**Braindump2go Guarantee All Exams 100% Pass
One Time!**

➤ **Vendor:** **Palo Alto Networks**

➤ **Exam Code:** **PCNSE**

➤ **Exam Name:** **Palo Alto Networks Certified Security Engineer (PCNSE)
PAN-OS 10.0**

➤ **New Updated Questions from Braindump2go**

➤ **(Updated in September/2021)**

Visit Braindump2go and Download Full Version PCNSE Exam Dumps

QUESTION 328
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

QUESTION 329
Which value in the Application column indicates UDP traffic that did not match an App-ID signature?

A. not-applicable
B. incomplete
C. unknown-ip
D. unknown-udp

Answer: D
Explanation:
To safely enable applications you must classify all traffic, across all ports, all the time. With App-ID, the only applications that are typically classified as unknown traffic--tcp, udp or non-syn-tcp--in the ACC and the Traffic logs are commercially available applications that have not yet been added to App-ID, internal or custom applications on your network, or potential threats.

QUESTION 330
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.

QUESTION 331
An organization has recently migrated its infrastructure and configuration to NGFWs, for which Panorama manages the devices.
The organization is coming from a L2-L4 firewall vendor, but wants to use App-ID while identifying policies that are no longer needed.
Which Panorama tool can help this organization?

A. Config Audit
B. Policy Optimizer
C. Application Groups
D. Test Policy Match

Answer: A

QUESTION 332
Which statement accurately describes service routes and virtual systems?

A. Virtual systems can only use one interface for all global service and service routes of the firewall
B. The interface must be used for traffic to the required external services
C. Virtual systems that do not have specific service routes configured inherit the global service and service route settings for the firewall
D. Virtual systems cannot have dedicated service routes configured: and virtual systems always use the global service and service route settings for the firewall

Answer: A

QUESTION 333
An administrator wants to upgrade a firewall HA pair to PAN-OS 10.1. The firewalls are currently running PAN-OS 8.1.17.
Which upgrade path maintains synchronization of the HA session (and prevents network outage)?

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

Answer: D

QUESTION 334
An engineer must configure a new SSL decryption deployment.
Which profile or certificate is required before any traffic that matches an SSL decryption rule is decrypted?

A. There must be a certificate with both the Forward Trust option and Forward Untrust option selected
B. A Decryption profile must be attached to the Decryption policy that the traffic matches
C. A Decryption profile must be attached to the Security policy that the traffic matches
D. There must be a certificate with only the Forward Trust option selected

Answer: A

QUESTION 335
When you import the configuration of an HA pair into Panorama, how do you prevent the import from affecting ongoing traffic?

A. Disable HA
B. Disable the HA2 link
C. Disable config sync
D. Set the passive link state to 'shutdown.-

Answer: C

QUESTION 336
Which configuration task is best for reducing load on the management plane?

A. Disable logging on the default deny rule
B. Enable session logging at start
C. Disable pre-defined reports
D. Set the URL filtering action to send alerts

Answer: A

QUESTION 337
Which Panorama objects restrict administrative access to specific device-groups?

A. templates
B. admin roles
C. access domains
D. authentication profiles

Answer: C

QUESTION 338
An administrator has 750 firewalls. The administrator's central-management Panorama instance deploys dynamic updates to the firewalls.
The administrator notices that the dynamic updates from Panorama do not appear on some of the firewalls.
If Panorama pushes the configuration of a dynamic update schedule to managed firewalls, but the configuration does not appear what is the root cause?

A. Panorama has no connection to Palo Alto Networks update servers
B. Panorama does not have valid licenses to push the dynamic updates
C. No service route is configured on the firewalls to Palo Alto Networks update servers
D. Locally-defined dynamic update settings take precedence over the settings that Panorama pushed

Answer: D

QUESTION 339
Which rule type controls end user SSL traffic to external websites?

A. SSL Outbound Proxyless Inspection
B. SSL Forward Proxy
C. SSL Inbound Inspection

D. SSH Proxy

Answer: C

QUESTION 340
Which two statements correctly identify the number of Decryption Broker security chains that are supported on a pair of decryption-forwarding interfaces? (Choose two)

A. A single transparent bridge security chain is supported per pair of interfaces
B. L3 security chains support up to 32 security chains
C. L3 security chains support up to 64 security chains
D. A single transparent bridge security chain is supported per firewall

Answer: AD

QUESTION 341
An organization is building a Bootstrap Package to deploy Palo Alto Networks VM-Series firewalls into their AWS tenant.
Which two statements are correct regarding the bootstrap package contents? (Choose two)

A. The /config /content and /software folders are mandatory while the /license and /plugin folders are optional
B. The bootstrap package is stored on an AFS share or a discrete container file bucket
C. The directory structure must include a /config /content, /software and /license folders
D. The init-cfg txt and bootstrap.xml files are both optional configuration items for the /config folder
E. The bootstrap xml file allows for automated deployment of VM-Senes firewalls with full network and policy configurations.

Answer: DE

QUESTION 342
Which action disables Zero Touch Provisioning (ZTP) functionality on a ZTP firewall during the onboarding process?

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

Answer: D

QUESTION 343
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: A

QUESTION 344
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

QUESTION 345
Use the image below If the firewall has the displayed link monitoring configuration what will cause a failover?
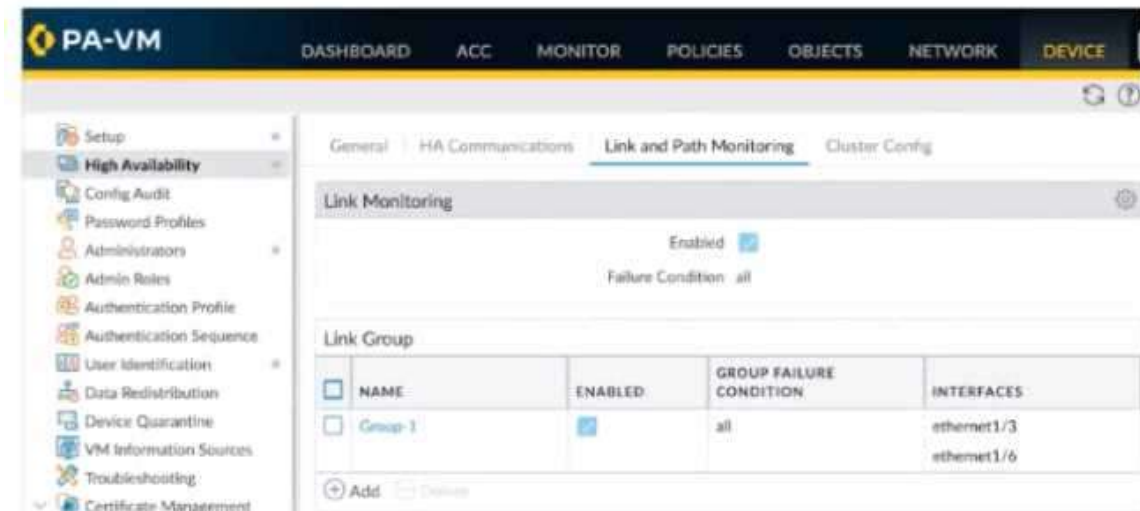
A. ethernet1/3 and ethernet1/6 going down
B. etheme!1/3 going down
C. ethernet1/6 going down
D. ethernet1/3 or ethernet1/6 going down

Answer: A

QUESTION 346
When overriding a template configuration locally on a firewall, what should you consider?

A. Only Panorama can revert the override
B. Panorama will lose visibility into the overridden configuration
C. Panorama will update the template with the overridden value
D. The firewall template will show that it is out of sync within Panorama

Answer: B

QUESTION 347
An administrator cannot see any Traffic logs from the Palo Alto Networks NGFW in Panorama reports.
The configuration problem seems to be on the firewall.
Which settings, if configured incorrectly, most likely would stop only Traffic logs from being sent from the NGFW to Panorama?

A.

Syslog Server Profile ⑦

Name SyslogProfile1

Servers   Custom Log Format

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

⊕ Add ⊖ Delete

Enter the IP address or FQDN of the Syslog server

OK   Cancel

B.

Security Policy Rule ⑦

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

Action Setting

Action Allow

☐ Send ICMP unreachable

Profile Setting

Profile Type : Profiles

Antivirus default

Vulnerability strict
Protection

Anti-Spyware strict

Log Setting

☐ Log at Session Start

☑ Log at Session End

Log Forwarding None

Other Settings

Schedule None

QoS Marking None

☐ Disable Server Response Inspection

C.

Panorama Settings ⑦

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

D.

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 Devices

[OK]   [Cancel]

Answer: D

QUESTION 348
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

QUESTION 349
The SSL Forward Proxy decryption policy is configured. The following four certificate authority (CA) certificates are installed on the firewall.

	NAME	SUBJECT	ISSUER	CA	KEY	EXPIRES	STATUS	ALGO...
☐	Forward-Trust-Certificate	CN = Forward-Trust-Certificate	CN = Forward-Trust-Certificate	✓	✓	Feb 10 02:48:4...	valid	RSA
☐	Forward-Untrust-Certificate	CN = Forward-Untrust-Certificate	CN = Forward-Untrust-Certificate	✓	✓	Feb 10 02:49:0...	valid	RSA
☐	Firewall-CA	CN = Firewall-CA	CN = Firewall-CA	✓	✓	Feb 10 02:55:2...	valid	RSA
☐	Firewall-Trusted-Root-CA	CN = Firewall-Trusted-Root-CA	CN = Firewall-Trusted-Root-CA	✓	✓	Feb 10 02:56:4...	valid	RSA

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

QUESTION 350
An engineer is planning an SSL decryption implementation.
Which of the following statements is a best practice for SSL decryption?

A. Obtain an enterprise CA-signed certificate for the Forward Trust certificate
B. Obtain a certificate from a publicly trusted root CA for the Forward Trust certificate
C. Use an enterprise CA-signed certificate for the Forward Untrust certificate
D. Use the same Forward Trust certificate on all firewalls in the network

Answer: D

QUESTION 351
When you configure an active/active high availability pair which two links can you use? (Choose two)

A. HA2 backup
B. HA3
C. Console Backup
D. HSCI-C

Answer: AC

QUESTION 352
Which CLI command displays the physical media that are connected to ethernetl/8?

A. > show system state filter-pretty sys.si.p8.stats
B. > show interface ethernetl/8
C. > show system state filter-pretty sys.sl.p8.phy
D. > show system state filter-pretty sys.si.p8.med

Answer: D

QUESTION 353
In a firewall, which three decryption methods are valid? (Choose three)

A. SSL Inbound Inspection
B. SSL Outbound Proxyless Inspection
C. SSL Inbound Proxy
D. Decryption Mirror
E. SSH Proxy

Answer: ADE

QUESTION 354
The UDP-4501 protocol-port is used between which two GlobalProtect components?

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

Answer: A

QUESTION 355
Refer to the exhibit. Which certificate can be used as the Forward Trust certificate?

A. Domain Sub-CA
B. Domain-Root-Cert
C. Certificate from Default Trusted Certificate Authorities
D. Forward-Trust

Answer: D

QUESTION 356
The following objects and policies are defined in a device group hierarchy
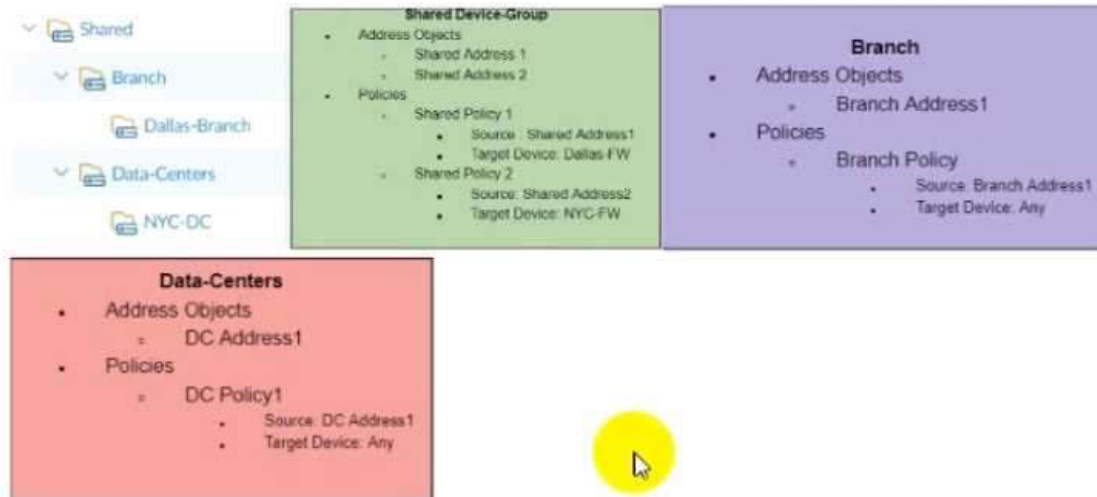
Dallas-Branch has **Dallas-FW** as a member of the **Dallas-Branch device-group**
NYC-DC has **NYC-FW** as a member of the **NYC-DC device-group**
What objects and policies will the **Dallas-FW** receive if "Share Unused Address and Service Objects" is enabled in Panorama?

A.

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

C. **Address Objects**
-Shared Address 1
-Branch Address 2
Policies
-Shared Polic1
-Branch Policy1

D. **Address Objects**
-Shared Address1
-Shared Address2
-Branch Address1
Policies
-Shared Policy1
-Shared Policy2
-Branch Policy1

Answer: A