



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)

Refer to the exhibit.

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

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

Answer: C

Explanation:

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

NEW QUESTION 3

- (Exam Topic 2)

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

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

Answer: B

Explanation:

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

NEW QUESTION 4

- (Exam Topic 2)

In which two types of deployment is active/active HA configuration supported? (Choose two.)

- A. TAP mode
- B. Layer 2 mode
- C. Virtual Wire mode
- D. Layer 3 mode

Answer: CD

NEW QUESTION 5

- (Exam Topic 2)

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

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

Answer: AB

Explanation:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIVHCA0> <http://live.paloaltonetworks.com/t5/image/serverpage/image-id/12862i950F549C7D4E6309>

NEW QUESTION 6

- (Exam Topic 2)

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

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

Answer: D

Explanation:

Reference:

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

NEW QUESTION 7

- (Exam Topic 2)

Which DoS protection mechanism detects and prevents session exhaustion attacks?

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

Answer: C

Explanation:

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

NEW QUESTION 8

- (Exam Topic 2)

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 session flooding because of denial of-service attacks. How can the Palo Alto Networks NGFW be configured to specifically protect this server against session floods originating from a single IP address?

- A. Define a custom App-ID to ensure that only legitimate application traffic reaches the server
- B. Add QoS Profiles to throttle incoming requests
- C. Add a tuned DoS Protection Profile
- D. Add an Anti-Spyware Profile to block attacking IP address

Answer: C

NEW QUESTION 10

- (Exam Topic 2)

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 10

- (Exam Topic 2)

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

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

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

Answer: D

Explanation:

Reference:

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

NEW QUESTION 15

- (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 20

- (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 22

- (Exam Topic 2)

SAML SLO is supported for which two firewall features? (Choose two.)

- A. GlobalProtect Portal
- B. CaptivePortal
- C. WebUI
- D. CLI

Answer: AB

NEW QUESTION 25

- (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 30

- (Exam Topic 2)

An administrator is defining protection settings on the Palo Alto Networks NGFW to guard against resource exhaustion. When platform utilization is considered, which steps must the administrator take to configure and apply packet buffer protection?

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

Answer: A

NEW QUESTION 35

- (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 38

- (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 41

- (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 invali
- 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 detecte
- D. The “Deny” action will supersede theper-severity defined actions defined in the associated Vulnerability Protection Profile.
- E. The configuration is invali

- 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 43

- (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 48

- (Exam Topic 2)

A session in the Traffic log is reporting the application as "incomplete." What does "incomplete" mean?

- A. The three-way TCP handshake was observed, but the application could not be identified.
- B. The three-way TCP handshake did not complete.
- C. The traffic is coming across UDP, and the application could not be identified.
- D. Data was received but was instantly discarded because of a Deny policy was applied before App-ID could be applied.

Answer: B

Explanation:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClibCAC>

NEW QUESTION 52

- (Exam Topic 2)

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

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

Answer: A

Explanation:

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

NEW QUESTION 55

- (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 59

- (Exam Topic 2)

Which three authentication services can administrator use to authenticate admins into the Palo Alto Networks NGFW without defining a corresponding admin account on the local firewall? (Choose three.)

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

Answer: ACF

Explanation:

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

The administrative accounts are defined on an external SAML, TACACS+, or RADIUS server. The server performs both authentication and authorization. For authorization, you define Vendor-Specific Attributes (VSAs) on the TACACS+ or RADIUS server, or SAML attributes on the SAML server. PAN-OS maps the attributes to administrator roles, access domains, user groups, and virtual systems that you define on the firewall. For details, see:

[Configure SAML Authentication](#)[Configure TACACS+ Authentication](#)[Configure RADIUS Authentication](#)

NEW QUESTION 62

- (Exam Topic 2)

Refer to exhibit.

An organization has Palo Alto Networks NGFWs that send logs to remote monitoring and security management platforms. The network team has reported excessive traffic on the corporate WAN.

How could the Palo Alto Networks NGFW administrator reduce WAN traffic while maintaining support for all existing monitoring/ security platforms?

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

Answer: A

Explanation:

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

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIKFCA0>

"When this has to be done over a WAN link with bandwidth limitation, it is necessary to consider reducing the number of log streams that are sent over the link"

"With this configuration, firewalls will forward logs to Panorama, assuming that log forwarding was configured correctly on the firewall. The logs are forwarded to the syslog server, thus reducing the number of log streams significantly."

NEW QUESTION 67

- (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 70

- (Exam Topic 2)

Which three file types can be forwarded to WildFire for analysis as a part of the basic WildFire service? (Choose three.)

- A. .dll
- B. .exe
- C. .src
- D. .apk
- E. .pdf
- F. .jar

Answer: DEF

Explanation:

<https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-admin/getting-started/enable-basic-wildfire-forwarding>

NEW QUESTION 74

- (Exam Topic 2)

Which feature must you configure to prevent users form 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 75

- (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 76

- (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 81

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 83

- (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 88

- (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 93

- (Exam Topic 2)

A customer wants to set up a site-to-site VPN using tunnel interfaces? Which two formats are correct for naming tunnel interfaces? (Choose two.)

- A. Vpn-tunnel.1024
- B. vpn-tunne.1
- C. tunnel 1025
- D. tunne
- E. 1

Answer: CD

NEW QUESTION 94

- (Exam Topic 2)

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

- A. exploitation
- B. IP command and control
- C. delivery
- D. reconnaissance

Answer: D

NEW QUESTION 99

- (Exam Topic 2)

Which two methods can be configured to validate the revocation status of a certificate? (Choose two.)

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

Answer: AC

NEW QUESTION 100

- (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 103

- (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 106

- (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 108

- (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 111

- (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 116

- (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 120

- (Exam Topic 1)

An engineer must configure the Decryption Broker feature

Which Decryption Broker security chain supports bi-directional traffic flow?

- A. Layer 2 security chain
- B. Layer 3 security chain
- C. Transparent Bridge security chain
- D. Transparent Proxy security chain

Answer: B

Explanation:

Together, the primary and secondary interfaces form a pair of decryption forwarding interfaces. Only interfaces that you have enabled to be Decrypt Forward interfaces are displayed here. Your security chain type (Layer 3 or Transparent Bridge) and the traffic flow direction (unidirectional or bidirectional) determine which of the two interfaces forwards allowed, clear text traffic to the security chain, and which interface receives the traffic back from the security chain after it has undergone additional enforcement.

NEW QUESTION 122

- (Exam Topic 1)

The UDP-4501 protocol-port is used between which two GlobalProtect components?

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

Answer: A

NEW QUESTION 126

- (Exam Topic 1)

What are two common reasons to use a "No Decrypt" action to exclude traffic from SSL decryption? (Choose two.)

- A. the website matches a category that is not allowed for most users
- B. the website matches a high-risk category
- C. the web server requires mutual authentication
- D. the website matches a sensitive category

Answer: AD

NEW QUESTION 127

- (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 129

- (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 132

- (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 organization?

- 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 135

- (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 PolicyI
- D)
Address Objects -Shared AddressI -Shared Address2 -Branch AddressI Policies -Shared PolicyI -Shared Policy2 -Branch PolicyI
- A. Option A
B. Option B
C. Option C
D. Option D

Answer: A

NEW QUESTION 137

- (Exam Topic 1)

A company needs to preconfigure firewalls to be sent to remote sites with the least amount of preconfiguration Once deployed each firewall must establish secure tunnels back to multiple regional data centers to include the future regional data centers

Which VPN preconfigured configuration would adapt to changes when deployed to the future site?

- A. IPsec tunnels using IKEv2
B. PPTP tunnels
C. GlobalProtect satellite
D. GlobalProtect client

Answer: C

NEW QUESTION 140

- (Exam Topic 1)

Please match the terms to their corresponding definitions.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 141

- (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 146

- (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 149

- (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 152

- (Exam Topic 2)

Which tool provides an administrator the ability to see trends in traffic over periods of time, such as threats detected in the last 30 days?

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

Answer: B

Explanation:

Reference:

<https://live.paloaltonetworks.com/t5/Management-Articles/Tips-and-Tricks-How-to-Use-the-Application-Comm ACC/ta-p/67342>

NEW QUESTION 154

- (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 156

- (Exam Topic 2)

An administrator wants a new Palo Alto Networks NGFW to obtain automatic application updates daily, so it is configured to use a scheduler for the application database. Unfortunately, they required the management network to be isolated so that it cannot reach the internet. Which configuration will enable the firewall to download and install application updates automatically?

- A. Configure a Policy Based Forwarding policy rule for the update server IP address so that traffic sourced from the management interface destined for the update servers goes out of the interface acting as your internet connection.
- B. Configure a security policy rule to allow all traffic to and from the update servers.
- C. Download and install application updates cannot be done automatically if the MGT port cannot reach the internet.
- D. Configure a service route for Palo Alto networks services that uses a dataplane interface that can route traffic to the internet, and create a security policy rule to allow the traffic from that interface to the update servers if necessary.

Answer: D

Explanation:

"By default, the firewall uses management interface to communicate to various servers including DNS, Email, Palo Alto Updates, User-ID agent, Syslog, Panorama etc. Service routes are used so that the communication between the firewall and servers go through the dataplane." <https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIGJCA0>

"The firewall uses the service route to connect to the Update Server and checks for new content release versions and, if there are updates available, displays them at the top of the list." <https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-web-interface-help/device/device-dynamic-updates#>

NEW QUESTION 161

- (Exam Topic 2)

Refer to the exhibit.

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

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

- A. Untrust (Any) to DMZ (10.1.1.100.10.1.1.101), ssh, web-browsing –Allow
- B. Untrust (Any) to DMZ (1.1.1.100), web-browsing –Allow
- C. Untrust (Any) to Untrust (10.1.1.1), web-browsing –Allow
- D. Untrust (Any) to Untrust (10.1.1.1), SSH -Allow
- E. Untrust (Any) to DMZ (1.1.1.100), SSH –Allow

Answer: BE

Explanation:

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

NEW QUESTION 163

- (Exam Topic 2)

A web server is hosted in the DMZ and the server is configured to listen for incoming connections on TCP port 443. A Security policies rules allowing access from the Trust zone to the DMZ zone needs to be configured to allow web-browsing access. The web server hosts its contents over HTTP(S). Traffic from Trust to DMZ is being decrypted with a Forward Proxy rule. Which combination of service and application, and order of Security policy rules, needs to be configured to allow cleartext web- browsing traffic to this server on tcp/443.

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

Answer: B

Explanation:

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

NEW QUESTION 164

- (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 from connecting to the GlobalProtect gateway from a quarantined device
- B. by using security 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 appropriate XSOAR playbook
- D. There is no native auto-quarantine feature so a custom script would need to be leveraged.

Answer: A

NEW QUESTION 165

- (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 170

- (Exam Topic 2)

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

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

Answer: B

Explanation:

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

NEW QUESTION 173

- (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 175

- (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 176

- (Exam Topic 3)

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

- A. Forward
- B. Block
- C. Alert
- D. Upload
- E. Reset-both
- F. Continue

Answer: ABC

Explanation:

<https://live.paloaltonetworks.com/t5/Configuration-Articles/File-Blocking-Rulebase-and-Action-Precedence/ta-p>

NEW QUESTION 181

- (Exam Topic 3)

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

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

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

Answer: D

NEW QUESTION 182

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 186

- (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 190

- (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 193

- (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 198

- (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 199

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 202

- (Exam Topic 3)

Which three items are import considerations during SD-WAN configuration planning? (Choose three.)

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

Answer: ACD

NEW QUESTION 203

- (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 208

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 213

- (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 218

- (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 220

- (Exam Topic 3)

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

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

Answer: ACD

NEW QUESTION 223

- (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 224

- (Exam Topic 3)

Click the Exhibit button below,

A firewall has three PBF rules and a default route with a next hop of 172.20.10.1 that is configured in the default VR. A user named Will has a PC with a 192.168.10.10 IP address. He makes an HTTPS connection to 172.16.10.20.

Which is the next hop IP address for the HTTPS traffic from Will's PC?

- A. 172.20.30.1
- B. 172.20.40.1
- C. 172.20.20.1
- D. 172.20.10.1

Answer: C

NEW QUESTION 228

- (Exam Topic 3)

A distributed log collection deployment has dedicated log Collectors. A developer needs a device to send logs to Panorama instead of sending logs to the Collector Group.

What should be done first?

- A. Remove the cable from the management interface, reload the log Collector and then re-connect that cable
- B. Contact Palo Alto Networks Support team to enter kernel mode commands to allow adjustments
- C. remove the device from the Collector Group

D. Revert to a previous configuration

Answer: C

NEW QUESTION 230

- (Exam Topic 3)

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

- A. Clean
- B. Bengin
- C. Adware
- D. Suspicious
- E. Grayware
- F. Malware

Answer: BEF

Explanation:

<https://www.paloaltonetworks.com/documentation/70/pan-os/newfeaturesguide/wildfire-features/wildfire-grayw>

NEW QUESTION 234

- (Exam Topic 3)

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

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

Answer: AB

NEW QUESTION 239

- (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 244

- (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 246

.....

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](#)