

# Paloalto-Networks

## Exam Questions PCNSE

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



### NEW QUESTION 1

- (Exam Topic 2)

Which option is part of the content inspection process?

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

**Answer:** B

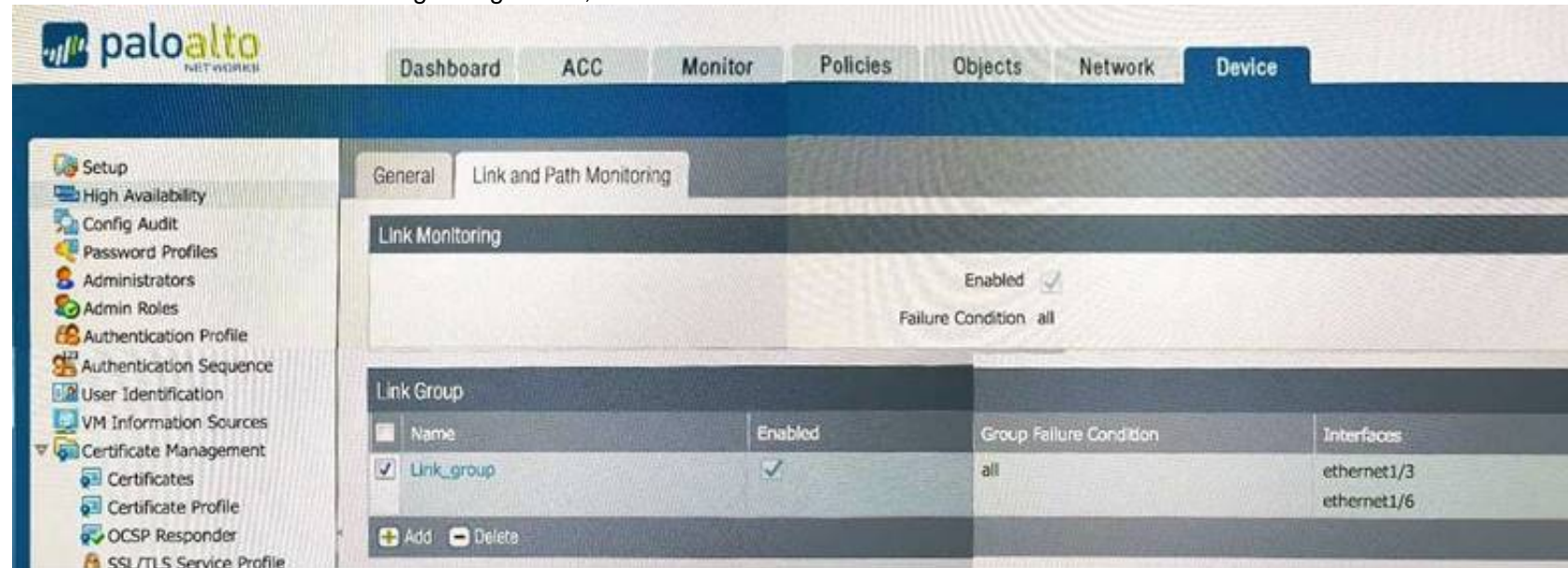
#### Explanation:

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

### NEW QUESTION 2

- (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 3

- (Exam Topic 2)

How can a candidate or running configuration be copied to a host external from Panorama?

- A. Commit a running configuration.
- B. Save a configuration snapshot.
- C. Save a candidate configuration.
- D. Export a named configuration snapshot.

**Answer:** D

#### Explanation:

Reference:

[https://www.paloaltonetworks.com/documentation/71/panorama/panorama\\_adminguide/administer-panorama/ba-panorama-and-firewall-configurations](https://www.paloaltonetworks.com/documentation/71/panorama/panorama_adminguide/administer-panorama/ba-panorama-and-firewall-configurations)

### NEW QUESTION 4

- (Exam Topic 2)

Refer to the exhibit.

```
#####
admin@Lab33-111-PA-3060(active)>show routing fib

id      destination      nexthop      flags      interface      mtu
-----
47      0.0.0.0/0          10.46.40.1   ug         ethernet1/3     1500
46      10.46.40.0/23      0.0.0.0      u          ethernet1/3     1500
45      10.46.41.111/32    0.0.0.0      uh         ethernet1/3     1500
70      10.46.41.113/32    10.46.40.1   ug         ethernet1/3     1500
51      192.168.111.0/24   0.0.0.0      u          ethernet1/6     1500
50      192.168.111.2/32   0.0.0.0      uh         ethernet1/6     1500
```

```
#####

admin@Lab33-111-PA-3060(active)>show virtual-wire all

total virtual-wire shown:
flags:  m-multicast firewalling
        p= link state pass-through
        s- vlan sub-interface
        i- ip+vlan sub-interface
        t-tenant sub-interface
```

name	interface1	interface2	flags	allowed-tags
VW-1	ethernet1/7	ethernet1/5	p	

```
#####
```

Which will be the egress interface if the traffic's ingress interface is ethernet 1/7 sourcing from 192.168.111.3 and to the destination 10.46.41.113?

- A. ethernet1/6
- B. ethernet1/3
- C. ethernet1/7
- D. ethernet1/5

**Answer:** D

#### NEW QUESTION 5

- (Exam Topic 2)

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

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

**Answer:** A

#### NEW QUESTION 6

- (Exam Topic 2)

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

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

**Answer:** D

#### NEW QUESTION 7

- (Exam Topic 2)

An administrator sees several inbound sessions identified as unknown-tcp in the traffic logs. The administrator determines that these sessions are from external users accessing the company's proprietary accounting application. The administrator wants to reliably identify this as their accounting application and to scan this traffic for threats. Which option would achieve this result?

- A. Create an Application Override policy and a custom threat signature for the application
- B. Create an Application Override policy
- C. Create a custom App-ID and use the "ordered conditions" check box
- D. Create a custom App ID and enable scanning on the advanced tab

**Answer:** D

**NEW QUESTION 8**

- (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 9**

- (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 10**

- (Exam Topic 2)

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

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

**Answer:** A

**NEW QUESTION 10**

- (Exam Topic 2)

What is the purpose of the firewall decryption broker?

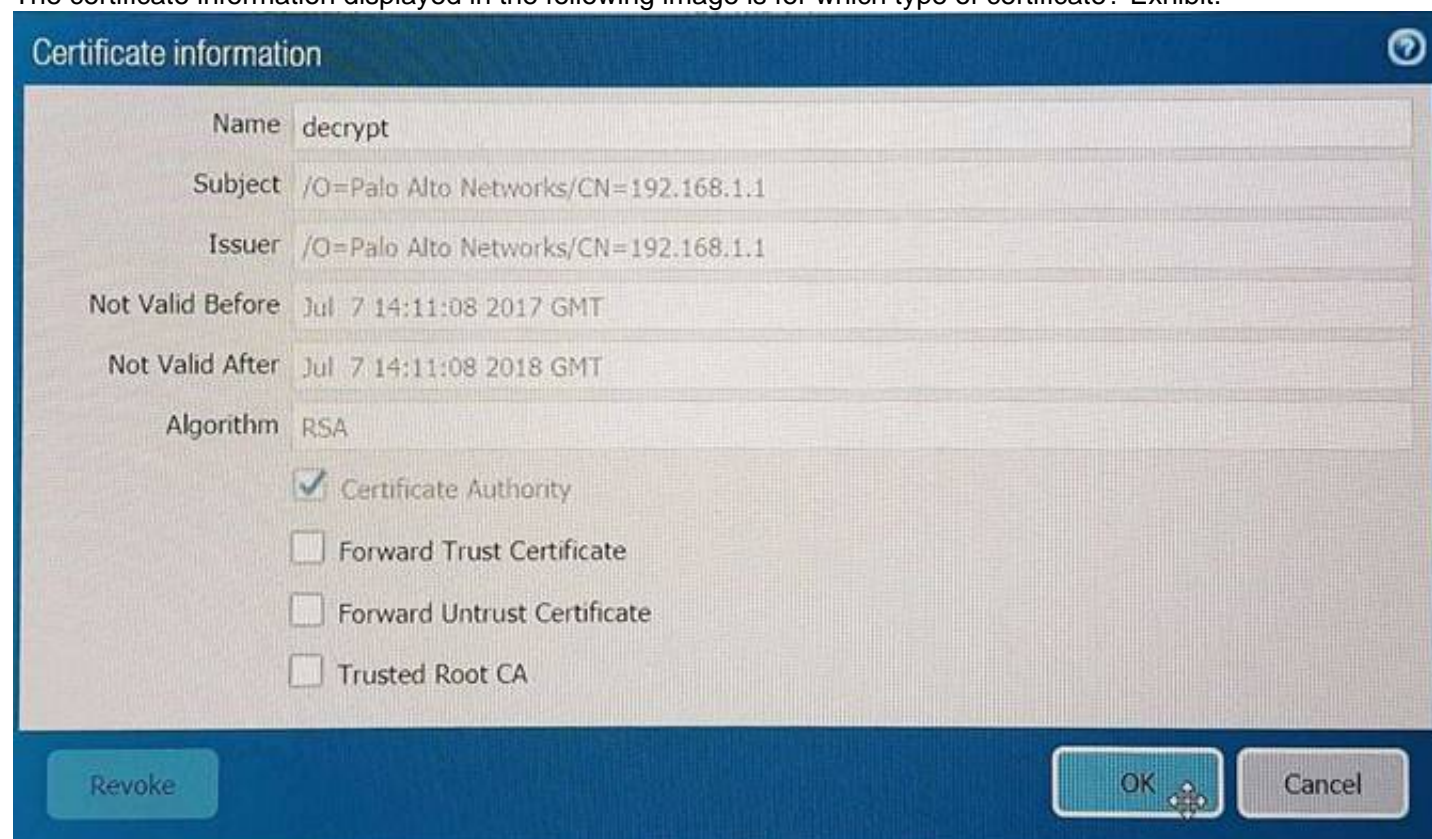
- A. Decrypt SSL traffic a then send it as cleartext to a security chain of inspection tools
- B. Force decryption of previously unknown cipher suites
- C. Inspection traffic within IPsec tunnel
- D. Reduce SSL traffic to a weaker cipher before sending it to a security chain of inspection tools

**Answer:** A

**NEW QUESTION 11**

- (Exam Topic 2)

The certificate information displayed in the following image is for which type of certificate? Exhibit:



- A. Forward Trust certificate



- B. Self-Signed Root CA certificate
- C. Web Server certificate
- D. Public CA signed certificate

**Answer:** B

#### NEW QUESTION 13

- (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 17

- (Exam Topic 2)

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

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

**Answer:** D

#### NEW QUESTION 22

- (Exam Topic 2)

When is the content inspection performed in the packet flow process?

- A. after the application has been identified
- B. before session lookup
- C. before the packet forwarding process
- D. after the SSL Proxy re-encrypts the packet

**Answer:** A

#### Explanation:

Reference:

<https://live.paloaltonetworks.com/t5/Learning-Articles/Packet-Flow-Sequence-in-PAN-OS/ta-p/56081>

#### NEW QUESTION 26

- (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 31

- (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 33

- (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 35

- (Exam Topic 2)

Which processing order will be enabled when a Panorama administrator selects the setting “Objects defined in ancestors will take higher precedence?”

- A. Descendant objects will take precedence over other descendant objects.
- B. Descendant objects will take precedence over ancestor objects.
- C. Ancestor objects will have precedence over descendant objects.
- D. Ancestor objects will have precedence over other ancestor objects.

**Answer:** C

#### Explanation:

Reference:

<https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/device/device-setup-manageme>

### NEW QUESTION 38

- (Exam Topic 2)

An administrator needs to upgrade an NGFW to the most current version of PAN-OS® software. The following is occurring:

- Firewall has Internet connectivity through e1/1.
- Default security rules and security rules allowing all SSL and web-browsing traffic to and from any zone.
- Service route is configured, sourcing update traffic from e1/1.
- A communication error appears in the System logs when updates are performed.
- Download does not complete.

What must be configured to enable the firewall to download the current version of PAN-OS software?

- A. DNS settings for the firewall to use for resolution
- B. scheduler for timed downloads of PAN-OS software
- C. static route pointing application PaloAlto-updates to the update servers
- D. Security policy rule allowing PaloAlto-updates as the application

**Answer:** D

### NEW QUESTION 42

- (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 44

- (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 47

- (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 50

- (Exam Topic 2)

Where can an administrator see both the management plane and data plane CPU utilization in the WebUI?

- A. System log
- B. CPU Utilization widget
- C. Resources widget
- D. System Utilization log

**Answer:** C

**Explanation:**

System Resources (widget) Displays the Management CPU usage, Data Plane usage, and the Session Count (the number of sessions established through the firewall or

Panorama). <https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-web-interface-help/dashboard/dashboard-widg>

#### NEW QUESTION 52

- (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 57

- (Exam Topic 2)

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

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

**Answer:** AB

#### NEW QUESTION 61

- (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 62

- (Exam Topic 2)

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

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

**Answer:** AC

**Explanation:**

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

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

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

**NEW QUESTION 67**

- (Exam Topic 2)

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

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

**Answer:** B

**Explanation:**

Reference:

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

**NEW QUESTION 70**

- (Exam Topic 2)

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

- A. Client Probing
- B. Port mapping
- C. Server monitoring
- D. Syslog listening

**Answer:** D

**Explanation:**

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

**NEW QUESTION 74**

- (Exam Topic 2)

Which feature can provide NGFWs with User-ID mapping information?

- A. GlobalProtect
- B. Web Captcha
- C. Native 802.1q authentication
- D. Native 802.1x authentication

**Answer:** A

**NEW QUESTION 75**

- (Exam Topic 2)

Which User-ID method maps IP addresses to usernames for users connecting through an 802.1x-enabled wireless network device that has no native integration with PAN-OS® software?

- A. XML API
- B. Port Mapping
- C. Client Probing
- D. Server Monitoring

**Answer:** A

**Explanation:**

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/user-id/user-id-concepts/user-mapping/xml-api.html>

**NEW QUESTION 79**

- (Exam Topic 1)



An administrator needs to gather information about the CPU utilization on both the management plane and the data plane  
Where does the administrator view the desired data?

- A. Monitor > Utilization
- B. Resources Widget on the Dashboard
- C. Support > Resources
- D. Application Command and Control Center

Answer: A

**NEW QUESTION 84**

- (Exam Topic 1)

An administrator wants to enable zone protection Before doing so, what must the administrator consider?

- A. Activate a zone protection subscription.
- B. To increase bandwidth no more than one firewall interface should be connected to a zone
- C. Security policy rules do not prevent lateral movement of traffic between zones
- D. The zone protection profile will apply to all interfaces within that zone

Answer: A

**NEW QUESTION 88**

- (Exam Topic 1)

A variable name must start with which symbol?

- A. \$
- B. &
- C. !
- D. #

Answer: A

**Explanation:**

<https://docs.paloaltonetworks.com/panorama/8-1/panorama-admin/manage-firewalls/manage-templates-and-tem>

**NEW QUESTION 91**

- (Exam Topic 1)

Match each GlobalProtect component to the purpose of that component

	Answer Area	
GlobalProtect Gateway	<input type="text"/>	management functions for GlobalProtect infrastructure
GlobalProtect clientless	<input type="text"/>	security enforcement for traffic from GlobalProtect apps
GlobalProtect Portal	<input type="text"/>	software on endpoints that enables access to network resources
GlobalProtect app	<input type="text"/>	secure remote access to common enterprise web applications
	<input type="text"/>	

- A. Mastered
- B. Not Mastered

Answer: A

**Explanation:**

The GlobalProtect portal provides the management functions for your GlobalProtect infrastructure The GlobalProtect gateways provide security enforcement for traffic from GlobalProtect apps  
The GlobalProtect app software runs on endpoints and enables access to your network resources

**NEW QUESTION 94**

- (Exam Topic 1)

In SSL Forward Proxy decryption, which two certificates can be used for certificate signing? (Choose two.)

- A. wildcard server certificate
- B. enterprise CA certificate
- C. client certificate
- D. server certificate
- E. self-signed CA certificate

Answer: BE

#### NEW QUESTION 98

- (Exam Topic 1)

An internal system is not functioning The firewall administrator has determined that the incorrect egress interface is being used After looking at the configuration, the administrator believes that the firewall is not using a static route  
What are two reasons why the firewall might not use a static route"? (Choose two.)

- A. no install on the route
- B. duplicate static route
- C. path monitoring on the static route
- D. disabling of the static route

**Answer:** C

#### NEW QUESTION 102

- (Exam Topic 1)

During SSL decryption which three factors affect resource consumption1? (Choose three )

- A. TLS protocol version
- B. transaction size
- C. key exchange algorithm
- D. applications that use non-standard ports
- E. certificate issuer

**Answer:** ABC

#### Explanation:

<https://docs.paloaltonetworks.com/best-practices/8-1/decryption-best-practices/decryption-best-practices/plan-ss>

#### NEW QUESTION 105

- (Exam Topic 1)

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

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

**Answer:** B

#### NEW QUESTION 107

- (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 OSFP 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 109

- (Exam Topic 1)

What does SSL decryption require to establish a firewall as a trusted third party and to establish trust between a client and server to secure an SSL/TLS connection?

- A. link state
- B. stateful firewall connection
- C. certificates
- D. profiles

**Answer:** C

#### Explanation:

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/decryption/decryption-overview.html#:~:text=SSL>

#### NEW QUESTION 114

- (Exam Topic 1)

What are two characteristic types that can be defined for a variable? (Choose two )

- A. zone

- B. FQDN
- C. path group
- D. IP netmask

**Answer:** BD

**Explanation:**

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface-help/panorama-web-interface/panorama-tem>

**NEW QUESTION 118**

- (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 120**

- (Exam Topic 1)

The SSL Forward Proxy decryption policy is configured. The following four certificate authority (CA) certificates are installed on the firewall.

An end-user visits the untrusted website <https://www.firewall-do-not-trust-website.com>

<input type="checkbox"/>	NAME	SUBJECT	ISSUER	CA	KEY	EXPIRES	STATUS	ALGO...
<input type="checkbox"/>	Forward-Trust-Certificate	CN = Forward-Trust-Certificate	CN = Forward-Trust-Certificate	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Feb 10 02:48:4...	valid	RSA
<input type="checkbox"/>	Forward-Untrust-Certificate	CN = Forward-Untrust-Certificate	CN = Forward-Untrust-Certificate	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Feb 10 02:49:0...	valid	RSA
<input type="checkbox"/>	Firewall-CA	CN = Firewall-CA	CN = Firewall-CA	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Feb 10 02:55:2...	valid	RSA
<input type="checkbox"/>	Firewall-Trusted-Root-CA	CN = Firewall-Trusted-Root-CA	CN = Firewall-Trusted-Root-CA	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Feb 10 02:56:4...	valid	RSA

Which certificate authority (CA) certificate will be used to sign the untrusted webserver certificate?

- A. Forward-Untrust-Certificate
- B. Forward-Trust-Certificate
- C. Firewall-CA
- D. Firewall-Trusted-Root-CA

**Answer:** B

**NEW QUESTION 123**

- (Exam Topic 1)

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

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

**Answer:** ADE

**NEW QUESTION 127**

- (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 128**

- (Exam Topic 1)

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

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

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

**Answer:** C

#### NEW QUESTION 129

- (Exam Topic 1)

As a best practice, which URL category should you target first for SSL decryption\*?

- A. Online Storage and Backup
- B. High Risk
- C. Health and Medicine
- D. Financial Services

**Answer:** A

#### NEW QUESTION 130

- (Exam Topic 1)

Which three statements accurately describe Decryption Mirror? (Choose three.)

- A. Decryption Mirror requires a tap interface on the firewall
- B. Decryption, storage, inspection and use of SSL traffic are regulated in certain countries
- C. Only management consent is required to use the Decryption Mirror feature
- D. You should consult with your corporate counsel before activating and using Decryption Mirror in a production environment
- E. Use of Decryption Mirror might enable malicious users with administrative access to the firewall to harvest sensitive information that is submitted via an encrypted channel

**Answer:** ABC

#### NEW QUESTION 131

- (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 134

- (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 139

- (Exam Topic 2)

Which two actions would be part of an automatic solution that would block sites with untrusted certificates without enabling SSL Forward Proxy? (Choose two.)

- A. Create a no-decrypt Decryption Policy rule.
- B. Configure an EDL to pull IP addresses of known sites resolved from a CRL.
- C. Create a Dynamic Address Group for untrusted sites
- D. Create a Security Policy rule with vulnerability Security Profile attached.
- E. Enable the "Block sessions with untrusted issuers" setting.

**Answer:** DE

#### NEW QUESTION 142

- (Exam Topic 2)

An administrator needs to optimize traffic to prefer business-critical applications over non-critical applications. QoS natively integrates with which feature to provide service quality?

- A. Port Inspection
- B. Certificate revocation



- C. Content-ID
- D. App-ID

**Answer:** D

**Explanation:**

Reference:  
<https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/quality-of-service/qos-for-applications-and>

**NEW QUESTION 143**

- (Exam Topic 2)

Which option describes the operation of the automatic commit recovery feature?

- A. It enables a firewall to revert to the previous configuration if rule shadowing is detected
- B. It enables a firewall to revert to the previous configuration if a commit causes Panorama connectivity failure.
- C. It enables a firewall to revert to the previous configuration if application dependency errors are found
- D. It enables a firewall to revert to the previous configuration if a commit causes HA partner connectivity failure

**Answer:** A

**NEW QUESTION 147**

- (Exam Topic 2)

An administrator has been asked to configure a Palo Alto Networks NGFW to provide protection against external hosts attempting to exploit a flaw in an operating system on an internal system.

Which Security Profile type will prevent this attack?

- A. Vulnerability Protection
- B. Anti-Spyware
- C. URL Filtering
- D. Antivirus

**Answer:** A

**Explanation:**

Reference:  
<https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/objects/objects-security-profile-vulnerability-protection>

**NEW QUESTION 148**

- (Exam Topic 2)

Based on the image, what caused the commit warning?

The screenshot shows the Palo Alto Networks web interface. The 'Device' tab is selected, and the 'Device Certificates' sub-tab is active. A table lists two certificates: 'FWDtrust' and 'FWD-UnTrust'. Both are valid and have RSA keys. The 'FWDtrust' certificate expires on Jun 29 02:02:05 2020 GMT, and the 'FWD-UnTrust' certificate expires on Jun 29 02:06:36 2019 GMT. Below the table, a 'Commit Status' dialog box is open. It shows the operation 'Commit' is 'Completed' with a 'Successful' result. The details state 'Configuration committed successfully'. A warning is displayed: 'Warning: cannot find complete certificate chain for certificate FWDtrust (Module: device)'. The warning is highlighted with an orange box.

Name	Subject	Issuer	CA	Key	Expires	Status	AI...	Usage
FWDtrust	CN=FWDtrust	DC = local, DC = lab, CN = lab-SRV2016-LABCA-CA	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Jun 29 02:02:05 2020 GMT	valid	RSA	Forward Trust Certificate
FWD-UnTrust	CN = FWD-UnTrust	CN = FWD-UnTrust	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Jun 29 02:06:36 2019 GMT	valid	RSA	Forward Trust Certificate

**Commit Status**

**Operation** Commit

**Status** Completed

**Result** Successful

**Details** Configuration committed successfully

**Warnings** Warning: cannot find complete certificate chain for certificate FWDtrust (Module: device)

Cancel Close

- A. The CA certificate for FWDtrust has not been imported into the firewall.
- B. The FWDtrust certificate has not been flagged as Trusted Root CA.
- C. SSL Forward Proxy requires a public certificate to be imported into the firewall.
- D. The FWDtrust certificate does not have a certificate chain.

**Answer:** D

#### NEW QUESTION 150

- (Exam Topic 2)

A web server is hosted in the DMZ and the server is configured to listen for incoming connections on TCP

port 443. A Security policies rules allowing access from the Trust zone to the DMZ zone needs to be configured to allow web-browsing access. The web server hosts its contents over HTTP(S). Traffic from Trust to DMZ is being decrypted with a Forward Proxy rule.

Which combination of service and application, and order of Security policy rules, needs to be configured to allow cleartext web- browsing traffic to this server on tcp/443.

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

**Answer:** B

#### Explanation:

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

#### NEW QUESTION 155

- (Exam Topic 3)

Which three fields can be included in a pcap filter? (Choose three)

- A. Egress interface
- B. Source IP
- C. Rule number
- D. Destination IP
- E. Ingress interface

**Answer:** BCD

#### Explanation:

(<https://live.paloaltonetworks.com/t5/Featured-Articles/Getting-Started-Packet-Capture/ta-p/72069>)

#### NEW QUESTION 158

- (Exam Topic 3)

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

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

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

**Answer:** BD

#### NEW QUESTION 160

- (Exam Topic 3)

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

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

**Answer:** C

#### NEW QUESTION 165

- (Exam Topic 3)

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

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

**Answer:** AD

#### NEW QUESTION 169

- (Exam Topic 3)

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

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

**Answer:** B

#### NEW QUESTION 172

- (Exam Topic 3)

Which two logs on the firewall will contain authentication-related information useful for troubleshooting purpose (Choose two)

- A. ms.log
- B. traffic.log
- C. system.log
- D. dp-monitor.log
- E. authd.log

**Answer:** CE

#### NEW QUESTION 173

- (Exam Topic 3)

Support for which authentication method was added in PAN-OS 8.0?

- A. RADIUS
- B. LDAP
- C. Diameter
- D. TACACS+

**Answer:** D

#### Explanation:

<https://www.paloaltonetworks.com/resources/datasheets/whats-new-in-pan-os-7-1>

#### NEW QUESTION 178

- (Exam Topic 3)

A file sharing application is being permitted and no one knows what this application is used for. How should this application be blocked?

- A. Block all unauthorized applications using a security policy
- B. Block all known internal custom applications
- C. Create a WildFire Analysis Profile that blocks Layer 4 and Layer 7 attacks
- D. Create a File blocking profile that blocks Layer 4 and Layer 7 attacks

**Answer:** D

#### NEW QUESTION 182

- (Exam Topic 3)

Which command can be used to validate a Captive Portal policy?

- A. eval captive-portal policy <criteria>
- B. request cp-policy-eval <criteria>
- C. test cp-policy-match <criteria>
- D. debug cp-policy <criteria>

**Answer:** C

#### NEW QUESTION 187

- (Exam Topic 3)

Which authentication source requires the installation of Palo Alto Networks software, other than PAN-OS 7x, to obtain a username-to-IP-address mapping?

- A. Microsoft Active Directory
- B. Microsoft Terminal Services
- C. Aerohive Wireless Access Point
- D. Palo Alto Networks Captive Portal

**Answer:** B

#### NEW QUESTION 191

- (Exam Topic 3)

Which client software can be used to connect remote Linux client into a Palo Alto Networks Infrastructure without sacrificing the ability to scan traffic and protect against threats?

- A. X-Auth IPsec VPN
- B. GlobalProtect Apple IOS

- C. GlobalProtect SSL
- D. GlobalProtect Linux

**Answer:** A

**Explanation:**

( <http://blog.webernetz.net/2014/03/31/palo-alto-globalprotect-for-linux-with-vpnc/> )

**NEW QUESTION 194**

- (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)

Site-A and Site-B have a site-to-site VPN set up between them. OSPF is configured to dynamically create the routes between the sites. The OSPF configuration in Site-A is configured properly, but the route for the tunnel is not being established. The Site-B interfaces in the graphic are using a broadcast Link Type. The administrator has determined that the OSPF configuration in Site-B is using the wrong Link Type for one of its interfaces.

Virtual Router - OSPF - Area						
Area ID		0.0.0.0				
Type	Range	Interface		Virtual Link		
<input type="checkbox"/>	Interface	Enable	Passive	Link Type	Metric	Priority
<input type="checkbox"/>	tunnel.10	<input checked="" type="checkbox"/>	<input type="checkbox"/>	broadcast	10	1
<input type="checkbox"/>	ethernet1/21	<input checked="" type="checkbox"/>	<input type="checkbox"/>	broadcast	10	1

Which Link Type setting will correct the error?

- A. Set tunne
- B. 1 to p2p
- C. Set tunne
- D. 1 to p2mp
- E. Set Ethernet 1/1 to p2mp
- F. Set Ethernet 1/1 to p2p

**Answer:** A

**NEW QUESTION 200**

- (Exam Topic 3)

A firewall administrator has been asked to configure a Palo Alto Networks NGFW to prevent against compromised hosts trying to phone-home or beacon out to external command-and-control (C2) servers.

Which security Profile type will prevent these behaviors?

- A. WildFire
- B. Anti-Spyware
- C. Vulnerability Protection
- D. Antivirus

**Answer:** D

**NEW QUESTION 202**

- (Exam Topic 3)

Which two statements are correct for the out-of-box configuration for Palo Alto Networks NGFWs? (Choose two)

- A. The devices are pre-configured with a virtual wire pair out the first two interfaces.
- B. The devices are licensed and ready for deployment.
- C. The management interface has an IP address of 192.168.1.1 and allows SSH and HTTPS connections.
- D. A default bidirectional rule is configured that allows Untrust zone traffic to go to the Trust zone.
- E. The interface are pingable.

**Answer:** BC

**NEW QUESTION 203**

- (Exam Topic 3)

The IT department has received complaints about VoIP call jitter when the sales staff is making or receiving calls. QoS is enabled on all firewall interfaces, but there



is no QoS policy written in the rulebase. The IT manager wants to find out what traffic is causing the jitter in real time when a user reports the jitter. Which feature can be used to identify, in real time, the applications taking up the most bandwidth?

- A. QoS Statistics
- B. Applications Report
- C. Application Command Center (ACC)
- D. QoS Log

**Answer:** A

#### NEW QUESTION 205

- (Exam Topic 3)

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

Which CLI command will help identify the issue?

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

**Answer:** C

#### NEW QUESTION 207

- (Exam Topic 3)

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

Rule2 allows youtube-base

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

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

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

**Answer:** C

#### NEW QUESTION 211

- (Exam Topic 3)

An Administrator is configuring an IPSec VPN to a Cisco ASA at the administrator's home and experiencing issues completing the connection. The following is the output from the command:

less mp-log ikemgr.log:

```
less mp-log ikemgr.log:
```

```
2014-08-05 03:51:41 [INFO]: IPsec-SA request for 108.81.64.59 queued since no phase1 found
2014-08-05 03:51:41 [PROTO_NOTIFY]: <====> PHASE-1 NEGOTIATION STARTED AS INITIATOR, MAIN MODE <====
====> Initiated SA: 69.15.96.53[500]-108.81.64.59[500] cookie:09e85260f28f4e15:0000000000000000 <====
2014-08-05 03:52:33 [PROTO_NOTIFY]: <====> PHASE-1 NEGOTIATION FAILED AS INITIATOR, MAIN MODE <====
====> Failed SA: 69.15.96.53[500]-108.81.64.59[500] cookie:09e85260f28f4e15:0000000000000000 <==== Due to
timeout.
2014-08-05 03:52:33 [INFO]: <====> PHASE-1 SA DELETED <====
====> Deleted SA: 69.15.96.53[500]-108.81.64.59[500] cookie:09e85260f28f4e15:0000000000000000 <====
2014-08-05 03:53:02 [INFO]: IPsec-SA request for 108.81.64.59 queued since no phase1 found
2014-08-05 03:53:02 [PROTO_NOTIFY]: <====> PHASE-1 NEGOTIATION STARTED AS INITIATOR, MAIN MODE <====
====> Initiated SA: 69.15.96.53[500]-108.81.64.59[500] cookie:53351420a9a1aa47:0000000000000000 <====
2014-08-05 03:53:54 [PROTO_NOTIFY]: <====> PHASE-1 NEGOTIATION FAILED AS INITIATOR, MAIN MODE <====
====> Failed SA: 69.15.96.53[500]-108.81.64.59[500] cookie:53351420a9a1aa47:0000000000000000 <==== Due to
timeout.
2014-08-05 03:53:54 [INFO]: <====> PHASE-1 SA DELETED <====
```

What could be the cause of this problem?

- A. The public IP addresses do not match for both the Palo Alto Networks Firewall and the ASA.
- B. The Proxy IDs on the Palo Alto Networks Firewall do not match the settings on the ASA.
- C. The shared secrets do not match between the Palo Alto firewall and the ASA
- D. The dead peer detection settings do not match between the Palo Alto Networks Firewall and the ASA

**Answer:** B

#### NEW QUESTION 216

- (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 221

- (Exam Topic 3)

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

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

**Answer:** B

#### NEW QUESTION 222

- (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 224

- (Exam Topic 3)

In an enterprise deployment, a network security engineer wants to assign to a group of administrators without creating local administrator accounts on the firewall. Which authentication method must be used?

- A. LDAP
- B. Kerberos
- C. Certification based authentication
- D. RADIUS with Vendor-Specific Attributes

**Answer:** D

#### NEW QUESTION 226

- (Exam Topic 3)

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

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

**Answer:** D

#### NEW QUESTION 228

- (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 233

- (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 238

- (Exam Topic 3)

Several offices are connected with VPNs using static IPv4 routes. An administrator has been tasked with implementing OSPF to replace static routing. Which step is required to accomplish this goal?

- A. Assign an IP address on each tunnel interface at each site
- B. Enable OSPFv3 on each tunnel interface and use Area ID 0.0.0.0
- C. Assign OSPF Area ID 0.0.0.0 to all Ethernet and tunnel interfaces
- D. Create new VPN zones at each site to terminate each VPN connection

**Answer:** C

#### NEW QUESTION 239

- (Exam Topic 3)

What can missing SSL packets when performing a packet capture on dataplane interfaces?

- A. The packets are hardware offloaded to the offloaded processor on the dataplane
- B. The missing packets are offloaded to the management plane CPU
- C. The packets are not captured because they are encrypted
- D. There is a hardware problem with offloading FPGA on the management plane

**Answer:** A

#### NEW QUESTION 243

- (Exam Topic 3)

A company has a web server behind a Palo Alto Networks next-generation firewall that it wants to make accessible to the public at 1.1.1.1. The company has decided to configure a destination NAT Policy rule.

Given the following zone information:

- DMZ zone: DMZ-L3
- Public zone: Untrust-L3
- Guest zone: Guest-L3
- Web server zone: Trust-L3
- Public IP address (Untrust-L3): 1.1.1.1
- Private IP address (Trust-L3): 192.168.1.50

What should be configured as the destination zone on the Original Packet tab of NAT Policy rule?

- A. Untrust-L3
- B. DMZ-L3
- C. Guest-L3
- D. Trust-L3

**Answer:** A

#### NEW QUESTION 247

- (Exam Topic 3)

An administrator is configuring an IPSec VPN to a Cisco ASA at the administrator's home and experiencing issues completing the connection. the following is the output from the command:

```
less mp-log ikemgr.log:

2014-08-05 03:51:41 [INFO]: IPsec-SA request for 108.81.64.59 queued since no phase1 found
2014-08-05 03:51:41 [PROTO_NOTIFY]: <====> PHASE-1 NEGOTIATION STARTED AS INITIATOR, MAIN MODE <====>
<====> Initiated SA: 69.15.96.53[500]-108.81.64.59[500] cookie:09e85260f22f4e15:0000000000000000 <====>
2014-08-05 03:52:33 [PROTO_NOTIFY]: <====> PHASE-1 NEGOTIATION FAILED AS INITIATOR, MAIN MODE <====>
<====> Failed SA: 69.15.96.53[500]-108.81.64.59[500] cookie:09e85260f22f4e15:0000000000000000 <====> Due to
timeout.
2014-08-05 03:52:33 [INFO]: <====> PHASE-1 SA DELETED <====>
<====> Deleted SA: 69.15.96.53[500]-108.81.64.59[500] cookie:09e85260f22f4e15:0000000000000000 <====>
2014-08-05 03:53:02 [INFO]: IPsec-SA request for 108.81.64.59 queued since no phase1 found
2014-08-05 03:53:02 [PROTO_NOTIFY]: <====> PHASE-1 NEGOTIATION STARTED AS INITIATOR, MAIN MODE <====>
<====> Initiated SA: 69.15.96.53[500]-108.81.64.59[500] cookie:33351420a9a1aa47:0000000000000000 <====>
2014-08-05 03:53:54 [PROTO_NOTIFY]: <====> PHASE-1 NEGOTIATION FAILED AS INITIATOR, MAIN MODE <====>
<====> Failed SA: 69.15.96.53[500]-108.81.64.59[500] cookie:33351420a9a1aa47:0000000000000000 <====> Due to
timeout.
2014-08-05 03:53:54 [INFO]: <====> PHASE-1 SA DELETED <====>
```

What could be the cause of this problem?

- A. The dead peer detection settings do not match between the Palo Alto Networks Firewall and the ASA.
- B. The Proxy IDs on the Palo Alto Networks Firewall do not match the setting on the ASA.
- C. The public IP addresses do not match for both the Palo Alto Networks Firewall and the ASA.
- D. The shared secrets do not match between the Palo Alto Networks Firewall and the ASA.

**Answer:** C

#### NEW QUESTION 248

- (Exam Topic 3)

How is the Forward Untrust Certificate used?

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

D. It is used for Captive Portal to identify unknown users.

**Answer:** C

#### NEW QUESTION 252

- (Exam Topic 3)

A logging infrastructure may need to handle more than 10,000 logs per second. Which two options support a dedicated log collector function? (Choose two)

- A. Panorama virtual appliance on ESX(i) only
- B. M-500
- C. M-100 with Panorama installed
- D. M-100

**Answer:** BC

#### Explanation:

(<https://live.paloaltonetworks.com/t5/Management-Articles/Panorama-Sizing-and-Design-Guide/ta-p/72181>)

#### NEW QUESTION 256

- (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 257

- (Exam Topic 3)

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

- A. Clean
- B. Benign
- 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 261

- (Exam Topic 3)

Which Security Policy Rule configuration option disables antivirus and anti-spyware scanning of server-to-client flows only?

- A. Disable Server Response Inspection
- B. Apply an Application Override
- C. Disable HIP Profile
- D. Add server IP Security Policy exception

**Answer:** A

#### NEW QUESTION 265

.....



## 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](#)**