

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)

Which CLI command enables an administrator to view details about the firewall including uptime, PAN-OS® version, and serial number?

- A. debug system details
- B. show session info
- C. show system info
- D. show system details

Answer: C

Explanation:

Reference:

https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/technical-documentation/pan-os-60/PAN_CLI-ref.pdf

NEW QUESTION 2

- (Exam Topic 2)

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 3

- (Exam Topic 2)

Which method will dynamically register tags on the Palo Alto Networks NGFW?

- A. Restful API or the VMWare API on the firewall or on the User-ID agent or the read-only domain controller (RODC)
- B. Restful API or the VMware API on the firewall or on the User-ID agent
- C. XML-API or the VMware API on the firewall or on the User-ID agent or the CLI
- D. XML API or the VM Monitoring agent on the NGFW or on the User-ID agent

Answer: D

Explanation:

Reference:

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/policy/monitor-changes-in-the-virtual-environmen>

NEW QUESTION 4

- (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 5

- (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 6

- (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 7

- (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 8

- (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 9

- (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 10

- (Exam Topic 2)

Which two virtualization platforms officially support the deployment of Palo Alto Networks VM-Series firewalls? (Choose two.)

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

Answer: BD

Explanation:

Reference:

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

NEW QUESTION 10

- (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 11

- (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 12

- (Exam Topic 2)

Which two options prevent the firewall from capturing traffic passing through it? (Choose two.)

- A. The firewall is in multi-vsyz mode.
- B. The traffic is offloaded.
- C. The traffic does not match the packet capture filter.
- D. The firewall's DP CPU is higher than 50%.

Answer: BC

Explanation:

Reference:

<https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/monitoring/take-packet-captures/disable-ha-offload>

NEW QUESTION 16

- (Exam Topic 2)

What is the purpose of the firewall decryption broker?

- A. Decrypt SSL traffic and then send it as cleartext to a security chain of inspection tools
- B. Force decryption of previously unknown cipher suites
- C. Inspection traffic within IPsec tunnel
- D. Reduce SSL traffic to a weaker cipher before sending it to a security chain of inspection tools

Answer: A

NEW QUESTION 21

- (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 EIGRP protocols)
- D. Layer 3 interfaces, but configuring EIGRP on the attached virtual router

Answer: A

NEW QUESTION 23

- (Exam Topic 2)

The firewall determines if a packet is the first packet of a new session or if a packet is part of an existing session using which kind of match?

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

Answer: A

Explanation:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIVECA0>

NEW QUESTION 27

- (Exam Topic 2)

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

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

Answer: D

Explanation:

"Security profiles are not used in the match criteria of a traffic flow. The security profile is applied to scan traffic after the application or category is allowed by the security policy."

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/policy/security-profiles.html#>

NEW QUESTION 31

- (Exam Topic 2)

When is the content inspection performed in the packet flow process?

- A. after the application has been identified
- B. before session lookup
- C. before the packet forwarding process
- D. after the SSL Proxy re-encrypts the packet

Answer: A

Explanation:

Reference:

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

NEW QUESTION 35

- (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 40

- (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 44

- (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 46

- (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 50

- (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=kA10g000000CIRqCAK>

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 52

- (Exam Topic 2)

A speed/duplex negotiation mismatch is between the Palo Alto Networks management port and the switch port which it connects. How would an administrator configure the interface to 1Gbps?

- A. set deviceconfig interface speed-duplex 1Gbps-full-duplex
- B. set deviceconfig system speed-duplex 1Gbps-duplex
- C. set deviceconfig system speed-duplex 1Gbps-full-duplex
- D. set deviceconfig Interface speed-duplex 1Gbps-half-duplex

Answer: C

Explanation:

Reference:

<https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Change-the-Speed-and-Duplex-of-the-Man-Port/ta-p/59034>

user@PA# set deviceconfig system speed-duplex 100Mbps-full-duplex

100Mbps-full-duplex 100Mbps-half-duplex 100Mbps-half-duplex 10Mbps-full-duplex 10Mbps-full-duplex 10Mbps-half-duplex 10Mbps-half-duplex 1Gbps-full-duplex

1Gbps-full-duplex 1Gbps-half-duplex 1Gbps-half-duplex auto-negotiate auto-negotiate

NEW QUESTION 55

- (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 56

- (Exam Topic 2)

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

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

Answer: C

Explanation:

Reference:

<https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/device/device-setup-manageme>

NEW QUESTION 60

- (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 65

- (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 66

- (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=kA10g000000CIKFCA0>

"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 68

- (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 72

- (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 76

- (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 81

- (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=kA10g000000CIFIcAK>

NEW QUESTION 82

- (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 86

- (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 91

- (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 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=kA10g000000CIRoCAK>

NEW QUESTION 94

- (Exam Topic 2)

A customer has an application that is being identified as unknown-top for one of their custom PostgreSQL database connections. Which two configuration options can be used to correctly categorize their custom database application? (Choose two.)

- A. Application Override policy.
- B. Security policy to identify the custom application.
- C. Custom application.
- D. Custom Service object.

Answer: AC

Explanation:

Unlike the App-ID engine, which inspects application packet contents for unique signature elements, the Application Override policy's matching conditions are limited to header-based data only. Traffic matched by an Application Override policy is identified by the App-ID entered in the Application entry box. Choices are limited to applications currently in the App-ID database. Because this traffic bypasses all Layer 7 inspection, the resulting security is that of a Layer-4 firewall. Thus, this traffic should be trusted without the need for Content-ID inspection. The resulting application assignment can be used in other firewall functions such as Security policy and QoS. Use Cases Three primary uses cases for Application Override Policy are:

To identify "Unknown" App-IDs with a different or custom application signature To re-identify an existing application signature

To bypass the Signature Match Engine (within the SP3 architecture) to improve processing times A discussion of typical uses of application override and specific implementation examples is here: <https://live.paloaltonetworks.com/t5/Learning-Articles/Tips-amp-Tricks-How-to-Create-an-Application>

NEW QUESTION 99

- (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 104

- (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 109

- (Exam Topic 2)

In the following image from Panorama, why are some values shown in red?

- A. sg2 session count is the lowest compared to the other managed devices.
- B. us3 has a logging rate that deviates from the administrator-configured thresholds.
- C. uk3 has a logging rate that deviates from the seven-day calculated baseline.
- D. sg2 has misconfigured session thresholds.

Answer: A

NEW QUESTION 114

- (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 116

- (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 119

- (Exam Topic 1)

An administrator wants to enable zone protection Before doing so, what must the administrator consider?

- A. Activate a zone protection subscription.
- B. To increase bandwidth no more than one firewall interface should be connected to a zone
- C. Security policy rules do not prevent lateral movement of traffic between zones
- D. The zone protection profile will apply to all interfaces within that zone

Answer: A

NEW QUESTION 123

- (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 125

- (Exam Topic 1)

An organization has recently migrated its infrastructure and configuration to NGFWs, for which Panorama manages the devices The organization is coming from a L2-L4 firewall vendor, but wants to use App-ID while identifying policies that are no longer needed Which Panorama tool can help this organization?

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

Answer: A

NEW QUESTION 129

- (Exam Topic 1)

When an in-band data port is set up to provide access to required services, what is required for an interface that is assigned to service routes?

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

Answer: A

NEW QUESTION 132

- (Exam Topic 1)

Which statement accurately describes service routes and virtual systems?

- A. Virtual systems can only use one interface for all global service and service routes of the firewall
- B. The interface must be used for traffic to the required external services
- C. Virtual systems that do not have specific service routes configured inherit the global service and service route settings for the firewall
- D. Virtual systems cannot have dedicated service routes configured: and virtual systems always use the global service and service route settings for the firewall

Answer: A

NEW QUESTION 133

- (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 136

- (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 137

- (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 141

- (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 143

- (Exam Topic 1)

A firewall is configured with SSL Forward Proxy decryption and has the following four enterprise certificate authorities (Cas)

- A. Enterprise-Trusted-CA; which is verified as Forward Trust Certificate (The CA is also installed in the trusted store of the end-user browser and system)i
- B. Enterpnse-Untrusted-CA, which is verified as Forward Untrust Certificateii
- C. Enterprise-Intermediate-CAi
- D. Enterprise-Root-CA which is verified only as Trusted Root CAAn end-user visits [https //www example-website com/](https://www.example-website.com/) with a server certificate Common Name (CN) [www example-website com](https://www.example-website.com/) The firewall does the SSL Forward Proxy decryption for the website and the server certificate is not trusted by the firewallThe end-

user's browser will show that the certificate for www example-website com was issued by which of the following?

- E. Enterprise-Untrusted-CA which is a self-signed CA
- F. Enterprise-Trusted-CA which is a self-signed CA
- G. Enterprise-Intermediate-CA which wa
- H. in turn, issued by Enterprise-Root-CA
- I. Enterprise-Root-CA which is a self-signed CA

Answer: B

NEW QUESTION 146

- (Exam Topic 1)

An administrator needs to implement an NGFW between their DMZ and Core network EIGRP Routing between the two environments is required Which interface type would support this business requirement?

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

Answer: D

NEW QUESTION 149

- (Exam Topic 1)

A traffic log might list an application as "not-applicable" for which two reasons'? (Choose two)

- A. 0The firewall did not install the session
- B. The TCP connection terminated without identifying any application data
- C. The firewall dropped a TCP SYN packet
- D. There was not enough application data after the TCP connection was established

Answer: AD

NEW QUESTION 150

- (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 154

- (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 157

- (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 160

- (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 162

- (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 167

- (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 172

- (Exam Topic 1)

Which action disables Zero Touch Provisioning (ZTP) functionality on a ZTP firewall during the onboarding process?

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

Answer: D

NEW QUESTION 173

- (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 175

- (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 177

- (Exam Topic 2)

What file type upload is supported as part of the basic WildFire service?

- A. PE
- B. BAT
- C. VBS

D. ELF

Answer: A

NEW QUESTION 181

- (Exam Topic 2)

An administrator wants multiple web servers in the DMZ to receive connections initiated from the internet. Traffic destined for 206.15.22.9 port 80/TCP needs to be forwarded to the server at 10.1.1.22

Based on the information shown in the image, which NAT rule will forward web-browsing traffic correctly? A)

B)

C)

D)

A. Option A

B. Option B

C. Option C

D. Option D

Answer: C

NEW QUESTION 183

- (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 187

- (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-and-Tricks-How-to-Use-the-Application-Comm-ACC/ta-p/67342>

NEW QUESTION 189

- (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 190

- (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 the management 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=kA10g000000CIGJCA0>

"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 192

- (Exam Topic 2)

Which option describes the operation of the automatic commit recovery feature?

- A. It enables a firewall to revert to the previous configuration if rule shadowing is detected
- B. It enables a firewall to revert to the previous configuration if a commit causes Panorama connectivity failure.
- C. It enables a firewall to revert to the previous configuration if application dependency errors are found
- D. It enables a firewall to revert to the previous configuration if a commit causes HA partner connectivity failure

Answer: A

NEW QUESTION 194

- (Exam Topic 2)

When backing up and saving configuration files, what is achieved using only the firewall and is not available in Panorama?

- A. Load named configuration snapshot
- B. Load configuration version
- C. Save candidate config
- D. Export device state

Answer: D

NEW QUESTION 196

- (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 web browsing access to the server.

Which application and service need to be configured to allow only cleartext web-browsing traffic to this 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 networking applications. 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 200

- (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 205

- (Exam Topic 2)

A web server is hosted in the DMZ and the server is configured to listen for incoming connections on TCP

port 443. A Security policies rules allowing access from the Trust zone to the DMZ zone needs to be configured to allow web-browsing access. The web server hosts its contents over HTTP(S). Traffic from Trust to DMZ is being decrypted with a Forward Proxy rule.

Which combination of service and application, and order of Security policy rules, needs to be configured to allow cleartext web-browsing traffic to this server on tcp/443.

- A. Rule #1: application: web-browsing; service: application-default; action: allow Rule #2: application: ssl; service: application-default; action: allow
- B. Rule #1: application: web-browsing; service: service-https; action: allow Rule #2: application: ssl; service: application-default; action: allow
- C. Rule # 1: application: ssl; service: application-default; action: allow Rule #2: application: web-browsing; service: application-default; action: allow
- D. Rule #1: application: web-browsing; service: service-http; action: allow Rule #2: application: ssl; service: application-default; action: allow

Answer: B

Explanation:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIEyCAK>

NEW QUESTION 208

- (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 209

- (Exam Topic 2)

An administrator wants to upgrade an NGFW from PAN-OS® 9.0 to PAN-OS® 10.0. The firewall is not a part of an HA pair. What needs to be updated first?

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

Answer: B

Explanation:

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

NEW QUESTION 211

- (Exam Topic 3)

Which three fields can be included in a pcap filter? (Choose three)

- A. Egress interface
- B. Source IP
- C. Rule number
- D. Destination IP
- E. Ingress interface

Answer: BCD

Explanation:

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

NEW QUESTION 214

- (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 219

- (Exam Topic 3)

Which two methods can be used to mitigate resource exhaustion of an application server? (Choose two)

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

Answer: BD

NEW QUESTION 221

- (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 224

- (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 225

- (Exam Topic 3)

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

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

Answer: D

Explanation:

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

NEW QUESTION 228

- (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 229

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 232

- (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 233

- (Exam Topic 3)

A client is deploying a pair of PA-5000 series firewalls using High Availability (HA) in Active/Passive mode. Which statement is true about this deployment?

- A. The two devices must share a routable floating IP address
- B. The two devices may be different models within the PA-5000 series
- C. The HA1 IP address from each peer must be on a different subnet
- D. The management port may be used for a backup control connection

Answer: D

NEW QUESTION 237

- (Exam Topic 3)

Which setting allow a DOS protection profile to limit the maximum concurrent sessions from a source IP address?

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

Answer: C

NEW QUESTION 239

- (Exam Topic 3)

Which authentication source requires the installation of Palo Alto Networks software, other than PAN-OS 7x, to obtain a username-to-IP-address mapping?

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

Answer: B

NEW QUESTION 241

- (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 243

- (Exam Topic 3)

A firewall administrator has completed most of the steps required to provision a standalone Palo Alto Networks Next-Generation Firewall. As a final step, the

administrator wants to test one of the security policies.

Which CLI command syntax will display the rule that matches the test?

- A. test security -policy- match source <ip_address> destination <IP_address> destination port <port number> protocol <protocol number>
- B. show security rule source <ip_address> destination <IP_address> destination port <port number> protocol <protocol number>
- C. test security rule source <ip_address> destination <IP_address> destination port <port number> protocol<protocol number>
- D. show security-policy-match source <ip_address> destination <IP_address> destination port <port number> protocol <protocol number>test security-policy-match source

Answer: A

Explanation:

test security-policy-match source <source IP> destination <destination IP> protocol <protocol number> <https://live.paloaltonetworks.com/t5/Management-Articles/How-to-Test-Which-Security-Policy-Applies-to-a-Tr>

NEW QUESTION 248

- (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 250

- (Exam Topic 3)

Company.com has an in-house application that the Palo Alto Networks device doesn't identify correctly. A Threat Management Team member has mentioned that this in-house application is very sensitive and all traffic being identified needs to be inspected by the Content-ID engine.

Which method should company.com use to immediately address this traffic on a Palo Alto Networks device?

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

Answer: D

NEW QUESTION 252

- (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 254

- (Exam Topic 3)

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

- A. Panorama Log Settings
- B. Panorama Log Templates
- C. Panorama Device Group Log Forwarding
- D. Collector Log Forwarding for Collector Groups

Answer: A

Explanation:

https://www.paloaltonetworks.com/documentation/61/panorama/panorama_adminguide/manage-log-collection/e

NEW QUESTION 257

- (Exam Topic 3)

A company is upgrading its existing Palo Alto Networks firewall from version 7.0.1 to 7.0.4.

Which three methods can the firewall administrator use to install PAN-OS 8.0.4 across the enterprise?(Choose three)

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

Answer: ACF

NEW QUESTION 259

- (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 261

- (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 265

- (Exam Topic 3)

Which two statements are correct for the out-of-box configuration for Palo Alto Networks NGFWs? (Choose two)

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

Answer: BC

NEW QUESTION 268

- (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 GlobalProtect 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 271

- (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 273

- (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 278

- (Exam Topic 3)

Which URL Filtering Security Profile action toggles the URL Filtering category to the URL Filtering log?

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

Answer: B

NEW QUESTION 281

- (Exam Topic 3)

A Network Administrator wants to deploy a Large Scale VPN solution. The Network Administrator has chosen a GlobalProtect Satellite solution. This configuration needs to be deployed to multiple remote offices and the Network Administrator decides to use Panorama to deploy the configurations.

How should this be accomplished?

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

Answer: B

NEW QUESTION 282

- (Exam Topic 3)

Which three items are important 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 283

- (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 287

- (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 292

- (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 293

- (Exam Topic 3)

YouTube videos are consuming too much bandwidth on the network, causing delays in mission-critical traffic. The administrator wants to throttle YouTube traffic.
The following interfaces and zones are in use on the firewall:

* ethernet1/1, Zone: Untrust (Internet-facing)

* ethernet1/2, Zone: Trust (client-facing)

A QoS profile has been created, and QoS has been enabled on both interfaces. A QoS rule exists to put the YouTube application into QoS class 6. Interface Ethernet1/1 has a QoS profile called Outbound, and interface Ethernet1/2 has a QoS profile called Inbound.

Which setting for class 6 with throttle YouTube traffic?

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

Answer: D

NEW QUESTION 296

- (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 300

- (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 303

- (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 308

- (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 313

- (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 316

- (Exam Topic 3)

Starting with PAN-OS version 9.1, application dependency information is now reported in which new locations? (Choose two.)

- A. On the App Dependency tab in the Commit Status window

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

Answer: AB

NEW QUESTION 318

- (Exam Topic 3)

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

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

Answer: BC

Explanation:

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

NEW QUESTION 322

- (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 324

- (Exam Topic 3)

A Palo Alto Networks firewall is being targeted by an NTP Amplification attack and is being flooded with tens thousands of bogus UDP connections per second to a single destination IP address and port.

Which option when enabled with the correction threshold would mitigate this attack without dropping legitimate traffic to other hosts inside the network?

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

Answer: D

NEW QUESTION 325

- (Exam Topic 3)

When a malware-infected host attempts to resolve a known command-and-control server, the traffic matches a security policy with DNS sinkhole enabled, generating a traffic log.

What will be the destination IP Address in that log entry?

- A. The IP Address of sinkhole.paloaltonetworks.com
- B. The IP Address of the command-and-control server
- C. The IP Address specified in the sinkhole configuration
- D. The IP Address of one of the external DNS servers identified in the anti-spyware database

Answer: C

Explanation:

<https://live.paloaltonetworks.com/t5/Management-Articles/How-to-Verify-DNS-Sinkhole-Function-is-Working/>

NEW QUESTION 327

- (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 332

- (Exam Topic 3)

Which option is an IPv6 routing protocol?

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

Answer: B

NEW QUESTION 335

- (Exam Topic 3)

A network administrator uses Panorama to push security policies 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 338

- (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 340

.....

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