- **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/2022)**

QUESTION 511
A company requires that a specific set of ciphers be used when remotely managing their Palo Alto Networks appliances. Which profile should be configured in order to achieve this?

A. SSH Service profile
B. SSL/TLS Service profile
C. Decryption profile
D. Certificate profile

Answer: A

QUESTION 512
A company is using wireless controllers to authenticate users. Which source should be used for User- ID mappings?

A. Syslog
B. XFF headers
C. server monitoring
D. client probing

Answer: A

QUESTION 513
An engineer is configuring SSL Inbound Inspection for public access to a company's application. Which certificate(s) need to be installed on the firewall to ensure that inspection is performed successfully?

A. Self-signed CA and End-entity certificate
B. Root CA and Intermediate CA(s)
C. Self-signed certificate with exportable private key
D. Intermediate CA (s) and End-entity certificate

Answer: D

QUESTION 514
A firewall administrator needs to be able to inspect inbound HTTPS traffic on servers hosted in their DMZ to prevent the hosted service from being exploited. Which combination of features can allow PAN-OS to detect exploit traffic in a session with TLS encapsulation?

A. Decryption policy and a Data Filtering profile
B. a WildFire profile and a File Blocking profile
C. Vulnerability Protection profile and a Decryption policy
D. a Vulnerability Protection profile and a QoS policy

Answer: C

QUESTION 515
Which two statements correctly describe Session 380280? (Choose two.)

A. The session went through SSL decryption processing.
B. The session has ended with the end-reason unknown.
C. The application has been identified as web-browsing.
D. The session did not go through SSL decryption processing.

Answer: AC

QUESTION 516
While analyzing the Traffic log, you see that some entries show "unknown-tcp" in the Application column What best explains these occurrences?

A. A handshake took place, but no data packets were sent prior to the timeout.

B. A handshake took place; however, there were not enough packets to identify the application.
C. A handshake did take place, but the application could not be identified.
D. A handshake did not take place, and the application could not be identified.

Answer: C

QUESTION 517
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. In the OSFP configuration, ensure that the correct redistribution profile is selected in the OSPF Export Rules section.
B. Within the redistribution profile ensure that Redist is selected.
C. Ensure that the OSPF neighbor state Is "2-Way."
D. In the redistribution profile check that the source type is set to "ospf."

Answer: AB

QUESTION 518
Which statement best describes the Automated Commit Recovery feature?

A. It performs a connectivity check between the firewall and Panorama after every configuration commit on the firewall. It reverts the configuration changes on the firewall if the check fails.
B. It restores the running configuration on a firewall and Panorama if the last configuration commit fails.
C. It performs a connectivity check between the firewall and Panorama after every configuration commit on the firewall. It reverts the configuration changes on the firewall and on Panorama if the check fails.
D. It restores the running configuration on a firewall if the last configuration commit fails.

Answer: A

QUESTION 519
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. Then, under traffic logs match list, create a new filter with application not equal to DNS.
C. Create a security rule to deny DNS traffic with the syslog server in the destination
D. Go to the Log Forwarding profile used to forward traffic logs to syslog. Then, under traffic logs match list, create a new filter with application equal to DNS.

Answer: D

QUESTION 520
An engineer is planning an SSL decryption implementation Which of the following statements is a best practice for SSL decryption?

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

Answer: C

QUESTION 521
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. certificate revocation
B. Content-ID
C. App-ID
D. port inspection

Answer: C

QUESTION 522
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

QUESTION 523
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

QUESTION 524
During the implementation of SSL Forward Proxy decryption, an administrator imports the company's Enterprise Root CA and Intermediate CA certificates onto the firewall. The company's Root and Intermediate CA certificates are also distributed to trusted devices using Group Policy and GlobalProtect. Additional device certificates and/or Subordinate certificates requiring an Enterprise CA chain of trust are signed by the company's Intermediate CA. Which method should the administrator use when creating Forward Trust and Forward Untrust certificates on the firewall for use with decryption?

A. Generate a single subordinate CA certificate for both Forward Trust and Forward Untrust.
B. Generate a CA certificate for Forward Trust and a self-signed CA for Forward Untrust.
C. Generate a single self-signed CA certificate for Forward Trust and another for Forward Untrust
D. Generate two subordinate CA certificates, one for Forward Trust and one for Forward Untrust.

Answer: B

QUESTION 525
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

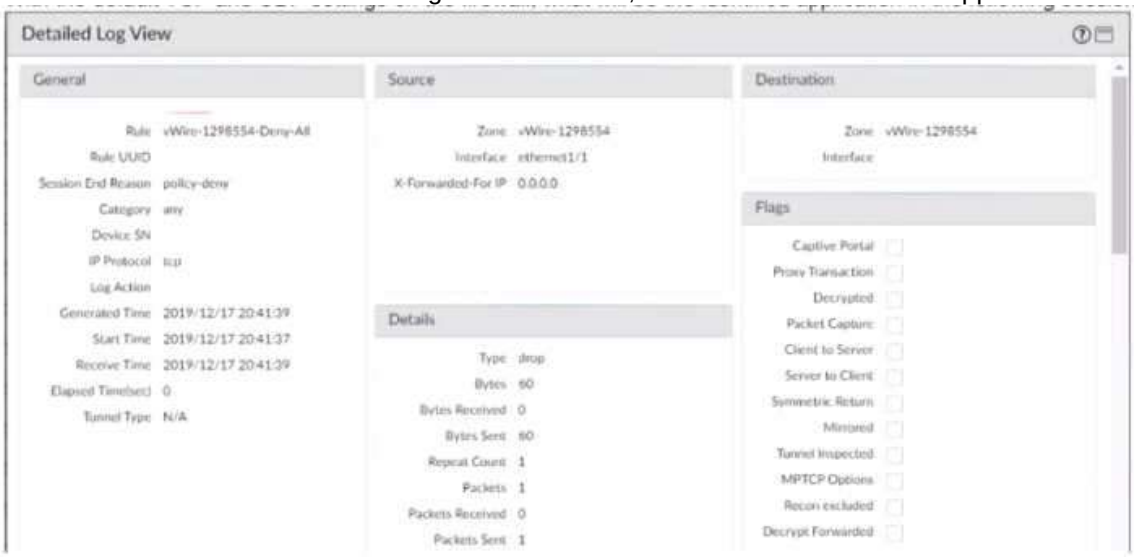
Answer: B

QUESTION 526
An administrator has configured a pair of firewalls using high availability in Active/Passive mode. Path Monitoring has been enabled with a Failure Condition of "any." A path group is configured with Failure Condition of "all" and contains a destination IP of 8.8.8.8 and 4.2.2.2 with a Ping Interval of 500ms and a Ping count of 3.
Which scenario will cause the Active firewall to fail over?

A. IP address 8.8.8.8 is unreachable for 1 second.
B. IP addresses 8.8.8.8 and 4.2.2.2 are unreachable for 1 second.
C. IP addresses 8.8.8.8 and 4.2.2.2 are unreachable for 2 seconds
D. IP address 4.2.2.2 is unreachable for 2 seconds.

Answer: C

QUESTION 527
With the default TCP and UDP settings on the firewall, what will be the identified application in the following session?



A. Incomplete
B. unknown-tcp
C. Insufficient-data
D. not-applicable

Answer: A

QUESTION 528
Which profile generates a packet threat type found in threat logs?

A. Zone Protection
B. WildFire
C. Anti-Spyware

D. Antivirus

Answer: C

QUESTION 529
A client wants to detect the use of weak and manufacturer-default passwords for loT devices. Which option will help the customer?

A. Configure a Data Filtering profile with alert mode.
B. Configure an Antivirus profile with alert mode.
C. Configure a Vulnerability Protection profile with alert mode
D. Configure an Anti-Spyware profile with alert mode.

Answer: C

QUESTION 530
A firewall administrator notices that many Host Sweep scan attacks are being allowed through the firewall sourced from the outside zone. What should the firewall administrator do to mitigate this type of attack?

A. Create a DOS Protection profile with SYN Flood protection enabled and apply it to all rules allowing traffic from the outside zone
B. Enable packet buffer protection in the outside zone.
C. Create a Security rule to deny all ICMP traffic from the outside zone.
D. Create a Zone Protection profile, enable reconnaissance protection, set action to Block, and apply it to the outside zone.

Answer: D

QUESTION 531
An engineer needs to permit XML API access to a firewall for automation on a network segment that is routed through a Layer 3 subinterface on a Palo Alto Networks firewall. However, this network segment cannot access the dedicated management interface due to the Security policy. Without changing the existing access to the management interface, how can the engineer fulfill this request?

A. Specify the subinterface as a management interface in Setup > Device > Interfaces.
B. Enable HTTPS in an Interface Management profile on the subinterface.
C. Add the network segment's IP range to the Permitted IP Addresses list
D. Configure a service route for HTTP to use the subinterface

Answer: B

QUESTION 532
An engineer needs to see how many existing SSL decryption sessions are traversing a firewall What command should be used?

A. show dataplane pool statistics I match proxy
B. debug dataplane pool statistics I match proxy
C. debug sessions I match proxy
D. show sessions all

Answer: B

QUESTION 533
Which steps should an engineer take to forward system logs to email?

A. Create a new email profile under Device > server profiles; then navigate to Objects > Log

Forwarding profile > set log type to system and the add email profile.

B. Enable log forwarding under the email profile in the Objects tab.
C. Create a new email profile under Device > server profiles: then navigate to Device > Log Settings > System and add the email profile under email.
D. Enable log forwarding under the email profile in the Device tab.

Answer: C

QUESTION 534
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

QUESTION 535
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

Answer: C

QUESTION 536
Which Panorama feature protects logs against data loss if a Panorama server fails?

A. Panorama HA automatically ensures that no logs are lost if a server fails inside the HA Cluster.
B. Panorama Collector Group with Log Redundancy ensures that no logs are lost if a server fails inside the Collector Group.
C. Panorama HA with Log Redundancy ensures that no logs are lost if a server fails inside the HA Cluster.
D. Panorama Collector Group automatically ensures that no logs are lost if a server fails inside the Collector Group

Answer: A

QUESTION 537
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 troubleshool 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

QUESTION 538
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. GlobalProtect
C. Windows-based User-ID agent
D. LDAP Server Profile configuration

Answer: B

QUESTION 539
What can be used to create dynamic address groups?

A. dynamic address
B. region objects
C. tags
D. FODN addresses

Answer: C

QUESTION 540
A firewall administrator has been tasked with ensuring that all Panorama configuration is committed and pushed to the devices at the end of the day at a certain time. How can they achieve this?

A. Use the Scheduled Config Export to schedule Commit to Panorama and also Push to Devices.
B. Use the Scheduled Config Push to schedule Push lo Devices and separately schedule an API call to commit all Panorama changes.
C. Use the Scheduled Config Export to schedule Push to Devices and separately schedule an API call to commit all Panorama changes.
D. Use the Scheduled Config Push taschedule Commit to Panorama and also Push to Devices.

Answer: D