both the management plane and the data plane
Where does the administrator view the desired data?

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

**Answer:** A

**NEW QUESTION 193**
- (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 194**
- (Exam Topic 1)
Refer to the exhibit.

Which certificate can be used as the Forward Trust certificate?

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

**Answer:** D

**NEW QUESTION 199**
- (Exam Topic 1)
Match each SD-WAN configuration element to the description of that element.

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
An SD-WAN Interface Profile
specifies the Tag that you apply to the physical interface, and also specifies the type of Link that interface is (ADSL/DSL, cable modem, Ethernet, fiber, LTE/3G/4G/5G, MPLS, microwave/radio, satellite, WiFi, or other). The Interface Profile is also where you specify the maximum upload and download speeds (in Mbps) of the ISP's connection. You can also change whether the firewall monitors the path frequently or not; the firewall monitors link types appropriately by default.
A Layer3 Ethernet
Interface

with an IPv4 address can support SD-WAN functionalities. You apply an SD-WAN Interface Profile to this
interface (red arrow) to indicate the characteristics of the interface. The blue arrow indicates that physical Interfaces are referenced and grouped in a virtual SD-WAN Interface.

A virtual SD-WAN Interface
is a VPN tunnel or DIA group of one or more interfaces that constitute a numbered, virtual SD-WAN Interface to which you can route traffic. The paths belonging to an SD-WAN Interface all go to the same destination WAN and are all the same type (either DIA or VPN tunnel). (Tag A and Tag B indicate that physical interfaces for the virtual interface can have different tags.)
A Path Quality Profile
specifies maximum latency, jitter, and packet loss thresholds. Exceeding a threshold indicates that the path has deteriorated and the firewall needs to select a new path to the target. A sensitivity setting of high, medium, or low lets you indicate to the firewall which path monitoring parameter is more important for the applications to which the profile applies. The green arrow indicates that you reference a Path Quality Profile in one or more SD-WAN Policy Rules; thus, you can specify different thresholds for rules applied to packets having different applications, services, sources, destinations, zones, and users.
A Traffic Distribution Profile
specifies how the firewall determines a new best path if the current preferred path exceeds a path quality threshold. You specify which Tags the distribution method uses to narrow its selection of a new path; hence, the yellow arrow points from Tags to the Traffic Distribution profile. A Traffic Distribution profile specifies the distribution method for the rule.
The preceding elements come together in
SD-WAN Policy Rules
The purple arrow indicates that you reference a Path Qualify Profile and a Traffic Distribution profile in a rule, along with packet applications/services, sources, destinations, and users to specifically indicate when and how the firewall performs application-based SD-WAN path selection for a packet not belonging to a session.
https://docs.paloaltonetworks.com/sd-wan/1-0/sd-wan-admin/sd-wan-overview/sd-wan-configuration-elements.h

**NEW QUESTION 200**
- (Exam Topic 1)
Match each GlobalProtect component to the purpose of that component

A. Mastered
B. Not Mastered

**Answer:** A

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

**NEW QUESTION 202**
- (Exam Topic 1)
Use the image below If the firewall has the displayed link monitoring configuration what will cause a failover?

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

**Answer:** A

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

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

**Answer:** DE

**NEW QUESTION 204**
- (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 208**
- (Exam Topic 1)
An engineer must configure a new SSL decryption deployment
Which profile or certificate is required before any traffic that matches an SSL decryption rule is decrypted?

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

**Answer:** A

**NEW QUESTION 209**
- (Exam Topic 1)
Place the steps in the WildFire process workflow in their correct order.

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
Timeline Description automatically generated

https://docs.paloaltonetworks.com/wildfire/9-1/wildfire-admin/wildfire-overview/about-wildfire.html

**NEW QUESTION 212**
- (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 216**
- (Exam Topic 1)
When you configure a Layer 3 interface what is one mandatory step?

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

**Answer:** A

**NEW QUESTION 219**
- (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 224**
- (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 228**
- (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 233**
- (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 236**
- (Exam Topic 1)
A firewall should be advertising the static route 10 2 0 0/24 into OSPF The configuration on the neighbor is correct but the route is not in the neighbor's routing table Which two configurations should you check on the firewall'? (Choose two )

A. Within the redistribution profile ensure that Redist is selected
B. In the redistribution profile check that the source type is set to "ospf"
C. In the OSFP configuration ensure that the correct redistribution profile is selected in the OSPF Export Rules section
D. Ensure that the OSPF neighbor state is "2-Way"

**Answer:** AC

**NEW QUESTION 239**
- (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 240**
- (Exam Topic 1)
What are two characteristic types that can be defined for a variable? (Choose two )

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

**Answer:** BD

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

**NEW QUESTION 244**
- (Exam Topic 1)
The UDP-4501 protocol-port is used between which two GlobalProtect components?

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

**Answer:** A

**NEW QUESTION 246**
- (Exam Topic 1)
Which two statements correctly identify the number of Decryption Broker security chains that are supported on a pair of decryption-forwarding interfaces'? (Choose two)

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

**Answer:** AD

**NEW QUESTION 248**
- (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 252**
- (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 257**
- (Exam Topic 1)
As a best practice, which URL category should you target first for SSL decryption*?

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

**Answer:** A

**NEW QUESTION 260**
- (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 264**
- (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 266**
- (Exam Topic 1)
An administrator wants to upgrade a firewall HA pair to PAN-OS 10.1 The firewalls are currently running PAN-OS 8.1.17.

Which upgrade path maintains synchronization of the HA session (and prevents network outage)?

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

**Answer:** D

**NEW QUESTION 268**
- (Exam Topic 1)
An administrator has a PA-820 firewall with an active Threat Prevention subscription The administrator is considering adding a WildFire subscription
How does adding the WildFire subscription improve the security posture of the organization1?

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

**Answer:** D

**NEW QUESTION 273**
- (Exam Topic 1)
Which value in the Application column indicates UDP traffic that did not match an App-ID signature?

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

**Answer:** D

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

**NEW QUESTION 274**
- (Exam Topic 1)
The following objects and policies are defined in a device group hierarchy

A)

B)

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

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

**Answer:** A

**NEW QUESTION 278**
- (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 279**
- (Exam Topic 1)
In a Panorama template which three types of objects are configurable? (Choose three)

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

**Answer:** ACE

**NEW QUESTION 281**
- (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 285**
- (Exam Topic 1)
Which Panorama objects restrict administrative access to specific device-groups?

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

**Answer:** C

**NEW QUESTION 289**
- (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 291**
- (Exam Topic 2)
Which two features can be used to tag a username so that it is included in a dynamic user group? (Choose two)

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

**Answer:** BC

**NEW QUESTION 293**
- (Exam Topic 2)
For which two reasons would a firewall discard a packet as part of the packet flow sequence? (Choose two )

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

**Answer:** BD

**NEW QUESTION 298**
- (Exam Topic 2)
Which tool provides an administrator the ability to see trends in traffic over periods of time, such as threats detected in the last 30 days?

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

**Answer:** B

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

**NEW QUESTION 299**
- (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 300**
- (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 302**
- (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 305**
- (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 307**
- (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 310**
- (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 313**
- (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 315**
- (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 316**
- (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 318**
- (Exam Topic 3)
The company's Panorama server (IP 10.10.10.5) is not able to manage a firewall that was recently deployed. The firewall's dedicated management port is being used to connect to the management network.
Which two commands may be used to troubleshoot this issue from the CLI of the new firewall? (Choose two)

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

**Answer:** BD

**NEW QUESTION 319**
- (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 323**
- (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 325**
- (Exam Topic 3)
Which two logs on the firewall will contain authentication-related information useful for troubleshooting purpose (Choose two)

A. ms.log
B. traffic.log
C. system.log
D. dp-monitor.log
E. authd.log

**Answer:** CE

**NEW QUESTION 329**
- (Exam Topic 3)
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.paloaltonetworks.com/t5/Configuration-Articles/File-Blocking-Rulebase-and-Action-Precedence/ta-p

**NEW QUESTION 330**
- (Exam Topic 3)
A VPN connection is set up between Site-A and Site-B, but no traffic is passing in the system log of Site-A, there is an event logged as like-nego-p1-fail-psk.
What action will bring the VPN up and allow traffic to start passing between the sites?

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

**Answer:** D

**NEW QUESTION 333**
- (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 336**
- (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 341**
- (Exam Topic 3)
Which Public Key infrastructure component is used to authenticate users for GlobalProtect when the Connect Method is set to pre-logon?

A. Certificate revocation list
B. Trusted root certificate
C. Machine certificate
D. Online Certificate Status Protocol

**Answer:** C

**NEW QUESTION 346**
- (Exam Topic 3)
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 347**
- (Exam Topic 3)
Starting with PAN-OS version 9.1, Global logging information is now recoded in which firewall log?

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

**Answer:** D

**NEW QUESTION 352**
- (Exam Topic 3)
Which CLI command displays the current management plane memory utilization?

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

**Answer:** D

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

**NEW QUESTION 353**
- (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 356**
- (Exam Topic 3)
A company.com wants to enable Application Override. Given the following screenshot:

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

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

**Answer:** AC

**NEW QUESTION 360**
- (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 364**
- (Exam Topic 3)
A network engineer has revived a report of problems reaching 98.139.183.24 through vr1 on the firewall. The routing table on this firewall is extensive and complex.
Which CLI command will help identify the issue?

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

**Answer:** C

**NEW QUESTION 366**
- (Exam Topic 3)
Only two Trust to Untrust allow rules have been created in the Security policy Rule1 allows google-base
Rule2 allows youtube-base
The youtube-base App-ID depends on google-base to function. The google-base App-ID implicitly uses SSL and web-browsing. When user try to accesss https://www.youtube.com in a web browser, they get an error indecating that the server cannot be found.
Which action will allow youtube.com display in the browser correctly?

A. Add SSL App-ID to Rule1
B. Create an additional Trust to Untrust Rule, add the web-browsing, and SSL App-ID's to it
C. Add the DNS App-ID to Rule2
D. Add the Web-browsing App-ID to Rule2

**Answer:** C

**NEW QUESTION 370**
- (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 373**
- (Exam Topic 3)
Which three options are available when creating a security profile? (Choose three)

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

**Answer:** ABF

**NEW QUESTION 378**
- (Exam Topic 3)
A network design change requires an existing firewall to start accessing Palo Alto Updates from a data plane interface address instead of the management interface.
Which configuration setting needs to be modified?

A. Service route
B. Default route
C. Management profile
D. Authentication profile

**Answer:** A

**NEW QUESTION 383**
- (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 387**
- (Exam Topic 3)
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 389**
- (Exam Topic 3)
Which three items are import considerations during SD-WAN configuration planning? (Choose three.)

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

**Answer:** ACD

**NEW QUESTION 392**
- (Exam Topic 3)
A critical US-CERT notification is published regarding a newly discovered botnet. The malware is very evasive and is not reliably detected by endpoint antivirus software. Furthermore, SSL is used to tunnel malicious traffic to command-and-control servers on the internet and SSL Forward Proxy Decryption is not enabled.
Which component once enabled on a perirneter firewall will allow the identification of existing infected hosts in an environment?

A. Anti-Spyware profiles applied outbound security policies with DNS Query action set to sinkhole
B. File Blocking profiles applied to outbound security policies with action set to alert
C. Vulnerability Protection profiles applied to outbound security policies with action set to block
D. Antivirus profiles applied to outbound security policies with action set to alert

**Answer:** A

**NEW QUESTION 396**
- (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 399**

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

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

**Answer:** D

**NEW QUESTION 402**
- (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 403**
- (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 407**
- (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 410**
- (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 414**
- (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 418**
- (Exam Topic 3)
A network design calls for a "router on a stick" implementation with a PA-5060 performing inter-VLAN routing All VLAN-tagged traffic will be forwarded to the PA-5060 through a single dot1q trunk interface
Which interface type and configuration setting will support this design?

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

**Answer:** D

**NEW QUESTION 422**
- (Exam Topic 3)
A host attached to Ethernet 1/4 cannot ping the default gateway. The widget on the dashboard shows Ethernet 1/1 and Ethernet 1/4 to be green. The IP address of Ethernet 1/1 is 192.168.1.7 and the IP address of Ethernet 1/4 is 10.1.1.7. The default gateway is attached to Ethernet 1/1. A default route is properly configured. What can be the cause of this problem?

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

**Answer:** A

**NEW QUESTION 424**
- (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 425**
- (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 426**
- (Exam Topic 3)
Which field is optional when creating a new Security Policy rule?

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

**Answer:** B

**NEW QUESTION 431**
- (Exam Topic 3)
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 the output from the command:

What could be the cause of this problem?

A. The dead peer detection settings do not match between the Palo Alto Networks Firewall and the ASA.
B. The Proxy IDs on the Palo Alto Networks Firewall do not match the setting on the ASA.
C. The public IP addresses do not match for both the Palo Alto Networks Firewall and the ASA.
D. The shared secrets do not match between the Palo Alto Networks Firewall and the ASA.

**Answer:** C

**NEW QUESTION 433**
- (Exam Topic 3)
Given the following table.

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

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

**Answer:** A

**NEW QUESTION 438**
- (Exam Topic 3)
What are three valid method of user mapping? (Choose three)

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

**Answer:** ABE

**NEW QUESTION 440**
- (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 444**
- (Exam Topic 3)
Which two mechanisms help prevent a spilt brain scenario an Active/Passive High Availability (HA) pair? (Choose two)

A. Configure the management interface as HA3 Backup
B. Configure Ethernet 1/1 as HA1 Backup
C. Configure Ethernet 1/1 as HA2 Backup
D. Configure the management interface as HA2 Backup
E. Configure the management interface as HA1 Backup
F. Configure ethernet1/1 as HA3 Backup

**Answer:** BE

**NEW QUESTION 445**
- (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 446**
- (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 451**
- (Exam Topic 3)
A company has a pair of Palo Alto Networks firewalls configured as an Acitve/Passive High Availability (HA) pair.
What allows the firewall administrator to determine the last date a failover event occurred?

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

**Answer:** B

**NEW QUESTION 454**
- (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 458**
- (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 463**
.....

# THANKS FOR TRYING THE DEMO OF OUR PRODUCT

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

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

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

## Money Back Guarantee

**PCNSE Practice Exam Features:**

* PCNSE Questions and Answers Updated Frequently

* PCNSE Practice Questions Verified by Expert Senior Certified Staff

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

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