

Palo Alto Networks PCNSE7 Exam

Volume: 96 Questions

Question: 1

Which three function are found on the dataplane of a PA-5050? (Choose three)

- A. Protocol Decoder
- B. Dynamic routing
- C. Management
- D. Network Processing
- E. Signature Match

Answer: B,D,E

Question: 2

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

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

Answer: B

Question: 3

A critical US-CERT notification is published regarding a newly discovered botnet. The malware is very evasive and is not reliably detected by endpoint antivirus software.

Furthermore, SSL is used to tunnel malicious traffic to command-and-control servers on the internet and SSL Forward Proxy Decryption is not enabled.

Which component once enabled on a perimeter firewall will allow the identification of existing infected hosts in an environment?

- A. Anti-Spyware profiles applied outbound security policies with DNS Query action set to

Palo Alto Networks PCNSE7 Exam

sinkhole

- B. File Blocking profiles applied to outbound security policies with action set to alert
- C. Vulnerability Protection profiles applied to outbound security policies with action set to block
- D. Antivirus profiles applied to outbound security policies with action set to alert

Answer: A

Question: 4

Support for which authentication method was added in PAN-OS 7.0?

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

Answer: D

Question: 5

A network security engineer has a requirement to allow an external server to access an internal web server. The internal web server must also initiate connections with the external server. What can be done to simplify the NAT policy?

- A. Configure ECMP to handle matching NAT traffic
- B. Configure a NAT Policy rule with Dynamic IP and Port
- C. Create a new Source NAT Policy rule that matches the existing traffic and enable the Bidirectional option
- D. Create a new Destination NAT Policy rule that matches the existing traffic and enable the Bi-directional option

Answer: C

Palo Alto Networks PCNSE7 Exam

Question: 6

What are three valid method of user mapping? (Choose three)

- A. Syslog
- B. XML API
- C. 802.1X
- D. WildFire
- E. Server Monitoring

Answer: A,B,E

Question: 7

Which three log-forwarding destinations require a server profile to be configured? (Choose three)

- A. SNMP Trap
- B. Email
- C. RADIUS
- D. Kerberos
- E. Panorama
- F. Syslog

Answer: A,B,F

Question: 8

A company has a policy that denies all applications it classifies as bad and permits only application it classifies as good. The firewall administrator created the following security policy on the company's firewall.

Which interface configuration will accept specific VLAN IDs?

Which two benefits are gained from having both rule 2 and rule 3 presents? (choose two)

Palo Alto Networks PCNSE7 Exam

	Name	Source			Destination		Application	Service	Action	Profile	Options
		Zone	Address	User	Zone	Address					
1	rule1	Trust-L3	any	any	UnTrust-L3	any	Known Good	application-default	allow	none	
2	rule2	Trust-L3	any	any	UnTrust-L3	any	Known Bad	any	deny	none	
3	rule3	Trust-L3	any	any	UnTrust-L3	any	any	any	deny	none	

- A. A report can be created that identifies unclassified traffic on the network.
- B. Different security profiles can be applied to traffic matching rules 2 and 3.
- C. Rule 2 and 3 apply to traffic on different ports.
- D. Separate Log Forwarding profiles can be applied to rules 2 and 3.

Answer: B,D

Question: 9

Which option is an IPv6 routing protocol?

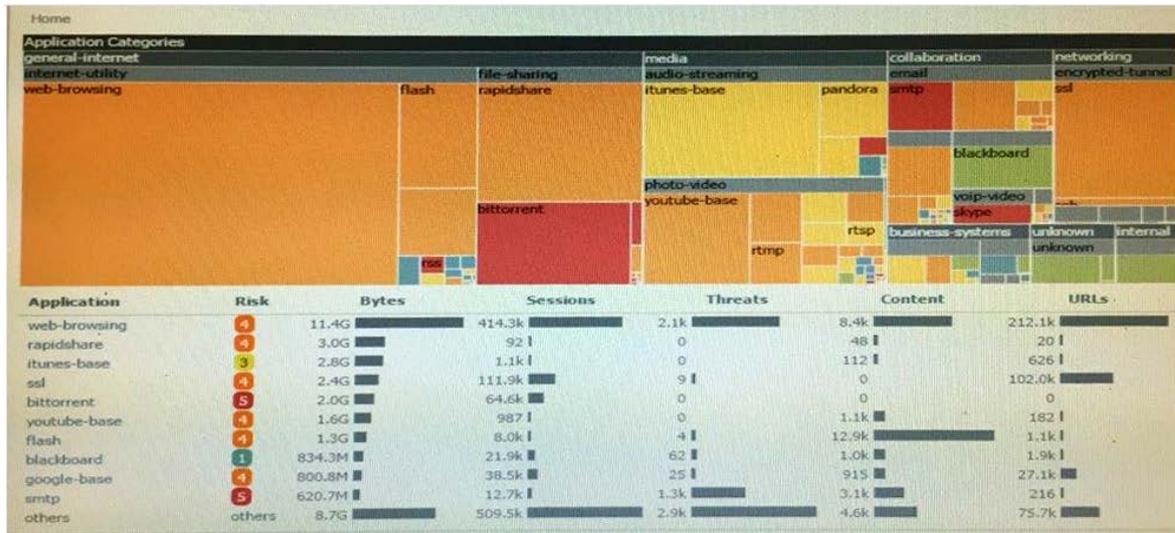
- A. RIPv3
- B. OSPFv3
- C. OSPv3
- D. BGP NG

Answer: B

Question: 10

Click the Exhibit button

Palo Alto Networks PCNSE7 Exam



An administrator has noticed a large increase in bittorrent activity. The administrator wants to determine where the traffic is going on the company.

What would be the administrator's next step?

- A. Right-Click on the bittorrent link and select Value from the context menu
- B. Create a global filter for bittorrent traffic and then view Traffic logs.
- C. Create local filter for bittorrent traffic and then view Traffic logs.
- D. Click on the bittorrent application link to view network activity

Answer: D

Question: 11

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

Palo Alto Networks PCNSE7 Exam

Question: 12

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

Question: 13

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: B,C

Question: 14

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

Palo Alto Networks PCNSE7 Exam

Question: 15

Which interface configuration will accept specific VLAN IDs?

- A. Tab Mode
- B. Subinterface
- C. Access Interface
- D. Trunk Interface

Answer: B

Question: 16

When is it necessary to activate a license when provisioning a new Palo Alto Networks firewall?

- A. When configuring Certificate Profiles
- B. When configuring GlobalProtect portal
- C. When configuring User Activity Reports
- D. When configuring Antivirus Dynamic Updates

Answer: D

Question: 17

A VPN connection is set up between Site-A and Site-B, but no traffic is passing in the system log of Site-A, there is an event logged as like-nego-p1-fail-psk.

What action will bring the VPN up and allow traffic to start passing between the sites?

- A. Change the Site-B IKE Gateway profile version to match Site-A,
- B. Change the Site-A IKE Gateway profile exchange mode to aggressive mode.
- C. Enable NAT Traversal on the Site-A IKE Gateway profile.
- D. Change the pre-shared key of Site-B to match the pre-shared key of Site-A

Answer: D

Palo Alto Networks PCNSE7 Exam

Question: 18

Click the Exhibition Button Below.

The screenshot shows two configuration windows. The top window, titled 'Exhibit Window', displays a table of Policy-Based Forwarding (PBF) rules. The bottom window displays a 'Forwarding' table.

		Source			Destination		
	Name	Tags	Zone/Interface	Address	User	Address	Application
1	PBF1	none	Trust-L3	192.168.10.0/24	any	172.16.10.0/24	any
2	PBF2	none	Trust-L3	192.168.10.0/24	any	172.16.10.0/24	any
3	PBF3	none	Trust-L3	192.168.10.0/24	Will	172.16.10.0/24	any

Forwarding				
Service	Action	Egress I/F	Next Hop	Enforce Symmetric Return
any	forward	ethernet1/2.2	172.20.20.1	false
service-http	forward	ethernet1/3.2	172.20.30.1	false
service-https	forward	ethernet1/3.3	172.20.40.1	false

A firewall has three PBF rules and a default route with a next hop of 172.20.10.1 that is configured in the default VR. A user named Will has a PC with a 192.168.10.10 IP address. He makes an HTTPS connection to 172.16.10.20.

Which is the next hop IP address for the HTTPS traffic from Will's PC?

- A. 172.20.30.1
- B. 172.20.40.1
- C. 172.20.20.1
- D. 172.20.10.1

Answer: B

Question: 19

A network design calls for a "router on a stick" implementation with a PA-5060 performing inter-VLAN routing. All VLAN-tagged traffic will be forwarded to the PA-5060 through a single dot1q trunk interface.

Which interface type and configuration setting will support this design?

- A. Trunk interface type with specified tag
- B. Layer 3 interface type with specified tag

Palo Alto Networks PCNSE7 Exam

C. Layer 2 interface type with a VLAN assigned

D. Layer 3 subinterface type with specified tag

Answer: D

Question: 20

How can a Palo Alto Networks firewall be configured to send syslog messages in a format compatible with non-standard syslog servers?

A. Enable support for non-standard syslog messages under device management

B. Check the custom-format check box in the syslog server profile

C. Select a non-standard syslog server profile

D. Create a custom log format under the syslog server profile

Answer: D

Question: 21

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

Question: 22

A network security engineer needs to configure a virtual router using IPv6 addresses. Which two routing options support these addresses? (Choose two)

A. BGP not sure

B. OSPFv3

Palo Alto Networks PCNSE7 Exam

C. RIP

D. Static Route

Answer: B,D

Question: 23

Which two methods can be used to mitigate resource exhaustion of an application server?
(Choose two)

A. Vulnerability Object

B. DoS Protection Profile

C. Data Filtering Profile

D. Zone Protection Profile

Answer: B,D

Question: 24

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

Question: 25

Company.com has an in-house application that the Palo Alto Networks device doesn't identify correctly. A Threat Management Team member has mentioned that this in-house application is very sensitive and all traffic being identified needs to be inspected by the Content-ID engine.