- **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)**

QUESTION 357
A company needs to preconfigure firewalls to be sent to remote sites with the least amount of preconfiguration. Once deployed each firewall must establish secure tunnels back to multiple regional data centers to include the future regional data centers.
Which VPN preconfigured configuration would adapt to changes when deployed to the future site?

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

Answer: C

QUESTION 358
PBF can address which two scenarios? (Select Two)

A. forwarding all traffic by using source port 78249 to a specific egress interface
B. providing application connectivity the primary circuit fails
C. enabling the firewall to bypass Layer 7 inspection
D. routing FTP to a backup ISP link to save bandwidth on the primary ISP link

Answer: AC

QUESTION 359
In a security-first network what is the recommended threshold value for content updates to be dynamically updated?

A. 1 to 4 hours
B. 6 to 12 hours
C. 24 hours
D. 36 hours

Answer: B

QUESTION 360
A firewall is configured with SSL Forward Proxy decryption and has the following four enterprise certificate authorities (Cas):
i. 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)
ii. Enterpnse-Untrusted-CA, which is verified as Forward Untrust Certificate
iii. Enterprise-Intermediate-CA
iv. Enterprise-Root-CA which is verified only as Trusted Root CA An end-user visits https //www example-website com/ with a server certificate Common Name (CN) www example-website com
The firewall does the SSL Forward Proxy decryption for the website and the server certificate is not trusted by the firewall.
The end-user's browser will show that the certificate for www example-website com was issued by which of the following?

A. Enterprise-Untrusted-CA which is a self-signed CA
B. Enterprise-Trusted-CA which is a self-signed CA
C. Enterprise-Intermediate-CA which was. in turn, issued by Enterprise-Root-CA
D. Enterprise-Root-CA which is a self-signed CA

Answer: B

QUESTION 361
An administrator plans to deploy 15 firewalls to act as GlobalProtect gateways around the world Panorama will manage the firewalls.
The firewalls will provide access to mobile users and act as edge locations to on-premises Infrastructure.
The administrator wants to scale the configuration out quickly and wants all of the firewalls to use the same template configuration.
Which two solutions can the administrator use to scale this configuration? (Choose two.)

A. variables
B. template stacks
C. collector groups
D. virtual systems

Answer: BC

QUESTION 362
A traffic log might list an application as "not-applicable" for which two reasons? (Choose two)

A. 0The firewall did not install the session
B. The TCP connection terminated without identifying any application data
C. The firewall dropped a TCP SYN packet
D. There was not enough application data after the TCP connection was established

Answer: AD

QUESTION 363
An administrator is considering upgrading the Palo Alto Networks NGFW and central management Panorama version.
What is considered best practice for this scenario?

A. Perform the Panorama and firewall upgrades simultaneously
B. Upgrade the firewall first wait at least 24 hours and then upgrade the Panorama version
C. Upgrade Panorama to a version at or above the target firewall version
D. Export the device state perform the update, and then import the device state

Answer: A

QUESTION 364

An administrator needs to implement an NGFW between their DMZ and Core network EIGRP Routing between the two environments is required.
Which interface type would support this business requirement?

A. Layer 3 interfaces but configuring EIGRP on the attached virtual router
B. Virtual Wire interfaces to permit EIGRP routing to remain between the Core and DMZ
C. Layer 3 or Aggregate Ethernet interfaces but configuring EIGRP on subinterfaces only
D. Tunnel interfaces to terminate EIGRP routing on an IPsec tunnel (with the GlobalProtect License to support LSVPN and EIGRP protocols)

Answer: D

QUESTION 365
When you configure a Layer 3 interface what is one mandatory step?

A. Configure Security profiles, which need to be attached to each Layer 3 interface
B. Configure Interface Management profiles which need to be attached to each Layer 3 interface
C. Configure virtual routers to route the traffic for each Layer 3 interface
D. Configure service routes to route the traffic for each Layer 3 interface

Answer: A

QUESTION 366
An administrator has a PA-820 firewall with an active Threat Prevention subscription.
The administrator is considering adding a WildFire subscription.
How does adding the WildFire subscription improve the security posture of the organization1?

A. Protection against unknown malware can be provided in near real-time
B. WildFire and Threat Prevention combine to provide the utmost security posture for the firewall
C. After 24 hours WildFire signatures are included in the antivirus update
D. WildFire and Threat Prevention combine to minimize the attack surface

Answer: D

QUESTION 367
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

QUESTION 368
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

QUESTION 369
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

QUESTION 370
What are two characteristic types that can be defined for a variable? (Choose two)

A. zone
B. FQDN
C. path group
D. IP netmask

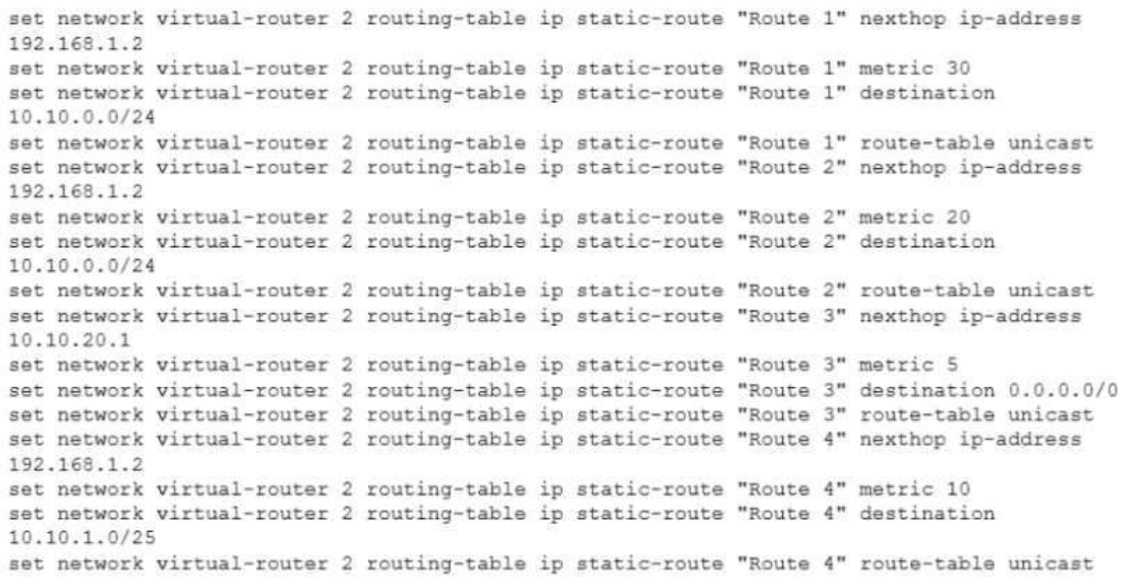
Answer: BD

QUESTION 371
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

QUESTION 372
Given the following configuration, which route is used for destination 10.10.0.4?



```
set network virtual-router 2 routing-table ip static-route "Route 1" nexthop ip-address
192.168.1.2
set network virtual-router 2 routing-table ip static-route "Route 1" metric 30
set network virtual-router 2 routing-table ip static-route "Route 1" destination
10.10.0.0/24
set network virtual-router 2 routing-table ip static-route "Route 1" route-table unicast
set network virtual-router 2 routing-table ip static-route "Route 2" nexthop ip-address
192.168.1.2
set network virtual-router 2 routing-table ip static-route "Route 2" metric 20
set network virtual-router 2 routing-table ip static-route "Route 2" destination
10.10.0.0/24
set network virtual-router 2 routing-table ip static-route "Route 2" route-table unicast
set network virtual-router 2 routing-table ip static-route "Route 3" nexthop ip-address
10.10.20.1
set network virtual-router 2 routing-table ip static-route "Route 3" metric 5
set network virtual-router 2 routing-table ip static-route "Route 3" destination 0.0.0.0/0
set network virtual-router 2 routing-table ip static-route "Route 3" route-table unicast
set network virtual-router 2 routing-table ip static-route "Route 4" nexthop ip-address
192.168.1.2
set network virtual-router 2 routing-table ip static-route "Route 4" metric 10
set network virtual-router 2 routing-table ip static-route "Route 4" destination
10.10.1.0/25
set network virtual-router 2 routing-table ip static-route "Route 4" route-table unicast
```

A. Route 4
B. Route 3
C. Route 1
D. Route 3

Answer: A

QUESTION 373
When an in-band data port is set up to provide access to required services, what is required for an interface that is assigned to service routes?

A. The interface must be used for traffic to the required services
B. You must enable DoS and zone protection
C. You must set the interface to Layer 2 Layer 3. or virtual wire
D. You must use a static IP address

Answer: A

QUESTION 374
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

QUESTION 375
When setting up a security profile which three items can you use? (Choose three)

A. Wildfire analysis
B. anti-ransom ware

C. antivirus
D. URL filtering
E. decryption profile

Answer: ACD

QUESTION 376
A variable name must start with which symbol?

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

Answer: A

QUESTION 377
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

QUESTION 378
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

QUESTION 379
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

QUESTION 380
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

QUESTION 381
Before you upgrade a Palo Alto Networks NGFW what must you do?

A. Make sure that the PAN-OS support contract is valid for at least another year
B. Export a device state of the firewall
C. Make sure that the firewall is running a version of antivirus software and a version of WildFire that support the licensed subscriptions.
D. Make sure that the firewall is running a supported version of the app + threat update

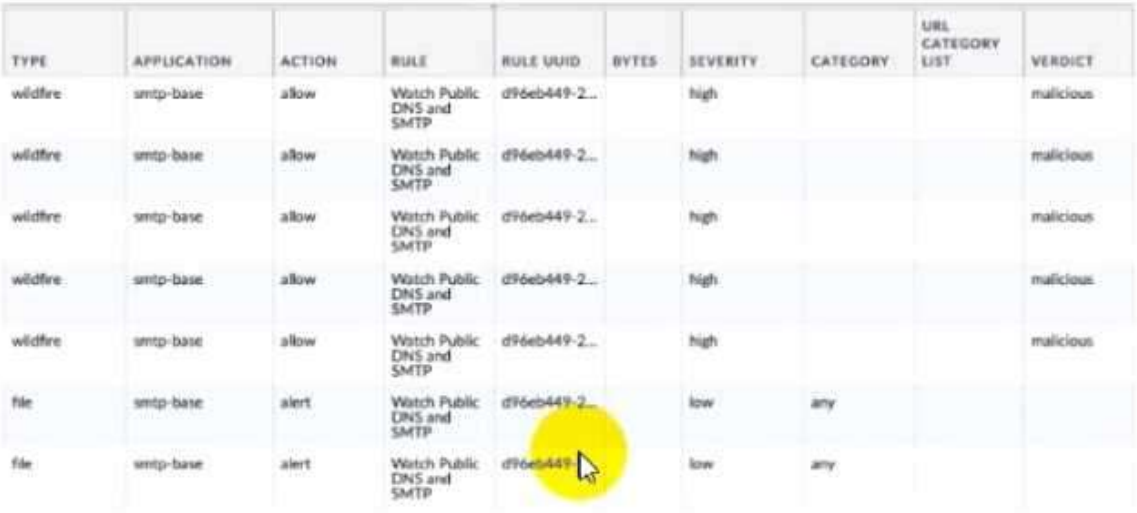
Answer: B

QUESTION 382
Which User-ID mapping method should be used in a high-security environment where all IP address-to-user mappings should always be explicitly known?

A. PAN-OS integrated User-ID agent
B. LDAP Server Profile configuration
C. GlobalProtect
D. Windows-based User-ID agent

Answer: A

QUESTION 383
Given the following snippet of a WildFire submission log. did the end-user get access to the requested information and why or why not?



TYPE	APPLICATION	ACTION	RULE	RULE UUID	BYTES	SEVERITY	CATEGORY	URL CATEGORY LIST	VERDICT
wildfire	smtp-base	allow	Watch Public DNS and SMTP	d96eb449-2...		high			malicious
wildfire	smtp-base	allow	Watch Public DNS and SMTP	d96eb449-2...		high			malicious
wildfire	smtp-base	allow	Watch Public DNS and SMTP	d96eb449-2...		high			malicious
wildfire	smtp-base	allow	Watch Public DNS and SMTP	d96eb449-2...		high			malicious
wildfire	smtp-base	allow	Watch Public DNS and SMTP	d96eb449-2...		high			malicious
file	smtp-base	alert	Watch Public DNS and SMTP	d96eb449-2...		low	any		
file	smtp-base	alert	Watch Public DNS and SMTP	d96eb449-		low	any		

A. Yes. because the action is set to "allow "
B. No because WildFire categorized a file with the verdict "malicious"
C. Yes because the action is set to "alert"

D. No because WildFire classified the seventy as "high."

Answer: B

QUESTION 384
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