

Paloalto-Networks

Exam Questions PCNSE

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



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 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 3

- (Exam Topic 2)

Which log file can be used to identify SSL decryption failures?

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

Answer: D

Explanation:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClboCAC>

NEW QUESTION 4

- (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 5

- (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 6

- (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-inte>

NEW QUESTION 7

- (Exam Topic 2)

VPN traffic intended for an administrator's Palo Alto Networks NGFW is being maliciously intercepted and retransmitted by the interceptor. When creating a VPN tunnel, which protection profile can be enabled to prevent this malicious behavior?

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

Answer: B

Explanation:

<https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/vpns/set-up-site-to-site-vpn/set-up-an-ipsec-tunnel#>

NEW QUESTION 8

- (Exam Topic 2)

Which is not a valid reason for receiving a decrypt-cert-validation error?

- A. Unsupported HSM
- B. Unknown certificate status
- C. Client authentication
- D. Untrusted issuer

Answer: A

NEW QUESTION 9

- (Exam Topic 2)

Starling with PAN-OS version 9.1, GlobalProtect logging information is now recorded in which firewall log?

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

Answer: C

NEW QUESTION 10

- (Exam Topic 2)

What are the differences between using a service versus using an application for Security Policy match?

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

Answer: B

NEW QUESTION 10

- (Exam Topic 2)

What is exchanged through the HA2 link?

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

Answer: C

Explanation:

Reference:

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

NEW QUESTION 11

- (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 16

- (Exam Topic 2)

Which two features does PAN-OS® software use to identify applications? (Choose two)

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

Answer: AD

Explanation:

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

NEW QUESTION 20

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 22

- (Exam Topic 2)

An administrator is using Panorama and multiple Palo Alto Networks NGFWs. After upgrading all devices to the latest PAN-OS® software, the administrator enables log forwarding from the firewalls to Panorama.

Pre-existing logs from the firewalls are not appearing in Panorama.

Which action would enable the firewalls to send their pre-existing logs to Panorama?

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

Answer: B

Explanation:

<https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-new-features/management-features/pa-7000-series-firewall>

NEW QUESTION 25

- (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 30

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 35

- (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 37

- (Exam Topic 2)

The firewall is not downloading IP addresses from MineMeld. Based, on the image, what most likely is wrong?

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

Answer: D

NEW QUESTION 40

- (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 43

- (Exam Topic 2)

To more easily reuse templates and template slacks , you can create term plate variables in place of firewall-specific and appliance-specific IP literals in your configurations

Which one is the correct configuration?

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

Answer: D

NEW QUESTION 46

- (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 51

- (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 56

- (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 57

- (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 58

- (Exam Topic 2)

Which three options are supported in HA Lite? (Choose three.)

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

Answer: BCD

Explanation:

"The PA-200 firewall supports HA Lite only. HA Lite is an active/passive deployment that provides configuration synchronization and some runtime data synchronization such as IPSec security associations. It does not support any session synchronization (HA2), and therefore does not offer stateful failover."

Reference:

<https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/device/device-high-availability>

NEW QUESTION 62

- (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 67

- (Exam Topic 2)

On the NGFW. how can you generate and block a private key from export and thus harden your security posture and prevent rogue administrators or other bad actors from misusing keys?

- A. * 1.Select Device > Certificate Management > Certificates >Devace > Certificates* 2. Import the certificate.* 3 Select Import Private Key* 4 Click Generate to generate the new certificate
- B. * 1 Select Device > Certificates * 2 Select Certificate Profile* 3 Generate the certificate* 4 Select Block Private Key Export.
- C. * 1 Select Device > Certificates * 2 Select Certificate Profile.* 3 Generate the certificate* 4 Select Block Private Key Export
- D. * 1 Select Device > Certificate Management > Certificates > Device > Certificates * 2 Generate the certificate* 3 Select Block Private Key Export* 4 Click Genet ale to generate the new certificate.

Answer: D

NEW QUESTION 71

- (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 73

- (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 76

- (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 77

- (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 82

- (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 85

- (Exam Topic 2)

Which option enables a Palo Alto Networks NGFW administrator to schedule Application and Threat updates while applying only new content-IDs to traffic?

- A. Select download-and-install.
- B. Select download-and-install, with "Disable new apps in content update" selected.
- C. Select download-only.
- D. Select disable application updates and select "Install only Threat updates"

Answer: C

NEW QUESTION 87

- (Exam Topic 2)

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

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

Answer: B

Explanation:

Reference:

<https://live.paloaltonetworks.com/t5/Learning-Articles/Tips-and-Tricks-How-to-Create-an-Application-Overrid>

<https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-admin/app-id/manage-custom-or-unknown-applications#>

NEW QUESTION 92

- (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 93

- (Exam Topic 2)

In a virtual router, which object contains all potential routes?

- A. MIB
- B. RIB
- C. SIP
- D. FIB

Answer: B

Explanation:

<https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/networking/virtual-routers>

NEW QUESTION 94

- (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 98

- (Exam Topic 2)

Which CLI command is used to simulate traffic going through the firewall and determine which Security policy rule, NAT translation, static route, or PBF rule will be triggered by the traffic?

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

Answer: C

Explanation:

Reference: <http://www.shanekillen.com/2014/02/palo-alto-useful-cli-commands.html>

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIQSCA0>

NEW QUESTION 103

- (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 104

- (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 108

- (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. Matching 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 113

- (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 115

- (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 119

- (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 124

- (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 126

- (Exam Topic 2)

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

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

Answer: AB

NEW QUESTION 130

- (Exam Topic 2)

Which Captive Portal mode must be configured to support MFA authentication?

- A. NTLM
- B. Redirect
- C. Single Sign-On
- D. Transparent

Answer: B

Explanation:

Reference:

<https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/authentication/configure-multi-factor-authentication>

NEW QUESTION 135

- (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 136

- (Exam Topic 2)

Decrypted packets from the website <https://www.microsoft.com> will appear as which application and service within the Traffic log?

- A. web-browsing and 443
- B. SSL and 80
- C. SSL and 443
- D. web-browsing and 80

Answer: A

Explanation:

We know that SSL decryption is supposed to give us visibility of traffic that would otherwise be encrypted. Therefore, we'd expect decrypted traffic to be identified as the underlying applications, such as web-browsing, facebook-base or other, but not as SSL.

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CmdLCAS>

NEW QUESTION 137

- (Exam Topic 2)

Which User-ID method maps IP address to usernames for users connecting through a web proxy that has already authenticated the user?

- A. Client Probing

- B. Port mapping
- C. Server monitoring
- D. Syslog listening

Answer: D

Explanation:

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

NEW QUESTION 139

- (Exam Topic 2)

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

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

Answer: A

Explanation:

Reference:

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

NEW QUESTION 144

- (Exam Topic 2)

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 149

- (Exam Topic 1)

Which CLI command displays the physical media that are connected to ethernetl/8?

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

Answer: D

NEW QUESTION 152

- (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 154

- (Exam Topic 1)

Below are the steps in the workflow for creating a Best Practice Assessment in a firewall and Panorama configuration Place the steps in order.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 155

- (Exam Topic 1)

Match each GlobalProtect component to the purpose of that component

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

The GlobalProtect portal provides the management functions for your GlobalProtect infrastructure The GlobalProtect gateways provide security enforcement for traffic from GlobalProtect apps

The GlobalProtect app software runs on endpoints and enables access to your network resources

NEW QUESTION 160

- (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 162

- (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 166

- (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 170

- (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-Series firewalls with full network and policy configurations.

Answer: DE

NEW QUESTION 174

- (Exam Topic 1)

An engineer must configure a new SSL decryption deployment

Which profile or certificate is required before any traffic that matches an SSL decryption rule is decrypted?

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

Answer: A

NEW QUESTION 175

- (Exam Topic 1)

When overriding a template configuration locally on a firewall, what should you consider?

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

Answer: B

NEW QUESTION 179

- (Exam Topic 1)

An 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 182

- (Exam Topic 1)

A firewall should be advertising the static route 10.2.0.0/24 into OSPF. The configuration on the neighbor is correct but the route is not in the neighbor's routing table. Which two configurations should you check on the firewall? (Choose two)

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

Answer: AC

NEW QUESTION 186

- (Exam Topic 1)

What are three valid qualifiers for a Decryption Policy Rule match? (Choose three)

- A. Destination Zone
- B. App-ID
- C. Custom URL Category
- D. User-ID
- E. Source Interface

Answer: ADE

NEW QUESTION 188

- (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 193

- (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 195

- (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 199

- (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 200

- (Exam Topic 1)

The following objects and policies are defined in a device group hierarchy

- A)
- B)
- C)
Address Objects
-Shared Address 1
-Branch Address2 Policies -Shared Polic1 I -Branch Policyl
- D)
Address Objects -Shared Addressl -Shared Address2 -Branch Addressl Policies -Shared Policyl -Shared Policy2 -Branch Policyl

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

Answer: A

NEW QUESTION 203

- (Exam Topic 1)

Please match the terms to their corresponding definitions.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 208

- (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 213

- (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 218

- (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 219

- (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: allowRule #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 221

- (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 225

- (Exam Topic 2)

How can an administrator configure the NGFW to automatically quarantine a device using GlobalProtect?

- A. by adding the device's Host ID to a quarantine list and configure GlobalProtect to prevent users fromconnecting to the GlobalProtect gateway from a quarantined device
- B. by using secunty policies, log forwarding profiles, and log settings.
- C. by exporting the list of quarantined devices to a pdf or csv file by selecting PDF/CSV at the bottom of the Device Quarantine page and leveraging the approbate XSOAR playbook
- D. There is no native auto-quarantine feature so a custom script would need to be leveraged.

Answer: A

NEW QUESTION 229

- (Exam Topic 2)

The administrator has enabled BGP on a virtual router on the Palo Alto Networks NGFW, but new routes do not seem to be populating the virtual router.

Which two options would help the administrator troubleshoot this issue? (Choose two.)

- A. View the System logs and look for the error messages about BGP.
- B. Perform a traffic pcap on the NGFW to see any BGP problems.
- C. View the Runtime Stats and look for problems with BGP configuration.
- D. View the ACC tab to isolate routing issues.

Answer: BC

Explanation:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIEWCA0>

NEW QUESTION 233

- (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 238

- (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 239

- (Exam Topic 3)

A network security engineer is asked to provide a report on bandwidth usage. Which tab in the ACC provides the information needed to create the report?

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

Answer: D

NEW QUESTION 242

- (Exam Topic 3)

When using the predefined default profile, the policy will inspect for viruses on the decoders. Match each decoder with its default action.

Answer options may be used more than once or not at all.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

IMAP , POP3 , SMTP - > Alert
HTTP,FTP,SMB -> Reset-both

NEW QUESTION 243

- (Exam Topic 3)

Which Device Group option is assigned by default in Panorama whenever a new device group is created to manage a Firewall?

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

Answer: C

NEW QUESTION 248

- (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 252

- (Exam Topic 3)

The web server is configured to listen for HTTP traffic on port 8080. The clients access the web server using the IP address 1.1.1.100 on TCP Port 80. The destination NAT rule is configured to translate both IP address and port to 10.1.1.100 on TCP Port 8080.

Which NAT and security rules must be configured on the firewall? (Choose two)

- A. A security policy with a source of any from untrust-I3 Zone to a destination of 10.1.1.100 in dmz-I3 zone using web-browsing application
- B. A NAT rule with a source of any from untrust-I3 zone to a destination of 10.1.1.100 in dmz-zone using service-http service.
- C. A NAT rule with a source of any from untrust-I3 zone to a destination of 1.1.1.100 in untrust-I3 zone using service-http service.
- D. A security policy with a source of any from untrust-I3 zone to a destination of 1.1.100 in dmz-I3 zone using web-browsing application.

Answer: BD

NEW QUESTION 253

- (Exam Topic 3)

Which three options does the WF-500 appliance support for local analysis? (Choose three)

- A. E-mail links
- B. APK files
- C. jar files
- D. PNG files
- E. Portable Executable (PE) files

Answer: ACE

NEW QUESTION 257

- (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 259

- (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 263

- (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 265

- (Exam Topic 3)

Which Palo Alto Networks VM-Series firewall is supported for VMware NSX?

- A. VM-100
- B. VM-200
- C. VM-1000-HV
- D. VM-300

Answer: C

NEW QUESTION 268

- (Exam Topic 3)

When is it necessary to activate a license when provisioning a new Palo Alto Networks firewall?

- A. When configuring Certificate Profiles
- B. When configuring GlobalProtect portal
- C. When configuring User Activity Reports
- D. When configuring Antivirus Dynamic Updates

Answer: D

NEW QUESTION 272

- (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 274

- (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 278

- (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 280

- (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 281

- (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 284

- (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 286

- (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 deep peer detection settings do not match between the Palo Alto Networks Firewall and the ASA

Answer: B

NEW QUESTION 290

- (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 291

- (Exam Topic 3)

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

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

Answer: D

Explanation:

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

NEW QUESTION 292

- (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 293

- (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 298

- (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 302

- (Exam Topic 3) A

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

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

Answer: C

NEW QUESTION 304

- (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 309

- (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 314

- (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 317

- (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 322

- (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 325

- (Exam Topic 3)

How can a Palo Alto Networks firewall be configured to send syslog messages in a format compatible with non-standard syslog servers?

- A. Enable support for non-standard syslog messages under device management
- B. Check the custom-format check box in the syslog server profile
- C. Select a non-standard syslog server profile
- D. Create a custom log format under the syslog server profile

Answer: D

NEW QUESTION 328

- (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 329

- (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 333

- (Exam Topic 3)

Which option is an IPv6 routing protocol?

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

Answer: B

NEW QUESTION 338

- (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 342

- (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 343

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

PCNSE Practice Exam Features:

- * PCNSE Questions and Answers Updated Frequently
- * PCNSE Practice Questions Verified by Expert Senior Certified Staff
- * PCNSE Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * PCNSE Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The PCNSE Practice Test Here](#)