

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 has been asked to configure active/active HA for a pair of Palo Alto Networks NGFWs. The firewall use Layer 3 interfaces to send traffic to a single gateway IP for the pair.

Which configuration will enable this HA scenario?

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

Answer: A

NEW QUESTION 2

- (Exam Topic 2)

Refer to the exhibit.

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

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

Answer: C

Explanation:

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

NEW QUESTION 3

- (Exam Topic 2)

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

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

Answer: BDE

NEW QUESTION 4

- (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=kA10g000000CIVHCA0> <http://live.paloaltonetworks.com/t5/image/serverpage/image-id/12862i950F549C7D4E6309>

NEW QUESTION 5

- (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 6

- (Exam Topic 2)

An administrator has users accessing network resources through Citrix XenApp 7 x. Which User-ID mapping solution will map multiple users who are using Citrix to connect to the network and access resources?

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

Answer: C

NEW QUESTION 7

- (Exam Topic 2)

Which DoS protection mechanism detects and prevents session exhaustion attacks?

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

Answer: C

Explanation:

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

NEW QUESTION 8

- (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 9

- (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 10

- (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 10

- (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 13

- (Exam Topic 2)

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

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

Answer: B

Explanation:

Reference:

<https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/getting-started/enable-autofocus-threat-intel>

NEW QUESTION 16

- (Exam Topic 2)

Refer to the exhibit.

Which will be the egress interface if the traffic's ingress interface is ethernet 1/7 sourcing from 192.168.111.3 and to the destination 10.46.41.113?

- A. ethernet1/6
- B. ethernet1/3
- C. ethernet1/7
- D. ethernet1/5

Answer: D

NEW QUESTION 18

- (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 if the port being used is a member of the application standardport list

Answer: B

NEW QUESTION 20

- (Exam Topic 2)

Refer to the exhibit.

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

Which two security policy rules will accomplish this configuration? (Choose two)

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

Answer: CD

NEW QUESTION 21

- (Exam Topic 2)

An administrator has been asked to create 100 virtual firewalls in a local, on-premise lab environment (not in “the cloud”). Bootstrapping is the most expedient way to perform this task.

Which option describes deployment of a bootstrap package in an on-premise virtual environment?

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

Answer: D

Explanation:

Reference:

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

NEW QUESTION 22

- (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 24

- (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 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 31

- (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.txt 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 in factory default state or have all private data deleted for bootstrapping
- B. The hostname is a required parameter, but it is missing in init-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 35

- (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 Policies > 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-manage-ssl-tls-service-profile>

NEW QUESTION 38

- (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 39

- (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-intel>

NEW QUESTION 44

- (Exam Topic 2)

An administrator has been asked to configure a Palo Alto Networks NGFW to provide protection against worms and trojans. Which Security Profile type will protect against worms and trojans?

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

Answer: D

Explanation:

Reference: <https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/policy/antivirus-profiles>

NEW QUESTION 48

- (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 51

- (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 object.
- C. Repeat for every additional VLAN and use a VLAN ID of 0 for untagged traffic.
- D. Assign each interface/sub interface to a unique zone.
- E. Create Layer 3 subinterfaces that are each assigned a single VLAN ID and a common virtual router. The physical Layer 3 interface would handle untagged traffic.
- G. Assign each interface/subinterface to a unique zone.
- H. unique zone.
- I. Do not assign any interface an IP address.
- J. Create VLAN objects for each VLAN and assign VLAN interfaces matching each VLAN ID.
- K. Repeat for every additional VLAN and use a VLAN ID of 0 for untagged traffic.
- 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-interfaces> 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 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 59

- (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 64

- (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 thresholds. Enable 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 per 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 68

- (Exam Topic 2)

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

- A. The firewall is in multi-vsyes 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 69

- (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 71

- (Exam Topic 2)

An administrator logs in to the Palo Alto Networks NGFW and reports that the WebUI is missing the Policies tab. Which profile is the cause of the missing Policies tab?

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

Answer: A

NEW QUESTION 74

- (Exam Topic 2)

The certificate information displayed in the following image is for which type of certificate? Exhibit:

- A. Forward Trust certificate
- B. Self-Signed Root CA certificate
- C. Web Server certificate
- D. Public CA signed certificate

Answer: B

NEW QUESTION 79

- (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 82

- (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 83

- (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 88

- (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 93

- (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 94

- (Exam Topic 2)

Which CLI command enables an administrator to check the CPU utilization of the dataplane?

- A. show running resource-monitor
- B. debug data-plane dp-cpu
- C. show system resources
- D. debug running resources

Answer: A

Explanation:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIXwCAK>

NEW QUESTION 96

- (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 98

- (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 101

- (Exam Topic 2)

Which virtual router feature determines if a specific destination IP address is reachable?

- A. Heartbeat Monitoring
- B. Failover
- C. Path Monitoring
- D. Ping-Path

Answer: C

Explanation:

Reference: <https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/policy/pbf>

NEW QUESTION 104

- (Exam Topic 2)

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

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

Answer: D

Explanation:

Reference:

<https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/decryption/decryption-mirroring>

“Before you can enable Decryption Mirroring, you must obtain and install a Decryption Port Mirror license. The license is free of charge and can be activated through the support portal as described in the following procedure. After you install the Decryption Port Mirror license and reboot the firewall, you can enable decryption port mirroring. “

NEW QUESTION 105

- (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 106

- (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-duplex100Mbps-full-duplex

100Mbps-full-duplex100Mbps-half-duplex 100Mbps-half-duplex10Mbps-full-duplex 10Mbps-full-duplex10Mbps-half-duplex 10Mbps-half-duplex1Gbps-full-duplex

1Gbps-full-duplex1Gbps-half-duplex 1Gbps-half-duplexauto-negotiate auto-negotiate

NEW QUESTION 110

- (Exam Topic 2)

Which Zone Pair and Rule Type will allow a successful connection for a user on the internet zone to a web server hosted in the DMZ zone? The web server is reachable using a destination Nat policy in the Palo Alto Networks firewall.

- A. Zone Pair:Source Zone: Internet Destination Zone: DMZ Rule Type:“intrazone”

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

Answer: B

Explanation:

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

NEW QUESTION 111

- (Exam Topic 2)

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 113

- (Exam Topic 2)

Which three split tunnel methods are supported by a globalProtect gateway? (Choose three.)

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

Answer: ABC

NEW QUESTION 115

- (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 116

- (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 119

- (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 124

- (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 126

- (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 129

- (Exam Topic 2)

If a template stack is assigned to a device and the stack includes three templates with overlapping settings, which settings are published to the device when the template stack is pushed?

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

Answer: A

Explanation:

Reference:

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

NEW QUESTION 133

- (Exam Topic 2)

Which feature must you configure to prevent users from accidentally submitting their corporate credentials to a phishing website?

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

Answer: A

Explanation:

Reference:

<https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/threat-prevention/prevent-credential-phishi>

NEW QUESTION 134

- (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 136

- (Exam Topic 2)

An administrator has created an SSL Decryption policy rule that decrypts SSL sessions on any port. Which log entry can the administrator use to verify that sessions are being decrypted?

- A. In the details of the Traffic log entries
- B. Decryption log
- C. Data Filtering log
- D. In the details of the Threat log entries

Answer: A

Explanation:

Reference:

<https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Implement-and-Test-SSL-Decryption/ta-p/5>

NEW QUESTION 138

- (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 141

- (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 146

- (Exam Topic 2)

Which PAN-OS® policy must you configure to force a user to provide additional credentials before he is allowed to access an internal application that contains highly-sensitive business data?

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

Answer: C

NEW QUESTION 151

- (Exam Topic 2)

Which administrative authentication method supports authorization by an external service?

- A. Certificates
- B. LDAP
- C. RADIUS
- D. SSH keys

Answer: C

NEW QUESTION 155

- (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 158

- (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 159

- (Exam Topic 2)

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

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

Answer: DE

NEW QUESTION 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 164

- (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 166

- (Exam Topic 2)

An administrator needs to determine why users on the trust zone cannot reach certain websites. The only information available is shown on the following image. Which configuration change should the administrator make?

A)

B)

C)

D)

E)

A. Option A

B. Option B

C. Option C

D. Option D

E. Option E

Answer: B

NEW QUESTION 167

- (Exam Topic 2)

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

A. exploitation

B. IP command and control

C. delivery

D. reconnaissance

Answer: D

NEW QUESTION 168

- (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 171

- (Exam Topic 2)

How would an administrator monitor/capture traffic on the management interface of the Palo Alto Networks NGFW?

- A. Use the debug dataplane packet-diag set capture stage firewall file command.
- B. Enable all four stages of traffic capture (TX, RX, DROP, Firewall).
- C. Use the debug dataplane packet-diag set capture stage management file command.
- D. Use the tcpdump command.

Answer: D

Explanation:

Reference: <https://live.paloaltonetworks.com/t5/Learning-Articles/How-to-Run-a-Packet-Capture/ta-p/62390> <https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/monitoring/take-packet-captures/take-a-packet-capt>

NEW QUESTION 175

- (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 180

- (Exam Topic 2)

Which logs enable a firewall administrator to determine whether a session was decrypted?

- A. Correlated Event
- B. Traffic
- C. Decryption
- D. Security Policy

Answer: B

NEW QUESTION 184

- (Exam Topic 1)

An administrator needs to gather information about the CPU utilization on both the management plane and the data plane
Where does the administrator view the desired data?

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

Answer: A

NEW QUESTION 189

- (Exam Topic 1)

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 191

- (Exam Topic 1)

Match each SD-WAN configuration element to the description of that element.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

A Layer3 Ethernet Interface with an IPv4 address can support SD-WAN functionalities. You apply an SD-WAN Interface Profile to this interface (red arrow) to indicate the characteristics of the interface. The blue arrow indicates that physical Interfaces are referenced and grouped in a virtual SD-WAN Interface.

A virtual SD-WAN Interface is a VPN tunnel or DIA group of one or more interfaces that constitute a numbered, virtual SD-WAN Interface to which you can route traffic. The paths belonging to an SD-WAN Interface all go to the same destination WAN and are all the same type (either DIA or VPN tunnel). (Tag A and Tag B indicate that physical interfaces for the virtual interface can have different tags.)

A Path Quality Profile specifies maximum latency, jitter, and packet loss thresholds. Exceeding a threshold indicates that the path has deteriorated and the firewall needs to select a new path to the target. A sensitivity setting of high, medium, or low lets you indicate to the firewall which path monitoring parameter is more important for the applications to which the profile applies. The green arrow indicates that you reference a Path Quality Profile in one or more SD-WAN Policy Rules; thus, you can specify different thresholds for rules applied to packets having different applications, services, sources, destinations, zones, and users.

A Traffic Distribution Profile specifies how the firewall determines a new best path if the current preferred path exceeds a path quality threshold. You specify which Tags the distribution method uses to narrow its selection of a new path; hence, the yellow arrow points from Tags to the Traffic Distribution profile. A Traffic Distribution profile specifies the distribution method for the rule.

The preceding elements come together in SD-WAN Policy Rules

The purple arrow indicates that you reference a Path Qualify Profile and a Traffic Distribution profile in a rule, along with packet applications/services, sources, destinations, and users to specifically indicate when and how the firewall performs application-based SD-WAN path selection for a packet not belonging to a session.

<https://docs.paloaltonetworks.com/sd-wan/1-0/sd-wan-admin/sd-wan-overview/sd-wan-configuration-elements.h>

NEW QUESTION 194

- (Exam Topic 1)

A variable name must start with which symbol?

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

Answer: A

Explanation:

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

NEW QUESTION 199

- (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 201

- (Exam Topic 1)

In SSL Forward Proxy decryption, which two certificates can be used for certificate signing? (Choose two.)

- A. wildcard server certificate
- B. enterprise CA certificate
- C. client certificate
- D. server certificate
- E. self-signed CA certificate

Answer: BE

NEW QUESTION 204

- (Exam Topic 1)

When setting up a security profile which three items can you use? (Choose three)

- A. Wildfire analysis
- B. anti-ransom ware
- C. antivirus
- D. URL filtering
- E. decryption profile

Answer: ACD

Explanation:

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/security-profiles>

NEW QUESTION 209

- (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 212

- (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 217

- (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 218

- (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 222

- (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 225

- (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 227

- (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)

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 233

- (Exam Topic 1)

During SSL decryption which three factors affect resource consumption? (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 236

- (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 237

- (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 239

- (Exam Topic 1)

An administrator cannot see any Traffic logs from the Palo Alto Networks NGFW in Panorama reports. The configuration problem seems to be on the firewall. Which settings, if configured incorrectly, most likely would stop only Traffic logs from being sent from the NGFW to Panorama?

- A)
- B)
- C)
- D)

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

Answer: B

NEW QUESTION 244

- (Exam Topic 1)

In a security-first network, what is the recommended threshold value for content updates to be dynamically updated?

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

Answer: B

Explanation:

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

NEW QUESTION 245

- (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 249

- (Exam Topic 1)

An engineer is planning an SSL decryption implementation

Which of the following statements is a best practice for SSL decryption?

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

Answer: D

NEW QUESTION 251

- (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 253

- (Exam Topic 1)

An administrator plans to deploy 15 firewalls to act as GlobalProtect gateways around the world Panorama will manage the firewalls

The firewalls will provide access to mobile users and act as edge locations to on-premises infrastructure The administrator wants to scale the configuration out quickly and wants all of the firewalls to use the same template configuration

Which two solutions can the administrator use to scale this configuration? (Choose two.)

- A. variables
- B. template stacks
- C. collector groups
- D. virtual systems

Answer: C

NEW QUESTION 254

- (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 258

- (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 262

- (Exam Topic 1)

When you import the configuration of an HA pair into Panorama, how do you prevent the import from affecting ongoing traffic?

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

Answer: C

NEW QUESTION 263

- (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 268

- (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 269

- (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 271

- (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. GlobalProtect agent
- C. User-ID Windows-based agent
- D. XML API

Answer: BC

NEW QUESTION 276

- (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 278

- (Exam Topic 2)

View the GlobalProtect configuration screen capture.

What is the purpose of this configuration?

- A. It configures the tunnel address of all internal clients to an IP address range starting at 192.168.10.1.
- B. It forces an internal client to connect to an internal gateway at IP address 192.168.10.1.
- C. It enables a client to perform a reverse DNS lookup on 192.168.10.1 to detect that it is an internal client.
- D. It forces the firewall to perform a dynamic DNS update, which adds the internal gateway's hostname and IP address to the DNS server.

Answer: C

Explanation:

Reference:

<https://www.paloaltonetworks.com/documentation/80/globalprotect/globalprotect-admin-guide/globalprotect-po-the-globalprotect-client-authentication-configurations/define-the-globalprotect-agent-configurations>

"Select this option to allow the GlobalProtect agent to determine if it is inside the enterprise network. This option applies only to endpoints that are configured to communicate with internal gateways. When the user attempts to log in, the agent does a reverse DNS lookup of an internal host using the specified Hostname to the specified IP Address. The host serves as a reference point that is reachable if the endpoint is inside the enterprise network. If the agent finds the host, the endpoint is inside the network and the agent connects to an internal gateway; if the agent fails to find the internal host, the endpoint is outside the network and the agent establishes a tunnel to one of the external gateways"

NEW QUESTION 280

- (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 284

- (Exam Topic 2)

Which two actions would be part of an automatic solution that would block sites with untrusted certificates without enabling SSL Forward Proxy? (Choose two.)

- A. Create a no-decrypt Decryption Policy rule.

- B. Configure an EDL to pull IP addresses of known sites resolved from a CRL.
- C. Create a Dynamic Address Group for untrusted sites
- D. Create a Security Policy rule with vulnerability Security Profile attached.
- E. Enable the “Block sessions with untrusted issuers” setting.

Answer: DE

NEW QUESTION 287

- (Exam Topic 2)

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

- A. Port Inspection
- B. Certificate revocation
- C. Content-ID
- D. App-ID

Answer: D

Explanation:

Reference:

<https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/quality-of-service/qos-for-applications-and>

NEW QUESTION 292

- (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 293

- (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 interface 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 298

- (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 303

- (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 304

- (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 administrator approves 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 308

- (Exam Topic 2)

Based on the image, what caused the commit warning?

- A. The CA certificate for FWDtrust has not been imported into the firewall.
- B. The FWDtrust certificate has not been flagged as Trusted Root CA.
- C. SSL Forward Proxy requires a public certificate to be imported into the firewall.
- D. The FWDtrust certificate does not have a certificate chain.

Answer: D

NEW QUESTION 313

- (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 318

- (Exam Topic 2)

Which method does an administrator use to integrate all non-native MFA platforms in PAN-OS® software?

- A. Okta
- B. DUO
- C. RADIUS
- D. PingID

Answer: C

Explanation:

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

NEW QUESTION 319

- (Exam Topic 2)

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

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

Answer: D

Explanation:

Palo Alto Networks Panorama 7.0 Administrator's Guide • 77 Manage Firewalls Manage Device Groups Manage Device Groups Add a Device Group Create a Device Group Hierarchy Create Objects for Use in Shared or Device Group Policy Revert to Inherited Object Values Manage Unused Shared Objects Manage Precedence of Inherited Objects Move or Clone a Policy Rule or Object to a Different Device Group Select a URL Filtering Vendor on Panorama Push a Policy Rule to a Subset of Firewalls Manage the Rule Hierarchy Add a Device Group After adding firewalls (see Add a Firewall as a Managed Device), you can group them into Device Groups (up to 256), as follows. Be sure to assign both firewalls in an active-passive high availability (HA) configuration to the same device group so that Panorama will push the same policy rules and objects to those firewalls. ##### PAN-OS doesn't synchronize pushed rules across HA peers. ##### To manage rules and objects at different administrative levels in your organization, Create a Device Group Hierarchy.

<https://docs.paloaltonetworks.com/panorama/8-0/panorama-admin/manage-firewalls/transition-a-firewall-to-pan>

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CleOCAS>

NEW QUESTION 322

- (Exam Topic 2)

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

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

Answer: A

Explanation:

Reference:

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

NEW QUESTION 325

- (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 328

- (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 329

- (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 333

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 336

- (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 337

- (Exam Topic 3)

What are three valid actions in a File Blocking Profile? (Choose three)

- A. Forward
- B. Block
- C. Alert
- 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 338

- (Exam Topic 3)

Site-A and Site-B need to use IKEv2 to establish a VPN connection. Site A connects directly to the internet using a public IP address. Site-B uses a private IP address behind an ISP router to connect to the internet.

How should NAT Traversal be implemented for the VPN connection to be established between Site-A and Site-B?

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

Answer: D

NEW QUESTION 339

- (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 341

- (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 346

- (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 351

- (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 355

- (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 358

- (Exam Topic 3)

A network security engineer needs to configure a virtual router using IPv6 addresses. Which two routing options support these addresses? (Choose two)

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

Answer: BD

Explanation:

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

NEW QUESTION 363

- (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 367

- (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 371

- (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 372

- (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 373

- (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 378

- (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 382

- (Exam Topic 3)

The IT department has received complaints about 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 385

- (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:

```
less mp-log ikemgr.log:
```

What could be the cause of this problem?

- A. The public IP addresses 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 secrets do not match between the Palo Alto firewall and the ASA
- D. The dead peer detection settings do not match between the Palo Alto Networks Firewall and the ASA

Answer: B

NEW QUESTION 390

- (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 391

- (Exam Topic 3)

A network security engineer is asked to perform a Return Merchandise Authorization (RMA) on a firewall Which part of files needs to be imported back into the replacement firewall that is using Panorama?

- A. Device state and license files
- B. Configuration and serial number files
- C. Configuration and statistics files
- D. Configuration and Large Scale VPN (LSVPN) setups file

Answer: A

NEW QUESTION 393

- (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 396

- (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 399

- (Exam Topic 3)

What must be used in Security Policy Rule that contain addresses where NAT policy applies?

- A. Pre-NAT addresse and Pre-NAT zones
- B. Post-NAT addresse and Post-Nat zones
- C. Pre-NAT addresse and Post-Nat zones
- D. Post-Nat addresses and Pre-NAT zones

Answer: C

NEW QUESTION 402

- (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 406

- (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 409

- (Exam Topic 3)

A host attached to ethernet1/3 cannot access the internet. The default gateway is attached to ethernet1/4. After troubleshooting. It is determined that traffic cannot pass from the ethernet1/3 to ethernet1/4. What can be the cause of the problem?

- A. DHCP has been set to Auto.
- B. Interface ethernet1/3 is in Layer 2 mode and interface ethernet1/4 is in Layer 3 mode.
- C. Interface ethernet1/3 and ethernet1/4 are in Virtual Wire Mode.
- D. DNS has not been properly configured on the firewall

Answer: B

NEW QUESTION 412

- (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 417

- (Exam Topic 3)

An administrator has left a firewall to use the data of port for all management service which there functions are performed by the data face? (Choose three.)

- A. NTP
- B. Antivirus
- C. Wildfire updates
- D. NAT
- E. File tracking

Answer: ACD

NEW QUESTION 420

- (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 422

- (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 426

- (Exam Topic 3)

What can missing SSL packets when performing a packet capture on dataplane interfaces?

- A. The packets are hardware offloaded to the offloaded processor on the dataplane
- B. The missing packets are offloaded to the management plane CPU
- C. The packets are not captured because they are encrypted
- D. There is a hardware problem with offloading FPGA on the management plane

Answer: A

NEW QUESTION 427

- (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 431

- (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 435

- (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 438

- (Exam Topic 3)

Firewall administrators cannot authenticate to a firewall GUI.

Which two logs on that firewall will contain authentication-related information useful in troubleshooting this issue? (Choose two.)

- A. ms log
- B. authd log
- C. System log
- D. Traffic log
- E. dp-monitor .log

Answer: BC

NEW QUESTION 439

- (Exam Topic 3)

Which interface configuration will accept specific VLAN IDs?

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

Answer: B

NEW QUESTION 443

- (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 444

- (Exam Topic 3)

Which two options are required on an M-100 appliance to configure it as a Log Collector? (Choose two)

- A. From the Panorama tab of the Panorama GUI select Log Collector mode and then commit changes
- B. Enter the command request system system-mode logger then enter Y to confirm the change to Log Collector mode.
- C. From the Device tab of the Panorama GUI select Log Collector mode and then commit changes.
- D. Enter the command logger-mode enable then enter Y to confirm the change to Log Collector mode.
- E. Log in the Panorama CLI of the dedicated Log Collector

Answer: BE

Explanation:

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

NEW QUESTION 446

- (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 451

- (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 453

- (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 456

- (Exam Topic 3)

What are three possible verdicts that WildFire can provide for an analyzed sample? (Choose three)

- A. Clean
- B. Benign
- 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 460

- (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 463

- (Exam Topic 3)

Which two virtualized environments support Active/Active High Availability (HA) in PAN-OS 8.0? (Choose two.)

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

Answer: AB

NEW QUESTION 468

- (Exam Topic 3)

Which option is an IPv6 routing protocol?

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

Answer: B

NEW QUESTION 471

- (Exam Topic 3)

A company has a pair of Palo Alto Networks firewalls configured as an Active/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 472

- (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 474

- (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 479

- (Exam Topic 3)

Which Security Policy Rule configuration option disables antivirus and anti-spyware scanning of server-to-client flows only?

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

Answer: A

NEW QUESTION 483

.....

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