



Paloalto-Networks

Exam Questions PCNSE

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

About ExamBible

Your Partner of IT Exam

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1

- (Exam Topic 2)

An Administrator is configuring Authentication Enforcement and they would like to create an exemption rule to exempt a specific group from authentication. Which authentication enforcement object should they select?

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

Answer: D

NEW QUESTION 2

- (Exam Topic 2)

Which option is part of the content inspection process?

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

Answer: B

Explanation:

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

NEW QUESTION 3

- (Exam Topic 2)

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

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

Answer: B

Explanation:

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

NEW QUESTION 4

- (Exam Topic 2)

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)

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 6

- (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 7

- (Exam Topic 2)

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

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

Answer: D

Explanation:

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

NEW QUESTION 8

- (Exam Topic 2)

If the firewall has the link monitoring configuration, what will cause a failover?

- A. ethernet1/3 and ethernet1/6 going down
- B. ethernet1/3 going down
- C. ethernet1/3 or Ethernet1/6 going down
- D. ethernet1/6 going down

Answer: A

NEW QUESTION 9

- (Exam Topic 2)

A client has a sensitive application server in their data center and is particularly concerned about resource exhaustion because of distributed denial-of-service attacks.

How can the Palo Alto Networks NGFW be configured to specifically protect this server against resource exhaustion originating from multiple IP addresses (DDoS attack)?

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

Answer: D

Explanation:

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

NEW QUESTION 10

- (Exam Topic 2)

A 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 14

- (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 15

- (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 standard port list

Answer: B

NEW QUESTION 19

- (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 21

- (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)

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 26

- (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 28

- (Exam Topic 2)

An administrator accidentally closed the commit window/screen before the commit was finished. Which two options could the administrator use to verify the progress or success of that commit task? (Choose two.)

- A. Exhibit A
- B. Exhibit B
- C. Exhibit C
- D. Exhibit D

Answer: AD

NEW QUESTION 32

- (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 37

- (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 9.1.x at a minimum but the firewall is running 10.0.x
- E. The bootstrap.xml file is a required file but it is missing

Answer: C

NEW QUESTION 39

- (Exam Topic 2)

Which option would an administrator choose to define the certificate and protocol that Panorama and its managed devices use for SSL/TLS services?

- A. Configure a Decryption Profile and select SSL/TLS services.

- B. Set up SSL/TLS under 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 42

- (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 47

- (Exam Topic 2)

Which three authentication factors does PAN-OS® software support for MFA (Choose three.)

- A. Push
- B. Pull
- C. Okta Adaptive
- D. Voice
- E. SMS

Answer: ADE

Explanation:

Reference:

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

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 to
- F. single VLAN ID and a common virtual router. The physical Layer 3 interface would handle untagged traffic
- G. Assign each interface/subinterface to
- 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 55

- (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 60

- (Exam Topic 2)

How does Panorama prompt VMWare NSX to quarantine an infected VM?

- A. HTTP Server Profile
- B. Syslog Server Profile
- C. Email Server Profile
- D. SNMP Server Profile

Answer: A

NEW QUESTION 63

- (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 64

- (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 66

- (Exam Topic 2)

A Palo Alto Networks NGFW just submitted a file to WildFire for analysis. Assume a 5-minute window for analysis. The firewall is configured to check for verdicts every 5 minutes.

How quickly will the firewall receive back a verdict?

- A. More than 15 minutes
- B. 5 minutes
- C. 10 to 15 minutes
- D. 5 to 10 minutes

Answer: D

NEW QUESTION 71

- (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 75

- (Exam Topic 2)

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

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

Answer: BCD

Explanation:

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

Reference:

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

NEW QUESTION 78

- (Exam Topic 2)

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

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

Answer: D

Explanation:

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

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

NEW QUESTION 81

- (Exam Topic 2)

An administrator creates an SSL decryption rule decrypting traffic on all ports. The administrator also creates a Security policy rule allowing only the applications DNS, SSL, and web-browsing.

The administrator generates three encrypted BitTorrent connections and checks the Traffic logs. There are three entries. The first entry shows traffic dropped as application Unknown. The next two entries show traffic allowed as application SSL.

Which action will stop the second and subsequent encrypted BitTorrent connections from being allowed as SSL?

- A. Create a decryption rule matching the encrypted BitTorrent traffic with action “No-Decrypt,” and place the rule at the top of the Decryption policy.
- B. Create a Security policy rule that matches application “encrypted BitTorrent” and place the rule at the top of the Security policy.
- C. Disable the exclude cache option for the firewall.
- D. Create a Decryption Profile to block traffic using unsupported cyphers, and attach the profile to the decryption rule.

Answer: D

NEW QUESTION 85

- (Exam Topic 2)

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 > Device > 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 Generate to generate the new certificate.

Answer: D

NEW QUESTION 87

- (Exam Topic 2)

Which three user authentication services can be modified to provide the Palo Alto Networks NGFW with both usernames and role names? (Choose three.)

- A. TACACS+

- B. Kerberos
- C. PAP
- D. LDAP
- E. SAML
- F. RADIUS

Answer: BDE

Explanation:

<https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/firewall-administration/manage-firewall-administra>

NEW QUESTION 88

- (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 89

- (Exam Topic 2)

ESTION NO: 94

If an administrator wants to decrypt SMTP traffic and possesses the server's certificate, which SSL decryption mode will allow the Palo Alto Networks NGFW to inspect traffic to the server?

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

Answer: B

Explanation:

Reference:

<https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/decryption/configure-ssl-inbound-inspectio>

NEW QUESTION 91

- (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 93

- (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 95

- (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 98

- (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 101

- (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 103

- (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 107

- (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 110

- (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 111

- (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 113

- (Exam Topic 2)

A user's traffic traversing a Palo Alto Networks NGFW sometimes can reach <http://www.company.com>. At other times the session times out. The NGFW has been configured with a PBF rule that the user's traffic matches when it goes to <http://www.company.com>.

How can the firewall be configured automatically disable the PBF rule if the next hop goes down?

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

Answer: B

Explanation:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIFIcAK>

NEW QUESTION 117

- (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 122

- (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 124

- (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 129

- (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 134

- (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 138

- (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 139

- (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 144

- (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 148

- (Exam Topic 2)

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

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

Answer: AC

Explanation:

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

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

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

NEW QUESTION 152

- (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 156

- (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 161

- (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 162

- (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 163

- (Exam Topic 2)

Which three steps will reduce the CPU utilization on the management plane? (Choose three.)

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

Answer: ACD

Explanation:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CieLCAS>

NEW QUESTION 164

- (Exam Topic 2)

When configuring the firewall for packet capture, what are the valid stage types?

- A. Receive, management , transmit , and drop
- B. Receive , firewall, send , and non-syn
- C. Receive management , transmit, and non-syn
- D. Receive , firewall, transmit, and drop

Answer: D

NEW QUESTION 165

- (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 167

- (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 171

- (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 172

- (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 177

- (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 180

- (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 183

- (Exam Topic 1)

Place the steps in the WildFire process workflow in their correct order.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Timeline Description automatically generated

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

NEW QUESTION 184

- (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 185

- (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 187

- (Exam Topic 1)

Which User-ID mapping method should be used in a high-security environment where all IP address-to-user mappings should always be explicitly known?

- A. PAN-OS integrated User-ID agent
- B. LDAP Server Profile configuration
- C. GlobalProtect
- D. Windows-based User-ID agent

Answer: A

NEW QUESTION 190

- (Exam Topic 1)

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

- A. Enterprise-Trusted-CA; which is verified as Forward Trust Certificate (The CA is also installed in the trusted store of the end-user browser and system)i
- B. Enterpnse-Untrusted-CA, which is verified as Forward Untrust Certificateii
- C. Enterprise-Intermediate-CAi
- D. Enterprise-Root-CA which is verified only as Trusted Root CAAn end-user visits [https //www example-website com/](https://www.example-website.com/) with a server certificate Common Name (CN) [www example-website com](https://www.example-website.com/) The firewall does the SSL Forward Proxy decryption for the website and the server certificate is not trusted by the firewallThe end-user's browser will show that the certificate for [www example-website com](https://www.example-website.com/) was issued by which of the following?
- E. Enterprise-Untrusted-CA which is a self-signed CA
- F. Enterprise-Trusted-CA which is a self-signed CA
- G. Enterprise-Intermediate-CA which wa
- H. in turn, issued by Enterprise-Root-CA
- I. Enterprise-Root-CA which is a self-signed CA

Answer: B

NEW QUESTION 195

- (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 197

- (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 198

- (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 200

- (Exam Topic 1)

An administrator needs to troubleshoot a User-ID deployment The administrator believes that there is an issue related to LDAP authentication The administrator wants to create a packet capture on the management plane

Which CLI command should the administrator use to obtain the packet capture for validating the configuration^

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

Answer: C

NEW QUESTION 204

- (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 206

- (Exam Topic 1)

Which configuration task is best for reducing load on the management plane?

- A. Disable logging on the default deny rule
- B. Enable session logging at start
- C. Disable pre-defined reports

D. Set the URL filtering action to send alerts

Answer: A

NEW QUESTION 210

- (Exam Topic 1)

Which rule type controls end user SSL traffic to external websites?

- A. SSL Outbound Proxyless Inspection
- B. SSL Forward Proxy
- C. SSL Inbound Inspection
- D. SSH Proxy

Answer: C

NEW QUESTION 212

- (Exam Topic 1)

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 216

- (Exam Topic 1)

An administrator wants to upgrade a firewall HA pair to PAN-OS 10.1 The firewalls are currently running PAN-OS 8.1.17. Which upgrade path maintains synchronization of the HA session (and prevents network outage)?

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

Answer: D

NEW QUESTION 220

- (Exam Topic 1)

An administrator has a PA-820 firewall with an active Threat Prevention subscription The administrator is considering adding a WildFire subscription How does adding the WildFire subscription improve the security posture of the organization1?

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

Answer: D

NEW QUESTION 222

- (Exam Topic 1)

In a Panorama template which three types of objects are configurable? (Choose three)

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

Answer: ACE

NEW QUESTION 227

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 230

- (Exam Topic 2)

Which four NGFW multi-factor authentication factors are supported by PAN-OS? (Choose four.)

- A. Short message service
- B. Push
- C. User logon
- D. Voice
- E. SSH key
- F. One-Time Password

Answer: ABDF

Explanation:

<https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/authentication/authentication-types/multi-factor-aut>

NEW QUESTION 233

- (Exam Topic 2)

Which two features can be used to tag a username so that it is included in a dynamic user group? (Choose two)

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

Answer: BC

NEW QUESTION 235

- (Exam Topic 2)

Which two settings can be configured only locally on the firewall and not pushed from a Panorama template or template stack? (Choose two)

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

Answer: AC

Explanation:

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

NEW QUESTION 238

- (Exam Topic 2)

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

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

B)

C)

D)

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

Answer: C

NEW QUESTION 239

- (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 242

- (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 243

- (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-Command-Center-ACC/ta-p/67342>

NEW QUESTION 244

- (Exam Topic 2)

An administrator encountered problems with inbound decryption. Which option should the administrator investigate as part of triage?

- A. Security policy rule allowing SSL to the target server
- B. Firewall connectivity to a CRL
- C. Root certificate imported into the firewall with “Trust” enabled
- D. Importation of a certificate from an HSM

Answer: A

Explanation:

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/decryption/configure-ssl-inbound-inspection.html>

NEW QUESTION 248

- (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 252

- (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 254

- (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 256

- (Exam Topic 2)

What are two benefits of nested device groups in Panorama? (Choose two.)

- A. Reuse of the existing Security policy rules and objects
- B. Requires configuring both function and location for every device
- C. All device groups inherit settings from the Shared group
- D. Overwrites local firewall configuration

Answer: AC

Explanation:

Creation of a device group hierarchy enables you to organize firewalls based on common policy requirements without redundant configuration. When you create objects for use in shared or device group policy once and use them many times, you reduce administrative overhead and ensure consistency across firewall policies.

NEW QUESTION 257

- (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 260

- (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 262

- (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 267

- (Exam Topic 3)

The company's Panorama server (IP 10.10.10.5) is not able to manage a firewall that was recently deployed. The firewall's dedicated management port is being used to connect to the management network.

Which two commands may be used to troubleshoot this issue from the CLI of the new firewall? (Choose two)

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

Answer: BD

NEW QUESTION 268

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 269

- (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 273

- (Exam Topic 3)

Which three function are found on the dataplane of a PA-5050? (Choose three)

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

Answer: BDE

NEW QUESTION 276

- (Exam Topic 3)

During the packet flow process, which two processes are performed in application identification? (Choose two.)

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

Answer: AD

NEW QUESTION 281

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 285

- (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 287

- (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 289

- (Exam Topic 3)

How are IPV6 DNS queries configured to user interface ethernet1/3?

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

Answer: D

NEW QUESTION 292

- (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 295

- (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 299

- (Exam Topic 3)

Which Public Key infrastructure component is used to authenticate users for GlobalProtect when the Connect Method is set to pre-login?

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

Answer: C

NEW QUESTION 302

- (Exam Topic 3)

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

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

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

Answer: A

Explanation:

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

NEW QUESTION 307

- (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 308

- (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 313

- (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 316

- (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 319

- (Exam Topic 3)

Which CLI command displays the current management plane memory utilization?

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

Answer: D

Explanation:

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

NEW QUESTION 320

- (Exam Topic 3)

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

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

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

Answer: ACF

NEW QUESTION 323

- (Exam Topic 3)

A firewall administrator is troubleshooting problems with traffic passing through the Palo Alto Networks firewall. Which method shows the global counters associated with the traffic after configuring the appropriate packet filters?

- A. From the CLI, issue the show counter global filter pcap yes command.
- B. From the CLI, issue the show counter global filter packet-filter yes command.
- C. From the GUI, select show global counters under the monitor tab.
- D. From the CLI, issue the show counter interface command for the ingress interface.

Answer: B

NEW QUESTION 326

- (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 330

- (Exam Topic 3)

A company.com wants to enable Application Override. Given the following screenshot:

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

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

Answer: AC

NEW QUESTION 335

- (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 337

- (Exam Topic 3)

A network engineer has revived a report of problems reaching 98.139.183.24 through vr1 on the firewall. The routing table on this firewall is extensive and complex.

Which CLI command will help identify the issue?

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

Answer: C

NEW QUESTION 341

- (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 343

- (Exam Topic 3)

Only two Trust to Untrust allow rules have been created in the Security policy Rule1 allows google-base Rule2 allows youtube-base

The youtube-base App-ID depends on google-base to function. The google-base App-ID implicitly uses SSL and web-browsing. When user try to access <https://www.youtube.com> in a web browser, they get an error indecating that the server cannot be found.

Which action will allow youtube.com display in the browser correctly?

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

Answer: C

NEW QUESTION 345

- (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 348

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 353

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 358

- (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 360

- (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 361

- (Exam Topic 3)

After pushing a security policy from Panorama to a PA-3020 firewall, the firewall administrator notices that traffic logs from the PA-3020 are not appearing in Panorama's traffic logs. What could be the problem?

- A. A Server Profile has not been configured for logging to this Panorama device.
- B. Panorama is not licensed to receive logs from this particular firewall.
- C. The firewall is not licensed for logging to this Panorama device.
- D. None of the firewall's policies have been assigned a Log Forwarding profile

Answer: D

NEW QUESTION 365

- (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 368

- (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 371

- (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 375

- (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 376

- (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 378

- (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 380

- (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 384

- (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 386

- (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 389

- (Exam Topic 3)

People are having intermittent quality issues during a live meeting via web application.

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

Answer: C

NEW QUESTION 394

- (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 399

- (Exam Topic 3)

How is the Forward Untrust Certificate used?

- A. It issues certificates encountered on the Untrust security zone when clients attempt to connect to a site that has been decrypted/
- B. It is used when web servers request a client certificate.
- C. It is presented to clients when the server they are connecting to is signed by a certificate authority that is not trusted by the firewall.
- D. It is used for Captive Portal to identify unknown users.

Answer: C

NEW QUESTION 400

- (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 402

- (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 407

- (Exam Topic 3)

What are three valid methods of user mapping? (Choose three)

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

Answer: ABE

NEW QUESTION 412

- (Exam Topic 3)

Which two mechanisms help prevent a split brain scenario in 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 414

- (Exam Topic 3)

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

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

Answer: B

Explanation:

<https://www.paloaltonetworks.com/documentation/70/pan-os/pan-os/url-filtering/url-filtering-profile-actions>

NEW QUESTION 418

- (Exam Topic 3)

A company hosts a publicly accessible web server behind a Palo Alto Networks next-generation firewall with the following configuration information:

- * Users outside the company are in the "Untrust-L3" zone.
- * The web server physically resides in the "Trust-L3" zone.
- * Web server public IP address: 23.54.6.10
- * Web server private IP address: 192.168.1.10

Which two items must the NAT policy contain to allow users in the Untrust-L3 zone to access the web server? (Choose two.)

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

Answer: AB

NEW QUESTION 419

- (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 423

- (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 427

- (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 432

- (Exam Topic 3)

A network security engineer has a requirement to allow an external server to access an internal web server. The internal web server must also initiate connections with the external server.

What can be done to simplify the NAT policy?

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

Answer: C

Explanation:

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

NEW QUESTION 433

.....

Relate Links

100% Pass Your PCNSE Exam with ExamBible Prep Materials

<https://www.exambible.com/PCNSE-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>