

- **Vendor: Palo Alto Networks**
- **Exam Code: PCNSE**
- **Exam Name: Palo Alto Networks Certified Security Engineer (PCNSE) PAN-OS 10.0**
- **New Updated Questions from [Braindump2go](#)**
- **(Updated in [November/2021](#))**

**Visit Braindump2go and Download Full Version PCNSE Exam Dumps**

**QUESTION 390**

Before an administrator of a VM-500 can enable DoS and zone protection, what actions need to be taken?

- A. Create a zone protection profile with flood protection configured to defend an entire egress zone against SYN, ICMP, ICMPv6, UDP, and other IP flood attacks.
- B. Add a WildFire subscription to activate DoS and zone protection features.
- C. Replace the hardware firewall, because DoS and zone protection are not available with VM-Series systems.
- D. Measure and monitor the CPU consumption of the firewall data plane to ensure that each firewall is properly sized to support DoS and zone protection.

**Answer: A**

**Explanation:**

Reference: <https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/zone-protection-and-dos-protection.html>

**QUESTION 391**

An administrator receives the following error message:

"IKE phase-2 negotiation failed when processing Proxy ID. Received local id 192. 168.33.33/24 type IPv4 address protocol 0 port 0, received remote id 172.16.33.33/24 type IPv4 address protocol 0 port 0."

How should the administrator identify the root cause of this error message?

- A. Verify that the IP addresses can be pinged and that routing issues are not causing the connection failure.
- B. Check whether the VPN peer on one end is set up correctly using policy-based VPN.
- C. In the IKE Gateway configuration, verify that the IP address for each VPN peer is accurate.
- D. In the IPSec Crypto profile configuration, verify that PFS is either enabled on both VPN peers or disabled on both VPN peers.

**Answer: B**

**Explanation:**

Reference: <https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/vpns/set-up-site-to-site-vpn/interpret-vpn-error-messages.html>

**QUESTION 392**

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

**[PCNSE Exam Dumps](#) [PCNSE Exam Questions](#) [PCNSE PDF Dumps](#) [PCNSE VCE Dumps](#)**

**<https://www.braindump2go.com/pcnse.html>**



Dallas-Branch has Dallas-FW as a member of the Dallas-Branch device-group NYC-DC has NYC-FW as a member of the NYC-DC device-group

What objects and policies will the Dallas-FW receive if "Share Unused Address and Service Objects" is enabled in Panorama?

- A. Address Objects
  - Shared Address1
  - Branch Address1
Policies
  - Shared Policy1
  - Branch Policy1
- B. Address Objects
  - Shared Address1
  - Shared Address2
  - Branch Address1
Policies
  - Shared Policy1
  - Shared Policy2
  - Branch Policy1
- C. Address Objects
  - Shared Address1
  - Shared Address2
  - Branch Address1
  - DC Address1
Policies
  - Shared Policy1
  - Shared Policy2
  - Branch Policy1
- D. Address Objects
  - Shared Address1
  - Shared Address2
  - Branch Address1
Policies
  - Shared Policy1
  - Branch Policy1

**Answer: C**

### QUESTION 393

An administrator has purchased WildFire subscriptions for 90 firewalls globally. What should the administrator consider with regards to the WildFire infrastructure?

- A. To comply with data privacy regulations, WildFire signatures and verdicts are not shared globally.
- B. Palo Alto Networks owns and maintains one global cloud and four WildFire regional clouds.
- C. Each WildFire cloud analyzes samples and generates malware signatures and verdicts independently of the other WildFire clouds.

D. The WildFire Global Cloud only provides bare metal analysis.

**Answer: C**

**Explanation:**

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

#### **QUESTION 394**

What are three reasons for excluding a site from SSL decryption? (Choose three.)

- A. the website is not present in English
- B. unsupported ciphers
- C. certificate pinning
- D. unsupported browser version
- E. mutual authentication

**Answer: BCE**

**Explanation:**

Reference: <https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/decryption/decryption-exclusions/exclude-a-server-from-decryption>

#### **QUESTION 395**

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

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

**Answer: ACD**

**Explanation:**

Reference: <https://manualzz.com/doc/10741747/pan%E2%80%90os-administrator%E2%80%99s-guide-policy>

#### **QUESTION 396**

What are three types of Decryption Policy rules? (Choose three.)

- A. SSL Inbound Inspection
- B. SSH Proxy
- C. SSL Forward Proxy
- D. Decryption Broker
- E. Decryption Mirror

**Answer: ABC**

**Explanation:**

Reference: <https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/decryption/decryption-overview.html#:~:text=The%20firewall%20provides%20three%20types,to%20control%20tunneled%20SSH%20traffic>

#### **QUESTION 397**

Which two features require another license on the NGFW? (Choose two.)

- A. SSL Inbound Inspection
- B. SSL Forward Proxy
- C. Decryption Mirror
- D. Decryption Broker

**Answer:** CD

**Explanation:**

Reference: <https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/decryption/configure-decryption-port-mirroring.html>

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/decryption/decryption-licenses.html>

#### **QUESTION 398**

A remote administrator needs access to the firewall on an untrust interface. Which three options would you configure on an Interface Management profile to secure management access? (Choose three.)

- A. Permitted IP Addresses
- B. SSH
- C. https
- D. User-ID
- E. HTTP

**Answer:** BCE

**Explanation:**

Reference: <https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/networking/configure-interfaces/use-interface-management-profiles-to-restrict-access.html>

#### **QUESTION 399**

A customer is replacing its legacy remote-access VPN solution. Prisma Access has been selected as the replacement. During onboarding, the following options and licenses were selected and enabled:

- Prisma Access for Remote Networks: 300Mbps
- Prisma Access for Mobile Users: 1500 Users
- Cortex Data Lake: 2TB
- Trusted Zones: trust
- Untrusted Zones: untrust
- Parent Device Group: shared

The customer wants to forward to a Splunk SIEM the logs that are generated by users that are connected to Prisma Access for Mobile Users. Which two settings must the customer configure? (Choose two.)

- A. Configure Panorama Collector group device log forwarding to send logs to the Splunk syslog server.
- B. Configure Cortex Data Lake log forwarding and add the Splunk syslog server.
- C. Configure a log forwarding profile and select the Panorama/Cortex Data Lake checkbox. Apply the Log Forwarding profile to all of the security policy rules in Mobile\_User\_Device\_Group.
- D. Configure a Log Forwarding profile, select the syslog checkbox, and add the Splunk syslog server. Apply the Log Forwarding profile to all of the security policy rules in the Mobile\_User\_Device\_Group.

**Answer:** BC

**Explanation:**

Reference: <https://docs.paloaltonetworks.com/cortex/cortex-data-lake/cortex-data-lake-getting-started/get-started-with-log-forwarding-app/forward-logs-from-logging-service-to-syslog-server.html>

#### **QUESTION 400**

A network security engineer has applied a File Blocking profile to a rule with the action of Block. The user of a Linux CLI operating system has opened a ticket. The ticket states that the user is being blocked by the firewall when trying to download a TAR file. The user is getting no error response on the system.

Where is the best place to validate if the firewall is blocking the user's TAR file?

- A. Threat log
- B. Data Filtering log

- C. WildFire Submissions log
- D. URL Filtering log

**Answer: B**

**Explanation:**

Reference: <https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIZ1CAK>

#### **QUESTION 401**

Using multiple templates in a stack to manage many firewalls provides which two advantages? (Choose two.)

- A. inherit address-objects from templates
- B. define a common standard template configuration for firewalls
- C. standardize server profiles and authentication configuration across all stacks
- D. standardize log-forwarding profiles for security policies across all stacks

**Answer: AB**

**Explanation:**

Reference: <https://docs.paloaltonetworks.com/panorama/10-0/panorama-admin/panorama-overview/centralized-firewall-configuration-and-update-management/templates-and-template-stacks>

#### **QUESTION 402**

An enterprise Information Security team has deployed policies based on AD groups to restrict user access to critical infrastructure systems. However, a recent phishing campaign against the organization has prompted information Security to look for more controls that can secure access to critical assets. For users that need to access these systems, Information Security wants to use PAN-OS multi-factor authentication (MFA) integration to enforce MFA. What should the enterprise do to use PAN-OS MFA?

- A. Use a Credential Phishing agent to detect, prevent, and mitigate credential phishing campaigns.
- B. Create an authentication profile and assign another authentication factor to be used by a Captive Portal authentication policy.
- C. Configure a Captive Portal authentication policy that uses an authentication sequence.
- D. Configure a Captive Portal authentication policy that uses an authentication profile that references a RADIUS profile.

**Answer: B**

**Explanation:**

Reference: [https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/authentication/configure-multi-factor-authentication.html#id1eeb304d-b2f4-46a3-a3b8-3d84c69fb214\\_idc4b47dbd-9777-4ec8-be70-c16ca0ea1756](https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/authentication/configure-multi-factor-authentication.html#id1eeb304d-b2f4-46a3-a3b8-3d84c69fb214_idc4b47dbd-9777-4ec8-be70-c16ca0ea1756)

#### **QUESTION 403**

An enterprise has a large Palo Alto Networks footprint that includes onsite firewalls and Prisma Access for mobile users, which is managed by Panorama. The enterprise already uses GlobalProtect with SAML authentication to obtain IP-to-user mapping information. However, Information Security wants to use this information in Prisma Access for policy enforcement based on group mapping. Information Security uses on-premises Active Directory (AD) but is uncertain about what is needed for Prisma Access to learn groups from AD. How can policies based on group mapping be learned and enforced in Prisma Access?

- A. Configure Prisma Access to learn group mapping via SAML assertion.
- B. Set up group mapping redistribution between an onsite Palo Alto Networks firewall and Prisma Access.
- C. Assign a master device in Panorama through which Prisma Access learns groups.
- D. Create a group mapping configuration that references an LDAP profile that points to on-premises domain controllers.

**Answer: C**

**Explanation:**

Reference: <https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-panorama-admin/configure-user-based-policies-with-prisma-access/retrieve-user-id-information.html#id823f5b30-2c1d-4c87-9ae6-a06573455af7>

**QUESTION 404**

What happens to traffic traversing SD-WAN fabric that doesn't match any SD-WAN policies?

- A. Traffic is dropped because there is no matching SD-WAN policy to direct traffic.
- B. Traffic matches a catch-all policy that is created through the SD-WAN plugin.
- C. Traffic matches implied policy rules and is redistributed round robin across SD-WAN links.
- D. Traffic is forwarded to the first physical interface participating in SD-WAN based on lowest interface number (i.e., Eth1/1 over Eth1/3).

**Answer: C**

**Explanation:**

Reference: <https://docs.paloaltonetworks.com/sd-wan/1-0/sd-wan-admin/configure-sd-wan/distribute-unmatched-sessions.html>

**QUESTION 405**

A remote administrator needs firewall access on an untrusted interface. Which two components are required on the firewall to configure certificate-based administrator authentication to the web UI? (Choose two.)

- A. certificate authority (CA) certificate
- B. server certificate
- C. client certificate
- D. certificate profile

**Answer: CD**

**Explanation:**

Reference: <https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/firewall-administration/manage-firewall-administrators/configure-administrative-accounts-and-authentication/configure-certificate-based-administrator-authentication-to-the-web-interface.html>

**QUESTION 406**

An administrator with 84 firewalls and Panorama does not see any WildFire logs in Panorama. All 84 firewalls have an active WildFire subscription. On each firewall, WildFire logs are available.

This issue is occurring because forwarding of which type of logs from the firewalls to Panorama is missing?

- A. WildFire logs
- B. System logs
- C. Threat logs
- D. Traffic logs

**Answer: A**

**Explanation:**

Reference: <https://docs.paloaltonetworks.com/panorama/8-1/panorama-admin/manage-log-collection/configure-log-forwarding-to-panorama.html>

**QUESTION 407**

A company wants to use their Active Directory groups to simplify their Security policy creation from Panorama. Which configuration is necessary to retrieve groups from Panorama?

- A. Configure an LDAP Server profile and enable the User-ID service on the management interface.
- B. Configure a group mapping profile to retrieve the groups in the target template.
- C. Configure a Data Redistribution Agent to receive IP User Mappings from User-ID agents.
- D. Configure a master device within the device groups.



**Answer:** D

**Explanation:**

Reference: <https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PMtpCAG>

#### **QUESTION 408**

How can packet buffer protection be configured?

- A. at zone level to protect firewall resources and ingress zones, but not at the device level
- B. at the interface level to protect firewall resources
- C. at the device level (globally) to protect firewall resources and ingress zones, but not at the zone level
- D. at the device level (globally) and, if enabled globally, at the zone level

**Answer:** D

**Explanation:**

Reference: <https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/zone-protection-and-dos-protection/configure-zone-protection-to-increase-network-security/configure-packet-buffer-protection>

#### **QUESTION 409**

An existing NGFW customer requires direct internet access offload locally at each site, and IPSec connectivity to all branches over public internet. One requirement is that no new SD-WAN hardware be introduced to the environment. What is the best solution for the customer?

- A. Configure a remote network on PAN-OS
- B. Upgrade to a PAN-OS SD-WAN subscription
- C. Configure policy-based forwarding
- D. Deploy Prisma SD-WAN with Prisma Access

**Answer:** B

**Explanation:**

Reference: <https://docs.paloaltonetworks.com/sd-wan/1-0/sd-wan-admin/sd-wan-overview/about-sd-wan.html>

#### **QUESTION 410**

A firewall administrator requires an A/P HA pair to fail over more quickly due to critical business application uptime requirements.

What is the correct setting?

- A. Change the HA timer profile to "user-defined" and manually set the timers.
- B. Change the HA timer profile to "fast".
- C. Change the HA timer profile to "aggressive" or customize the settings in advanced profile.
- D. Change the HA timer profile to "quick" and customize in advanced profile.

**Answer:** C

**Explanation:**

Reference: <https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/high-availability/set-up-activepassive-ha/configure-activepassive-ha.html>

#### **QUESTION 411**

What is the function of a service route?

- A. The service packets exit the firewall on the port assigned for the external service. The server sends its response to the configured source interface and source IP address.
- B. The service packets enter the firewall on the port assigned from the external service. The server sends its response to the configured destination interface and destination IP address.
- C. The service route is the method required to use the firewall's management plane to provide

services to applications.

- D. Service routes provide access to external services, such as DNS servers, external authentication servers or Palo Alto Networks services like the Customer Support Portal.

**Answer:** A

**Explanation:**

Reference: <https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/networking/service-routes.html>

#### QUESTION 412

Which of the following commands would you use to check the total number of the sessions that are currently going through SSL Decryption processing?

- A. show session all filter ssl-decryption yes total-count yes
- B. show session all ssl-decrypt yes count yes
- C. show session all filter ssl-decrypt yes count yes
- D. show session filter ssl-decryption yes total-count yes

**Answer:** C

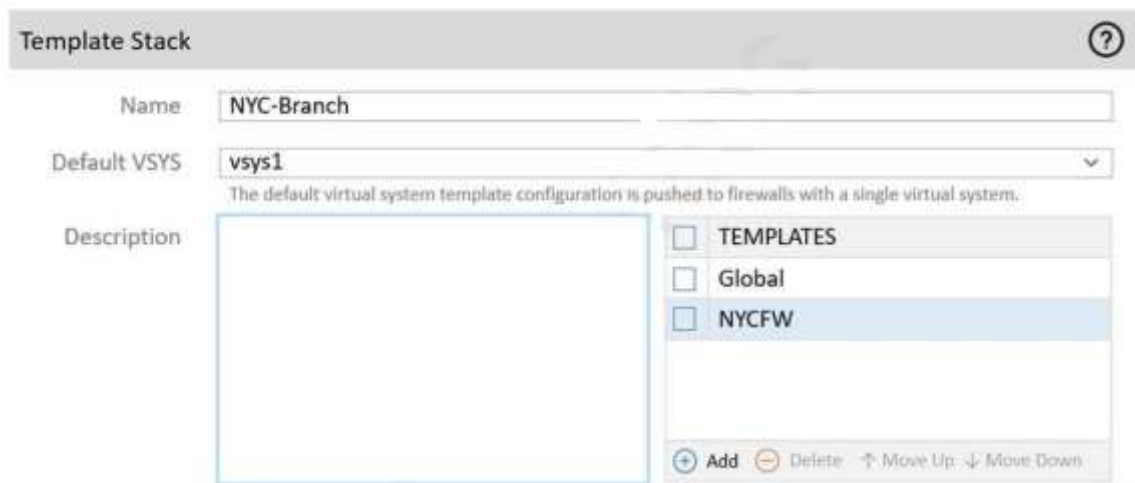
**Explanation:**

Reference: <https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000C1F2CAK>

#### QUESTION 413

Refer to the image. An administrator is tasked with correcting an NTP service configuration for firewalls that cannot use the Global template NTP servers. The administrator needs to change the IP address to a preferable server for this template stack but cannot impact other template stacks.

How can the issue be corrected?



- A. Override the value on the NYCFW template.
- B. Override a template value using a template stack variable.
- C. Override the value on the Global template.
- D. Enable "objects defined in ancestors will take higher precedence" under Panorama settings.

**Answer:** A

**Explanation:**

Reference: <https://docs.paloaltonetworks.com/panorama/9-0/panorama-admin/panorama-overview/centralized-firewall-configuration-and-update-management/templates-and-template-stacks>

#### QUESTION 414

While troubleshooting an SSL Forward Proxy decryption issue, which PAN-OS CLI command would you use to check the details of the end entity certificate that is signed by the Forward Trust Certificate or Forward Untrust Certificate?



- A. show system setting ssl-decrypt certs
- B. show system setting ssl-decrypt certificate
- C. debug dataplane show ssl-decrypt ssl-stats
- D. show system setting ssl-decrypt certificate-cache

**Answer:** B

**Explanation:**

Reference: <https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000C1F2CAK>

#### **QUESTION 415**

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

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

**Answer:** C

**Explanation:**

Reference: [https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u0000001UiOCAU&lang=en\\_US%E2%80%A9&refURL=http%3A%2F%2Fknowledgebase.paloaltonetworks.com%2FKCSArticleDetail](https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u0000001UiOCAU&lang=en_US%E2%80%A9&refURL=http%3A%2F%2Fknowledgebase.paloaltonetworks.com%2FKCSArticleDetail)

#### **QUESTION 416**

In URL filtering, which component matches URL patterns?

- A. live URL feeds on the management plane
- B. security processing on the data plane
- C. single-pass pattern matching on the data plane
- D. signature matching on the data plane

**Answer:** C

**Explanation:**

Reference: <https://www.firewall.cx/networking-topics/firewalls/palo-alto-firewalls/1152-palo-alto-firewall-single-pass-parallel-processing-hardware-architecture.html>

#### **QUESTION 417**

In a template, you can configure which two objects? (Choose two.)

- A. Monitor profile
- B. application group
- C. SD-WAN path quality profile
- D. IPsec tunnel

**Answer:** BC

#### **QUESTION 418**

An organization's administrator has the funds available to purchase more firewalls to increase the organization's security posture.

The partner SE recommends placing the firewalls as close as possible to the resources that they protect. Is the SE's advice correct, and why or why not?

- A. No. Firewalls provide new defense and resilience to prevent attackers at every stage of the cyberattack lifecycle, independent of placement.
- B. Yes. Firewalls are session-based, so they do not scale to millions of CPS.

- C. No. Placing firewalls in front of perimeter DDoS devices provides greater protection for sensitive devices inside the network.
- D. Yes. Zone Protection profiles can be tailored to the resources that they protect via the configuration of specific device types and operating systems.

**Answer: D**

**Explanation:**

Reference: <https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/zone-protection-and-dos-protection.html>

#### **QUESTION 419**

An administrator needs to validate that policies that will be deployed will match the appropriate rules in the device-group hierarchy.

Which tool can the administrator use to review the policy creation logic and verify that unwanted traffic is not allowed?

- A. Preview Changes
- B. Policy Optimizer
- C. Managed Devices Health
- D. Test Policy Match

**Answer: D**

**Explanation:**

Reference: <https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/test-policy-rule-traffic-matches.html>

#### **QUESTION 420**

What is a key step in implementing WildFire best practices?

- A. Configure the firewall to retrieve content updates every minute.
- B. Ensure that a Threat Prevention subscription is active.
- C. In a mission-critical network, increase the WildFire size limits to the maximum value.
- D. In a security-first network, set the WildFire size limits to the minimum value.

**Answer: B**

**Explanation:**

Reference: <https://docs.paloaltonetworks.com/wildfire/9-1/wildfire-admin/wildfire-deployment-best-practices/wildfire-best-practices>

#### **QUESTION 421**

What happens when an A/P firewall cluster synchronizes IPsec tunnel security associations (SAs)?

- A. Phase 2 SAs are synchronized over HA2 links.
- B. Phase 1 and Phase 2 SAs are synchronized over HA2 links.
- C. Phase 1 SAs are synchronized over HA1 links.
- D. Phase 1 and Phase 2 SAs are synchronized over HA3 links.

**Answer: A**

**Explanation:**

Reference:

[https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000HAuZCAW&lang=en\\_US%E2%80%A99&refURL=http%3A%2F%2Fknowledgebase.paloaltonetworks.com%2FKCSArticleDetail](https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000HAuZCAW&lang=en_US%E2%80%A99&refURL=http%3A%2F%2Fknowledgebase.paloaltonetworks.com%2FKCSArticleDetail)