Palo Alto Networks Certified Network Security Engineer

1. Topic #: 1
Given the following snippet of a WildFire submission log, did the end user successfully download a file?

A. A. Yes, because the final action is set to “allow.”

B. B. No, because the action for the wildfire-virus is “reset-both.”

C. C. No, because the URL generated an alert.

D. D. Yes, because both the web-browsing application and the flash file have the “alert” action.

Answer(s): B

---

2. Question #: 586
Topic #: 1
A firewall engineer is managing a Palo Alto Networks NGFW which is not in line of any DHCP traffic.

A. Which interface mode can the engineer use to generate Enhanced Application logs (EALs) for classifying IoT devices while receiving broadcast DHCP traffic?

Answer(s): A

---

3. Question #: 1
Topic #: 1
Which CLI command is used to simulate traffic going through the firewall and determine which Security policy rule, NAT translation, static route, or PBF rule will be triggered by the traffic?

A. A. check

B. B. find

C. C. test

D. D. sim

Answer(s): C

---

4. Question #: 244
Topic #: 1
What is the function of a service route?

A. A. The service packets exit the firewall on the port assigned for the external service. The server sends its response to the configured source interface and source IP address.

B. B. The service packets enter the firewall on the port assigned from the external service. The server sends its response to the configured destination interface and destination IP address.

C. C. The service route is the method required to use the firewall’s management plane to provide services to applications.

D. D. Service routes provide access to external services, such as DNS servers, external authentication servers or Palo Alto Networks services like the Customer Support Portal.

Answer(s): D

---

5. Question #: 231
Topic #: 1
An enterprise Information Security team has deployed policies based on AD groups to restrict user access to critical infrastructure systems. However, a recent phishing campaign against the organization has prompted information Security to look for more controls that can secure access to critical assets. For users that need to access these systems, Information Security wants to use PAN-OS multi-factor authentication (MFA) integration to enforce MFA.
What should the enterprise do to use PAN-OS MFA?

A. A. Use a Credential Phishing agent to detect, prevent, and mitigate credential phishing campaigns.

B. B. Create an authentication profile and assign another authentication factor to be used by a Captive Portal authentication policy.

C. C. Configure a Captive Portal authentication policy that uses an authentication sequence.

D. D. Configure a Captive Portal authentication policy that uses an authentication profile that references a RADIUS profile.

Answer(s): D

---

6. Question #: 541
Topic #: 1
An engineer creates a set of rules in a Device Group (Panorama) to permit traffic to various services for a specific LDAP user group.

A. What needs to be configured to ensure Panorama can retrieve user and group information for use in these rules?

Answer(s): C

---

7. Question #: 538
Topic #: 1
Phase two of a VPN will not establish a connection. The peer is using a policy-based VPN configuration.

A. What part of the configuration should the engineer verify?

Answer(s): C

---

8. Question #: 534
Topic #: 1
A company has recently migrated their branch office’s PA-220s to a centralized Panorama. This Panorama manages a number of PA-7000 Series and PA-5200 Series devices. All device group and template configuration is managed solely within Panorama.

A. They notice that commit times have drastically increased for the PA-220s after the migration.

Answer(s): A

---

9. Question #: 533
Topic #: 1
An engineer manages a high availability network and requires fast failover of the routing protocols. The engineer decides to implement BFD.

A. Which three dynamic routing protocols support BFD? (Choose three.)

Answer(s): ADE

---

10. Question #: 529
Topic #: 1
With the default TCP and UDP settings on the firewall, what will be the identified application in the following session?

A. A. insufficient-data

B. B. incomplete

C. C. not-applicable

D. D. unknown-tcp

Answer(s): C

---

11. Question #: 527
Topic #: 1
An organization conducts research on the benefits of leveraging the Web Proxy feature of PAN-OS 11.0.

A. What are two benefits of using an explicit proxy method versus a transparent proxy method? (Choose two.)

Answer(s): CD

---

12. Question #: 526
Topic #: 1
An engineer is configuring a firewall with three interfaces:

A. • MGT connects to a switch with internet access.

B. • Ethernet1/1 connects to an edge router.

C. • Ethernet1/2 connects to a virtualization network.

Answer(s): B

---

13. Question #: 525
Topic #: 1
Which three items must be configured to implement application override? (Choose three.)

A. A. Application filter

B. B. Application override policy rule

C. C. Custom app

D. D. Decryption policy rule

E. E. Security policy rule

Answer(s): BCE

---

14. Question #: 206
Topic #: 1
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” re 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. A. Route 1

B. B. Route 3

C. C. Route 2

D. D. Route 4

Answer(s): C

---

15. Question #: 568
Topic #: 1
An organization wants to begin decrypting guest and BYOD traffic.

A. Which NGFW feature can be used to identify guests and BYOD users, instruct them how to download and install the CA certificate, and clearly notify them that their traffic will be decrypted?

Answer(s): A

---

16. Question #: 566
Topic #: 1
An engineer is monitoring an active/active high availability (HA) firewall pair.

A. Which HA firewall state describes the firewall that is currently processing traffic?

Answer(s): D

---

17. Question #: 564
Topic #: 1

An administrator configures a site-to-site IPsec VPN tunnel between a PA-850 and an external customer on their policy-based VPN devices.

A. What should an administrator configure to route interesting traffic through the VPN tunnel?

Answer(s): A

---

18. Question #: 561
Topic #: 1
After switching to a different WAN connection, users have reported that various websites will not load, and timeouts are occurring. The web servers work fine from other locations.

A. The firewall engineer discovers that some return traffic from these web servers is not reaching the users behind the firewall. The engineer later concludes that the maximum transmission unit (MTU) on an upstream router interface is set to 1400 bytes.

Answer(s): B

---

19. Question #: 578
Topic #: 1
What can the Log Forwarding built-in action with tagging be used to accomplish?

A. A. Forward selected logs to the Azure Security Center.

B. B. Block the destination zones of selected unwanted traffic.

C. C. Block the source zones of selected unwanted traffic.

D. D. Block the destination IP addresses of selected unwanted traffic.

Answer(s): D

---

20. Question #: 580
Topic #: 1
A firewall administrator wants to be able to see all NAT sessions that are going through a firewall with source NAT.

A. Which CLI command can the administrator use?

Answer(s): A
