

## PCNSE Dumps

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

<https://www.certleader.com/PCNSE-dumps.html>



**NEW QUESTION 1**

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. URL Filtering log
- B. Data Filtering log
- C. Threat log
- D. WildFire Submissions log

**Answer:** B

**NEW QUESTION 2**

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 3**

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

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

**Answer:** D

**Explanation:**

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/policy/security-profiles.html> First note in above link states:

"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."

The first thing the firewall checks per its flow is the security policy match and action. The Security Profile never gets checked if a match happens on a policy set to deny that match.

**NEW QUESTION 4**

A standalone firewall with local objects and policies needs to be migrated into Panorama. What procedure should you use so Panorama is fully managing the firewall?

- A. Use the "import Panorama configuration snapshot" operation, then perform a device-group commit push with "include device and network templates"
- B. Use the "import device configuration to Panorama" operation, then "export or push device config bundle" to push the configuration
- C. Use the "import Panorama configuration snapshot" operation, then "export or push device config bundle" to push the configuration
- D. Use the "import device configuration to Panorama" operation, then perform a device-group commit push with "include device and network templates"

**Answer:** B

**Explanation:**

<https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/manage-firewalls/transition-a-firewall-to-pan>

**NEW QUESTION 5**

Given the screenshot, how did the firewall handle the traffic?

Detailed Log View		
General	Source	Destination
Session ID: 202702	Source User: [REDACTED]	Destination User: [REDACTED]
Action: allow	Source: [REDACTED]	Destination: 191.96.150.165
Action Source: from-policy	Source DAG: [REDACTED]	Destination DAG: [REDACTED]
Host ID: [REDACTED]	Country: 192.168.0.0-192.168.255.255	Country: United States
Application: ssl	Port: 51153	Port: 9002
Rule: non-standard-ports	Zone: LAN	Zone: Internet
Rule UUID: c88e907d-1d17-457e-8600-b7e2654f78b1	Interface: ethernet1/2	Interface: ethernet1/8
Session End Reason: threat	NAT IP: [REDACTED]	NAT IP: 191.96.150.165
Category: proxy-avoidance-and-anonymizers	NAT Port: 47076	NAT Port: 9002
Device SN: 007251000156341	X-Forwarded-For IP: 0.0.0.0	
IP Protocol: tcp		
Log Action: global-logs		
Generated Time: 2022/03/08 07:36:29		
Start Time: 2022/03/08 07:34:55		
Receive Time: 2022/03/08 07:36:38		
Elapsed Time(sec): 0		
Tunnel Type: N/A		
Details		
Type: end		
Bytes: 801		
Bytes Received: 74		
Bytes Sent: 727		
Repeat Count: 1		
Packets: 4		
Packets Received: 1		
Packets Sent: 3		
Source UUID: [REDACTED]		
Destination UUID: [REDACTED]		
Dynamic User Group: [REDACTED]		
Network Slice ID SD: 0		
Network Slice ID SST: 0		
App Category: networking		
App Subcategory: encrypted-tunnel		
App Technology: browser-based		
App Characteristic: used-by-malware,able-to-transfer-file,has-known-vulnerability,tunnel-other-application,pervasive-use		
App Container: [REDACTED]		
App Risk: 4		
App SaaS: no		
App Sanctioned State: no		
SDWAN		
Flags		
Captive Portal: <input type="checkbox"/>		
Proxy Transaction: <input type="checkbox"/>		
Decrypted: <input type="checkbox"/>		
Packet Capture: <input type="checkbox"/>		
Client to Server: <input type="checkbox"/>		
Server to Client: <input type="checkbox"/>		
Symmetric Return: <input type="checkbox"/>		
Mirrored: <input type="checkbox"/>		
Tunnel Inspected: <input type="checkbox"/>		
MPTCP Options: <input type="checkbox"/>		
Recon excluded: <input type="checkbox"/>		
Forwarded to Security Chain: <input type="checkbox"/>		
DeviceID		
Source Device Category: Network Security Equipment		
Source Device Profile: Palo Alto Networks Device		
Source Device Model: MacPro		
Source Device Vendor: Palo Alto Networks, Inc.		
Source Device OS Family: PAN-OS		
Source Device OS Version: [REDACTED]		
Source Device Host: MacPro		

- A. Traffic was allowed by profile but denied by policy as a threat
- B. Traffic was allowed by policy but denied by profile as..
- C. Traffic was allowed by policy but denied by profile as ..
- D. Traffic was allowed by policy but denied by profile as a..

**Answer: D**

#### NEW QUESTION 6

A company with already deployed Palo Alto firewalls has purchased their first Panorama server. The security team has already configured all firewalls with the Panorama IP address and added all the firewall serial numbers in Panorama. What are the next steps to migrate configuration from the firewalls to Panorama?

- A. Use API calls to retrieve the configuration directly from the managed devices
- B. Export Named Configuration Snapshot on each firewall followed by Import Named Configuration Snapshot in Panorama
- C. import Device Configuration to Panorama followed by Export or Push Device Config Bundle
- D. Use the Firewall Migration plugin to retrieve the configuration directly from the managed devices

**Answer: C**

#### NEW QUESTION 7

Which benefit do policy rule UUIDs provide?

- A. An audit trail across a policy's lifespan
- B. Functionality for scheduling policy actions
- C. The use of user IP mapping and groups in policies
- D. Cloning of policies between device-groups

**Answer: A**

#### NEW QUESTION 8

A firewall administrator has been tasked with ensuring that all Panorama-managed firewalls forward traffic logs to Panorama. In which section is this configured?

- A. Panorama > Managed Devices
- B. Monitor > Logs > Traffic
- C. Device Groups > Objects > Log Forwarding
- D. Templates > Device > Log Settings

**Answer: C**

#### NEW QUESTION 9

An engineer wants to configure aggregate interfaces to increase bandwidth and redundancy between the firewall and switch. Which statement is correct about the

configuration of the interfaces assigned to an aggregate interface group?

- A. They can have a different bandwidth.
- B. They can have a different interface type such as Layer 3 or Layer 2.
- C. They can have a different interface type from an aggregate interface group.
- D. They can have different hardware media such as the ability to mix fiber optic and copper.

**Answer: C**

#### NEW QUESTION 10

Which statement regarding HA timer settings is true?

- A. Use the Recommended profile for typical failover timer settings
- B. Use the Moderate profile for typical failover timer settings
- C. Use the Aggressive profile for slower failover timer settings.
- D. Use the Critical profile for faster failover timer settings.

**Answer: A**

#### NEW QUESTION 10

A company is looking to increase redundancy in their network. Which interface type could help accomplish this?

- A. Layer 2
- B. Virtual wire
- C. Tap
- D. Aggregate ethernet

**Answer: D**

#### Explanation:

An aggregate group increases the bandwidth between peers by load balancing traffic across the combined interfaces. It also provides redundancy  
<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-networking-admin/configure-interfaces/configure-an-agg>

#### NEW QUESTION 13

A network administrator is trying to prevent domain username and password submissions to phishing sites on some allowed URL categories  
Which set of steps does the administrator need to take in the URL Filtering profile to prevent credential phishing on the firewall?

- A. Choose the URL categories on Site Access column and set action to block Click the User credential Detection tab and select IP User Mapping Commit
- B. Choose the URL categories in the User Credential Submission column and set action to block Select the User credential Detection tab and select use IP User Mapping Commit
- C. Choose the URL categories in the User Credential Submission column and set action to block Select the URL filtering settings and enable Domain Credential Filter Commit
- D. Choose the URL categories in the User Credential Submission column and set action to block Select the User credential Detection tab and select Use Domain Credential Filter Commit

**Answer: D**

#### Explanation:

credential phishing prevention works by scanning username and password submissions to websites and comparing those submissions to known corporate credentials. You can configure solutions that detect and prevent credential phishing using URL filtering profiles and User-ID agents.

#### NEW QUESTION 14

In the screenshot above which two pieces of information can be determined from the ACC configuration shown? (Choose two )



- A. The Network Activity tab will display all applications, including FTP.
- B. Threats with a severity of "high" are always listed at the top of the Threat Name list
- C. Insecure-credentials, brute-force and protocol-anomaly are all a part of the vulnerability Threat Type
- D. The ACC has been filtered to only show the FTP application

**Answer: AC**

**NEW QUESTION 18**

An administrator is seeing one of the firewalls in a HA active/passive pair moved to 'suspended' state due to Non-functional loop. Which three actions will help the administrator troubleshoot this issue? (Choose three.)

- A. Use the CLI command show high-availability flap-statistics
- B. Check the HA Link Monitoring interface cables.
- C. Check the High Availability > Link and Path Monitoring settings.
- D. Check High Availability > Active/Passive Settings > Passive Link State
- E. Check the High Availability > HA Communications > Packet Forwarding settings.

**Answer:** ABC

**NEW QUESTION 20**

Refer to the image.

Template Stack

Name: NYC-Branch

Default VSYS: vsys1

The default virtual system template configuration is pushed to firewalls with a single virtual system.

Description:

- ☐ TEMPLATES
- ☐ Global
- ☒ NYCFW

+ Add - Delete ↑ Move Up ↓ Move Down

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:** B

**Explanation:**

Both templates and template stacks support variables. Variables allow you to create placeholder objects with their value specified in the template or template stack based on your configuration needs. Create a template or template stack variable to replace IP addresses, Group IDs, and interfaces in your configurations. <https://docs.paloaltonetworks.com/panorama/10-0/panorama-admin/manage-firewalls/manage-templates-and-te>

**NEW QUESTION 24**

What is the best description of the HA4 Keep-Alive Threshold (ms)?

- A. the maximum interval between hello packets that are sent to verify that the HA functionality on the other firewall is operational.
- B. The time that a passive or active-secondary firewall will wait before taking over as the active or active-primary firewall
- C. the timeframe within which the firewall must receive keepalives from a cluster member to know that the cluster member is functional.
- D. The timeframe that the local firewall wait before going to Active state when another cluster member is preventing the cluster from fully synchronizing.

**Answer:** C

**NEW QUESTION 25**

A network administrator wants to use a certificate for the SSL/TLS Service Profile. Which type of certificate should the administrator use?

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

**Answer:** D

**Explanation:**

Use only signed certificates, not CA certificates, in SSL/TLS service profiles. <https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/certificate-management/configure-an-ssltls-service>

**NEW QUESTION 28**

After configuring HA in Active/Passive mode on a pair of firewalls the administrator gets a failed commit with the following details.



What are two explanations for this type of issue? (Choose two)

- A. The peer IP is not included in the permit list on Management Interface Settings
- B. The Backup Peer HA1 IP Address was not configured when the commit was issued
- C. Either management or a data-plane interface is used as HA1-backup
- D. One of the firewalls has gone into the suspended state

Answer: BC

Explanation:

Cause The issue is seen when the HA1-backup is configured with either management (MGT) or an in-band interface. The "Backup Peer HA1 IP Address" is not configured : [https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u0000008UmPCAU&lang=en\\_US%E](https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u0000008UmPCAU&lang=en_US%E)

NEW QUESTION 31

Refer to the exhibit.

Device Group

DATACENTER\_DG

	NAME	LOCATION	ADDRESS
<input type="checkbox"/>	Server-1	DATACENTER_DG	2.2.2.2
<input type="checkbox"/>	Server-1	Shared	1.1.1.1

Device Group

DC\_FW\_DG

	NAME	LOCATION	ADDRESS
<input type="checkbox"/>	Server-1	DC_FW_DG	3.3.3.3
<input type="checkbox"/>	Server-1	Shared	1.1.1.1

Device Group

FW-1\_DG

	NAME	LOCATION	ADDRESS
<input type="checkbox"/>	Server-1	FW-1_DG	4.4.4.4
<input type="checkbox"/>	Server-1	Shared	1.1.1.1

☐

NAME ^

☐ Shared

☐ DATACENTER\_DG

☐ DC\_FW\_DG

☐ FW-1\_DG

☐ REGIONAL\_DG

☐ OFFICE\_FW\_DG

- Review the screenshots and consider the following information:
- FW-1 is assigned to the FW-1\_DG device group, and FW-2 is assigned to OFFICE\_FW\_DG.
  - There are no objects configured in REGIONAL\_DG and OFFICE\_FW\_DG device groups.
- Which IP address will be pushed to the firewalls inside Address Object Server-1?

- A. Server-1 on FW-1 will have IP 1.1.1.1. Server-1 will not be pushed to FW-2.
- B. Server-1 on FW-1 will have IP 3.3.3.3. Server-1 will not be pushed to FW-2.
- C. Server-1 on FW-1 will have IP 2.2.2.2. Server-1 will not be pushed to FW-2.
- D. Server-1 on FW-1 will have IP 4.4.4.4. Server-1 on FW-2 will have IP 1.1.1.1.

Answer: C

NEW QUESTION 33

An engineer has been tasked with reviewing traffic logs to find applications the firewall is unable to identify with App-ID. Why would the application field display as

incomplete?

- A. The client sent a TCP segment with the PUSH flag set.
- B. The TCP connection was terminated without identifying any application data.
- C. There is insufficient application data after the TCP connection was established.
- D. The TCP connection did not fully establish.

**Answer: C**

#### NEW QUESTION 36

A network security administrator has been tasked with deploying User-ID in their organization. What are three valid methods of collecting User-ID information in a network? (Choose three.)

- A. Windows User-ID agent
- B. GlobalProtect
- C. XMLAPI
- D. External dynamic list
- E. Dynamic user groups

**Answer: ABC**

#### Explanation:

User-ID is a feature that enables the firewall to identify users and groups based on their IP addresses, usernames, or other attributes.

There are three valid methods of collecting User-ID information in a network:

- Windows User-ID agent: This is a software agent that runs on a Windows server and collects user mapping information from Active Directory, Exchange servers, or other sources.
- GlobalProtect: This is a VPN solution that provides secure remote access for users and devices. It also collects user mapping information from endpoints that connect to the firewall using GlobalProtect.
- XMLAPI: This is an application programming interface that allows third-party applications or scripts to send user mapping information to the firewall using XML format.

#### NEW QUESTION 40

An engineer discovers the management interface is not routable to the User-ID agent What configuration is needed to allow the firewall to communicate to the User-ID agent?

- A. Create a NAT policy for the User-ID agent server
- B. Add a Policy Based Forwarding (PBF) policy to the User-ID agent IP
- C. Create a custom service route for the UID Agent
- D. Add a static route to the virtual router

**Answer: C**

#### Explanation:

To allow the firewall to communicate with the User-ID agent, you need to configure a custom service route f the UID Agent23. A custom service route allows you to specify which interface and source IP address the firewall uses to connect to a specific destination service. By default, the firewall uses its management interface for services such as User-ID, but you can override this behavior by creating a custom service route.

To configure a custom service route for the UID Agent, you need to do the following steps:

- Go to Device > Setup > Services and click Service Route Configuration.
- In the Service column, select User-ID Agent from the drop-down list.
- In the Interface column, select an interface that can reach the User-ID agent server from the drop-down list.
- In the Source Address column, select an IP address that belongs to that interface from the drop-down list.
- Click OK and Commit your changes.

The correct answer is C. Create a custom service route for UID Agent

#### NEW QUESTION 45

An administrator wants to grant read-only access to all firewall settings, except administrator accounts, to a new-hire colleague in the IT department. Which dynamic role does the administrator assign to the new-hire colleague?

- A. Device administrator (read-only)
- B. System administrator (read-only)
- C. Firewall administrator (read-only)
- D. Superuser (read-only)

**Answer: A**

#### NEW QUESTION 49

Review the screenshot of the Certificates page.

Device Certificates									
Default Trusted Certificate Authorities									
NAME	SUBJECT	ISSUER	CA	KEY	EXPIRES	STATUS	AUTHORITY	USAGE	
Self-Signed Root CA	C = US, ST = CA, O = Small Business LLC, CN = 192.168.127.24, mail=...	C = US, ST = CA, O = Small Business LLC, CN = 192.168.127.24, emailAddress = admin@smallbusiness...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Exp: 13/09/26 17:00:00 GMT	valid	RSA	Trusted Root CA Certificate	
Firewall Untrusted	CN = 192.168.127.24	CN = 192.168.127.24	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Exp: 13/09/26 17:00:00 GMT	valid	RSA	Firewall Untrusted Certificate	
External Root	CN = 192.168.127.24	CN = 192.168.127.24	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Exp: 13/09/26 17:00:00 GMT	valid	RSA	External Root Certificate	

An administrator for a small LLC has created a series of certificates as shown, to use for a planned Decryption roll out The administrator has also installed the self-signed root certificate <n all client systems When testing, they noticed that every time a user visited an SSL site they received unsecured website warnings What is the cause of the unsecured website warnings.

- A. The forward trust certificate has not been signed by the self-signed root CA certificate
- B. The self-signed CA certificate has the same CN as the forward trust and untrust certificates
- C. The forward untrust certificate has not been signed by the self-signed root CA certificate
- D. The forward trust certificate has not been installed in client systems

**Answer:** C

#### NEW QUESTION 53

An administrator is receiving complaints about application performance degradation. After checking the ACC, the administrator observes that there is an excessive amount of SSL traffic

Which three elements should the administrator configure to address this issue? (Choose three.)

- A. QoS on the ingress interface for the traffic flows
- B. An Application Override policy for the SSL traffic
- C. A QoS policy for each application ID
- D. A QoS profile defining traffic classes
- E. QoS on the egress interface for the traffic flows

**Answer:** BCD

#### NEW QUESTION 54

When planning to configure SSL Forward Proxy on a PA 5260, a user asks how SSL decryption can be implemented using phased approach in alignment with Palo Alto Networks best practices

What should you recommend?

- A. Enable SSL decryption for known malicious source IP addresses
- B. Enable SSL decryption for source users and known malicious URL categories
- C. Enable SSL decryption for malicious source users
- D. Enable SSL decryption for known malicious destination IP addresses

**Answer:** B

#### NEW QUESTION 56

An engineer has discovered that certain real-time traffic is being treated as best effort due to it exceeding defined bandwidth. Which QoS setting should the engineer adjust?

- A. QoS profile: Egress Max
- B. QoS interface: Egress Guaranteed
- C. QoS profile: Egress Guaranteed
- D. QoS interface: Egress Max

**Answer:** C

#### Explanation:

When the egress guaranteed bandwidth is exceeded, the firewall passes traffic on a best-effort basis. <https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/quality-of-service/qos-concepts/qos-bandwidth-management>

#### NEW QUESTION 61

What best describes the HA Promotion Hold Time?

- A. the time that is recommended to avoid an HA failover due to the occasional flapping of neighboring devices
- B. the time that is recommended to avoid a failover when both firewalls experience the same link/path monitor failure simultaneously
- C. the time that the passive firewall will wait before taking over as the active firewall after communications with the HA peer have been lost
- D. the time that a passive firewall with a low device priority will wait before taking over as the active firewall if the firewall is operational again

**Answer:** C

#### NEW QUESTION 63

An administrator is configuring SSL decryption and needs to ensure that all certificates for both SSL Inbound inspection and SSL Forward Proxy are installed properly on the firewall. When certificates are being imported to the firewall for these purposes, which three certificates require a private key? (Choose three.)

- A. Forward Untrust certificate
- B. Forward Trust certificate
- C. Enterprise Root CA certificate
- D. End-entity (leaf) certificate
- E. Intermediate certificate(s)

**Answer:** ABD

#### Explanation:

This is discussed in the Palo Alto Networks PCNSE Study Guide in Chapter 9: Decryption, under the section "SSL Forward Proxy and Inbound Inspection Certificates":

"When importing SSL decryption certificates, you need to provide private keys for the forward trust, forward untrust, and end-entity (leaf) certificates. You do not need to provide private keys for the root CA and intermediate certificates."

#### NEW QUESTION 66

An administrator Just enabled HA Heartbeat Backup on two devices However, the status on tie firewall's dashboard is showing as down High Availability. What could an administrator do to troubleshoot the issue?

- A. Goto Device > High Availability> General > HA Pair Settings > Setup and configuring the peer IP for heartbeat backup
- B. Check peer IP address In the permit list In Device > Setup > Management > Interfaces > Management Interface Settings
- C. Go to Device > High Availability > HA Communications> General> and check the Heartbeat Backup under Election Settings
- D. Check peer IP address for heartbeat backup to Device > High Availability > HA Communications > Packet Forwarding settings.

**Answer: B**

**Explanation:**

If the HA status is showing as down after enabling HA Heartbeat Backup on two devices, an administrator could troubleshoot the issue by checking the peer IP address in the permit list in Device > Setup > Management > Interfaces > Management Interface Settings. This is described in the Palo Alto Networks PCNSE Study Guide in Chapter 7: High Availability, under the section "Configure Heartbeat Backup for Redundancy":

"Verify that the management interface's permitted IP addresses on each peer includes the IP address of the other peer's Heartbeat Backup interface."

**NEW QUESTION 69**

What is the function of a service route?

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

**NEW QUESTION 73**

How would an administrator configure a Bidirectional Forwarding Detection profile for BGP after enabling the Advance Routing Engine run on PAN-OS 10.2?

- A. create a BFD profile under Network > Network Profiles > BFD Profile and then select the BFD profile under Network > Virtual Router > BGP > BFD
- B. create a BFD profile under Network > Routing > Routing Profiles > BFD and then select the BFD profile under Network > Virtual Router > BGP > General > Global BFD Profile
- C. create a BFD profile under Network > Routing > Routing Profiles > BFD and then select the BFD profile under Network > Routing > Logical Routers > BGP > General > Global BFD Profile
- D. create a BFD profile under Network > Network Profiles > BFD Profile and then select the BFD profile under Network > Routing > Logical Routers > BGP > BFD

**Answer: B**

**NEW QUESTION 74**

Refer to the exhibit.

	NAME	LOCATION	TAGS	TYPE
1	Intrazone-default	Shared	none	Intrazone
2	Interzone-default	Predefined	none	Interzone

Based on the screenshots above what is the correct order in which the various rules are deployed to firewalls inside the DATACENTER\_DG device group?

- A. shared pre-rules DATACENTER DG pre rulesrules configured locally on the firewall shared post-rules DATACENTER\_DG post-rules DATACENTER.DG default rules
- B. shared pre-rulesDATACENTER\_DG pre-rulesrules configured locally on the firewall shared post-rulesDATACENTER.DG post-rules shared default rules
- C. shared pre-rules DATACENTER\_DG pre-rulesrules configured locally on the firewall DATACENTER\_DG post-rules shared post-rulesshared default rules
- D. shared pre-rules DATACENTER\_DG pre-rulesrules configured locally on the firewall DATACENTER\_DG post-rules shared post-rules DATACENTER\_DG default rules

**Answer: A**

**NEW QUESTION 77**

Which GlobalProtect component must be configured to enable Clientless VPN?

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

**Answer: C**

**Explanation:**

Creating the GlobalProtect portal is as simple as letting it know if you have accessed it already. A new gateway for accessing the GlobalProtect portal will appear. Client authentication can be used with an existing one.

<https://www.nstec.com/how-to-configure-clientless-vpn-in-palo-alto/#5>

**NEW QUESTION 79**

An administrator has two pairs of firewalls within the same subnet. Both pairs of firewalls have been configured to use High Availability mode with Active/Passive.

The ARP tables for upstream routes display the same MAC address being shared for some of these firewalls.  
What can be configured on one pair of firewalls to modify the MAC addresses so they are no longer in conflict?

- A. Configure a floating IP between the firewall pairs.
- B. Change the Group IDs in the High Availability settings to be different from the other firewall pair on the same subnet.
- C. Change the interface type on the interfaces that have conflicting MAC addresses from L3 to VLAN.
- D. On one pair of firewalls, run the CLI command: set network interface vlan arp.

**Answer: B**

**Explanation:**

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Cm1OCAS>

change the Group IDs in the High Availability settings to be different from the other firewall pair on the same subnet. This will prevent the MAC addresses from conflicting and allow the firewalls to properly route traffic. You can also configure a floating IP between the firewall pairs if necessary.

**NEW QUESTION 82**

An administrator has configured a pair of firewalls using high availability in Active/Passive mode. Link and Path Monitoring Is enabled with the Failure Condition set to "any." There is one link group configured containing member interfaces ethernet1/1 and ethernet1/2 with a Group Failure Condition set to "all."  
Which HA state will the Active firewall go into if ethernet1/1 link goes down due to a failure?

- A. Non-functional
- B. Passive
- C. Active-Secondary
- D. Active

**Answer: D**

**NEW QUESTION 85**

A network security administrator has an environment with multiple forms of authentication. There is a network access control system in place that authenticates and restricts access for wireless users, multiple Windows domain controllers, and an MDM solution for company-provided smartphones. All of these devices have their authentication events logged.

Given the information, what is the best choice for deploying User-ID to ensure maximum coverage?

- A. Syslog listener
- B. agentless User-ID with redistribution
- C. standalone User-ID agent
- D. captive portal

**Answer: C**

**NEW QUESTION 88**

Refer to the diagram. Users at an internal system want to ssh to the SSH server The server is configured to respond only to the ssh requests coming from IP 172.16.16.1.

In order to reach the SSH server only from the Trust zone, which Security rule and NAT rule must be configured on the firewall?



A)

NAT Rule:

Source Zone: Trust  
Source IP: Any  
Destination Zone: Server  
Destination IP: 172.16.15.10  
Source Translation : dynamic-ip-and-port / ethernet1/4

Security Rule:

Source Zone: Trust  
Source IP: Any  
Destination Zone: Server  
Destination IP: 172.16.15.10  
Application: ssh

B)

NAT Rule:

Source Zone: Trust  
Source IP: Any  
Destination Zone: Server  
Destination IP: 172.16.15.10  
Source Translation : Static IP / 172.16.15.1

Security Rule:

Source Zone: Trust  
Source IP: Any  
Destination Zone: Trust  
Destination IP: 172.16.15.10  
Application: ssh

C)

NAT Rule:

Source Zone: Trust  
Source IP: Any  
Destination Zone: Trust  
Destination IP: 192.168.15.1  
Destination Translation : Static IP / 172.16.15.10

Security Rule:

Source Zone: Trust  
Source IP: Any  
Destination Zone: Server  
Destination IP: 172.16.15.10  
Application: ssh

D)

NAT Rule:

Source Zone: Trust  
Source IP: 192.168.15.0/24  
Destination Zone: Trust  
Destination IP: 192.168.15.1  
Destination Translation : Static IP / 172.16.15.10

Security Rule:

Source Zone: Trust  
Source IP: 192.168.15.0/24  
Destination Zone: Server  
Destination IP: 172.16.15.10  
Application: ssh

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

**Answer: C**

#### NEW QUESTION 89

What is a correct statement regarding administrative authentication using external services with a local authorization method?

- A. Prior to PAN-OS 10.2, an administrator used the firewall to manage role assignments, but access domains have not been supported by this method.
- B. Starting with PAN-OS 10.2, an administrator needs to configure Cloud Identity Engine to use external authentication services for administrative authentication.
- C. The administrative accounts you define locally on the firewall serve as references to the accounts defined on an external authentication server.
- D. The administrative accounts you define on an external authentication server serve as references to the accounts defined locally on the firewall.

**Answer: B**

#### NEW QUESTION 93

A customer is replacing their legacy remote access VPN solution. The current solution is in place to secure only internet egress for the connected clients. Prisma Access has been selected to replace the current remote access VPN solution. 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

How can you configure Prisma Access to provide the same level of access as the current VPN solution?

- A. Configure mobile users with trust-to-untrust Security policy rules to allow the desired traffic outbound to the internet.
- B. Configure mobile users with a service connection and trust-to-trust Security policy rules to allow the desired traffic outbound to the internet.
- C. Configure remote networks with a service connection and trust-to-untrust Security policy rules to allow the desired traffic outbound to the internet.
- D. Configure remote networks with trust-to-trust Security policy rules to allow the desired traffic outbound to the internet.

**Answer: D**

#### NEW QUESTION 95

Which three actions can Panorama perform when deploying PAN-OS images to its managed devices? (Choose three.)

- A. upload-only
- B. upload and install and reboot
- C. verify and install
- D. upload and install
- E. install and reboot

**Answer: CDE**

#### NEW QUESTION 100

What can an engineer use with GlobalProtect to distribute user-specific client certificates to each GlobalProtect user?

- A. Certificate profile

- B. SSL/TLS Service profile
- C. OCSP Responder
- D. SCEP

**Answer:** D

#### NEW QUESTION 101

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

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

**Answer:** D

#### NEW QUESTION 104

What would allow a network security administrator to authenticate and identify a user with a new BYOD-type device that is not joined to the corporate domain'?

- A. a Security policy with 'known-user' selected in the Source User field
- B. an Authentication policy with 'unknown' selected in the Source User field
- C. a Security policy with 'unknown' selected in the Source User field
- D. an Authentication policy with 'known-user' selected in the Source User field

**Answer:** C

#### NEW QUESTION 105

An engineer needs to collect User-ID mappings from the company's existing proxies. What two methods can be used to pull this data from third party proxies? (Choose two.)

- A. Syslog
- B. XFF Headers
- C. Client probing
- D. Server Monitoring

**Answer:** AB

#### NEW QUESTION 106

An administrator is using Panorama to manage me and suspects an IKE Crypto mismatch between peers, from the firewalls to Panorama. However, pre-existing logs from the firewalls are not appearing in Panorama.

Which action should be taken to enable the firewalls to send their pre-existing logs to Panorama?

- A. Export the log database.
- B. Use the import option to pull logs.
- C. Use the ACC to consolidate the logs.
- D. Use the scp logdb export command.

**Answer:** D

#### NEW QUESTION 107

An administrator is attempting to create policies for deployment of a device group and template stack. When creating the policies, the zone drop down list does not include the required zone.

What must the administrator do to correct this issue?

- A. Specify the target device as the master device in the device group
- B. Enable "Share Unused Address and Service Objects with Devices" in Panorama settings
- C. Add the template as a reference template in the device group
- D. Add a firewall to both the device group and the template

**Answer:** D

#### NEW QUESTION 109

An administrator can not 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)

**Security Policy Rule** ⓘ

General Source Destination Application Service/URL Category **Actions** Usage

**Action Setting**

Action: **Allow**

☐ Auto NAT Calculation

**Profile Setting**

Profile Type: Profiles

Antivirus: default

Vulnerability Protection: strict

Anti-Spyware: strict

URL Filtering: default

File Blocking: None

Data Filtering: None

Workflow Profiles: default

**Log Setting**

☐ Log at Session Start

☒ Log at Session End

Log Retention: None

**Other Settings**

Schedule: None

QoS Marking: None

☐ Disable Scheduler Response Inspection

OK Cancel

B)

**Panorama Settings** ⓘ

Receive Timeout for Connection to Device (sec): 240

Send Timeout for Connection to Device (sec): 240

Retry Count for SSL Send to Device: 25

☐ Share Unused Address and Service Objects with Devices

☐ Objects defined in ancestors will take higher precedence

☐ Enable reporting and filtering on groups

When enabled Panorama will locally store users and groups from Master Policies

OK Cancel

C)

**Syslog Server Profile** ⓘ

Name: **initat(profile1)**

**Servers** Custom Log Format

NAME	SYSLOG SERVER	TRANSPORT	PORT	FORMAT	FACILITY
SyslogServer1	192.168.229.17	UDP	514	BSD	LOG_USER

Add Remove

Enter any IP address or FQDN of the Syslog server

OK Cancel

D)

**Panorama Settings** ⓘ

**Panorama Servers**

10.99.1.21

☒ Enable pushing device monitoring data to Panorama

Receive Timeout for Connection to Panorama (sec): 240

Send Timeout for Connection to Panorama (sec): 240

Retry Count for SSL Send to Panorama: 25

☒ Enable automated commit recovery

Number of attempts to check for Panorama connectivity: 1

Interval between retries (sec): 10

Disable Panorama Policy and Objects Disable Device and Network Template OK Cancel

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

D. Option D

**Answer:** C

**NEW QUESTION 112**

Which data flow describes redistribution of user mappings?

- A. User-ID agent to firewall
- B. firewall to firewall
- C. Domain Controller to User-ID agent
- D. User-ID agent to Panorama

**Answer:** B

**Explanation:**

<https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/user-id/configure-firewalls-to-redistribute-> <https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/user-id/deploy-user-id-in-a-large-scale-network/red>

**NEW QUESTION 117**

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:** C

**NEW QUESTION 122**

You have upgraded your Panorama and Log Collectors to 10.2 x. Before upgrading your firewalls using Panorama, what do you need to do?

- A. Refresh your licenses with Palo Alto Network Support - Panorama/Licenses/Retrieve License Keys from License Server.
- B. Re-associate the firewalls in Panorama/Managed Devices/Summary.
- C. Commit and Push the configurations to the firewalls.
- D. Refresh the Master Key in Panorama/Master Key and Diagnostic

**Answer:** C

**NEW QUESTION 126**

A firewall administrator wants to avoid overflowing the company syslog server with traffic logs. What should the administrator do to prevent the forwarding of DNS traffic logs to syslog?

- A. Disable logging on security rules allowing DNS.
- B. Go to the Log Forwarding profile used to forward traffic logs to syslog
- C. Then, under traffic logs match list, create a new filter with application not equal to DNS.
- D. Create a security rule to deny DNS traffic with the syslog server in the destination
- E. Go to the Log Forwarding profile used to forward traffic logs to syslog
- F. Then, under traffic logs match list, create a new filter with application equal to DNS.

**Answer:** D

**NEW QUESTION 129**

A network administrator is troubleshooting an issue with Phase 2 of an IPSec VPN tunnel. The administrator determines that the lifetime needs to be changed to match the peer.

Where should this change be made?

- A. IKE Gateway profile
- B. IPSec Crypto profile
- C. IPSec Tunnel settings
- D. IKE Crypto profile

**Answer:** C

**NEW QUESTION 134**

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:**

Reasons that sites break decryption technically include pinned certificates, client authentication, incomplete certificate chains, and unsupported ciphers.

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/decryption/decryption-exclusions/exclude-a-server>

**NEW QUESTION 135**

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 a single VLAN ID and a common virtual router. The physical Layer 3 interface would handle untagged traffic
- F. Assign each interface/subinterface to a unique zone
- G. unique zone
- H. Do not assign any interface an IP address.
- I. Create VLAN objects for each VLAN and assign VLAN interfaces matching each VLAN ID
- J. Repeat for every additional VLAN and use a VLAN ID of 0 for untagged traffic
- K. 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-interface> 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 137**

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

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

**Answer:** B

**NEW QUESTION 141**

After importing a pre-configured firewall configuration to Panorama, what step is required to ensure a commit/push is successful without duplicating local configurations?

- A. Ensure Force Template Values is checked when pushing configuration.
- B. Push the Template first, then push Device Group to the newly managed firewall.
- C. Perform the Export or push Device Config Bundle to the newly managed firewall.
- D. Push the Device Group first, then push Template to the newly managed firewall

**Answer:** C

**Explanation:**

When importing a pre-configured firewall configuration to Panorama, you need to perform the following steps 12:

- Add the serial number of the firewall under Panorama > Managed Devices
- In Panorama, import the firewall's configuration bundle under Panorama > Setup > Operations > Import device configuration to Panorama
- Commit the changes you made to Panorama
- Perform an Export or push Device Config Bundle operation under Panorama > Setup > Operations

The Export or push Device Config Bundle operation allows you to push a complete configuration bundle from Panorama to a managed firewall without duplicating local configurations<sup>3</sup>. This operation ensures that any local settings on the firewall are preserved and merged with the settings from Panorama.

**NEW QUESTION 146**

Which source is the most reliable for collecting User-ID user mapping?

- A. GlobalProtect
- B. Microsoft Active Directory
- C. Microsoft Exchange
- D. Syslog Listener

**Answer:** A

**Explanation:**

User-ID is a feature that enables you to identify and control users on your network based on their usernames instead of their IP addresses<sup>1</sup>. User mapping is the process of mapping IP addresses to usernames using various sources of information<sup>1</sup>.

The most reliable source for collecting User-ID user mapping is GlobalProtect<sup>2</sup>. GlobalProtect is a solution that provides secure access to your network and resources from anywhere. GlobalProtect agents on endpoints send user mapping information directly to the firewall or Panorama, which eliminates the need for probing other sources<sup>2</sup>. GlobalProtect also supports dynamic IP address changes and roaming users<sup>2</sup>.

**NEW QUESTION 147**

An administrator analyzes the following portion of a VPN system log and notices the following issue "Received local id 10 10 1 4/24 type IPv4 address protocol 0 port 0, received remote id 10.1.10.4/24 type IPv4 address protocol 0 port 0."  
What is the cause of the issue?

- A. IPSec crypto profile mismatch
- B. IPSec protocol mismatch
- C. mismatched Proxy-IDs
- D. bad local and peer identification IP addresses in the IKE gateway

**Answer:** C

#### NEW QUESTION 149

An administrator creates an application-based security policy rule and commits the change to the firewall. Which two methods should be used to identify the dependent applications for the respective rule? (Choose two.)

- A. Use the show predefined xpath <value> command and review the output.
- B. Review the App Dependency application list from the Commit Status view.
- C. Open the security policy rule and review the Depends On application list.
- D. Reference another application group containing similar applications.

**Answer:** AB

#### NEW QUESTION 154

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

- A. 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
- B. Create a zone protection profile with flood protection configured to defend an entire egress zone against SY
- C. ICMP ICMPv6, UD
- D. and other IP flood attacks
- E. Add a WildFire subscription to activate DoS and zone protection features
- F. Replace the hardware firewall because DoS and zone protection are not available with VM-Series systems

**Answer:** A

#### Explanation:

\* 1 <https://docs.paloaltonetworks.com/best-practices/8-1/dos-and-zone-protection-best-practices/dos-and-zone-prote>

\* 2 <https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/zone-protection-and-dos-protection/zone-defense/ta>

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/zone-protection-and-dos-protection.html>

#### NEW QUESTION 157

An engineer is tasked with configuring SSL forward proxy for traffic going to external sites. Which of the following statements is consistent with SSL decryption best practices?

- A. The forward trust certificate should not be stored on an HSM.
- B. The forward untrust certificate should be signed by a certificate authority that is trusted by the clients.
- C. Check both the Forward Trust and Forward Untrust boxes when adding a certificate for use with SSL decryption
- D. The forward untrust certificate should not be signed by a Trusted Root CA

**Answer:** B

#### Explanation:

According to the PCNSE Study Guide<sup>1</sup>, SSL forward proxy is a feature that allows the firewall to decrypt and inspect SSL traffic going to external sites. The firewall acts as a proxy between the client and the server, generating a certificate on the fly for each site.

The best practices for configuring SSL forward proxy are<sup>23</sup>:

- Use a forward trust certificate that is signed by a certificate authority (CA) that is trusted by the clients This certificate is used to sign certificates for sites that have valid certificates from trusted CAs. The clients will not see any certificate errors if they trust the forward trust certificate.
- Use a forward untrust certificate that is not signed by a trusted CA. This certificate is used to sign certificates for sites that have invalid or untrusted certificates. The clients will see certificate errors if they do not trust the forward untrust certificate. This helps alert users of potential risks and prevent man-in-the-middle attacks.
- Do not store the forward trust or untrust certificates on an HSM (hardware security module). The HSM does not support on-the-fly signing of certificates, which is required for SSL forward proxy.

#### NEW QUESTION 162

An administrator device-group commit push is tailing due to a new URL category How should the administrator correct this issue?

- A. verify that the URL seed Tile has been downloaded and activated on the firewall
- B. change the new category action to alert" and push the configuration again
- C. update the Firewall Apps and Threat version to match the version of Panorama
- D. ensure that the firewall can communicate with the URL cloud

**Answer:** C

#### Explanation:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PNqw>

#### NEW QUESTION 167

The Aggregate Ethernet interface is showing down on a passive PA-7050 firewall of an active/passive HA pair. The HA Passive Link State is set to "Auto" under

Device > High Availability > General > Active/Passive Settings. The AE interface is configured with LACP enabled and is up only on the active firewall. Why is the AE interface showing down on the passive firewall?

- A. It does not perform pre-negotiation LACP unless "Enable in HA Passive State" is selected under the High Availability Options on the LACP tab of the AE Interface.
- B. It does not participate in LACP negotiation unless Fast Failover is selected under the Enable LACP selection on the LACP tab of the AE Interface.
- C. It participates in LACP negotiation when Fast is selected for Transmission Rate under the Enable LACP selection on the LACP tab of the AE Interface.
- D. It performs pre-negotiation of LACP when the mode Passive is selected under the Enable LACP selection on the LACP tab of the AE Interface.

**Answer:** A

#### **NEW QUESTION 172**

The firewall identifies a popular application as an unKnown-tcp.  
Which two options are available to identify the application? (Choose two.)

- A. Create a custom application.
- B. Submit an App-ID request to Palo Alto Networks.
- C. Create a custom object for the application server.
- D. Create a Security policy to identify the custom application.

**Answer:** AB

#### **NEW QUESTION 175**

.....

## Thank You for Trying Our Product

\* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

\* One year free update

You can enjoy free update one year. 24x7 online support.

\* Trusted by Millions

We currently serve more than 30,000,000 customers.

\* Shop Securely

All transactions are protected by VeriSign!

**100% Pass Your PCNSE Exam with Our Prep Materials Via below:**

<https://www.certleader.com/PCNSE-dumps.html>