Palo Alto Networks Certified Network Security Administrator

1. Topic #: 1
Four configuration choices are listed, and each could be used to block access to a specific URL. If you configured each choice to block the same URL then which choice would be the last to block access to the URL?

A. A. EDL in URL Filtering Profile

B. B. Custom URL category in URL Filtering Profile

C. C. Custom URL category in Security policy rule

D. D. PAN-DB URL category in URL Filtering Profile

Answer(s): D

---

2. Question #: 405
Topic #: 1
Which path in PAN-OS 11.x would you follow to see how new and modified App-IDs impact a Security policy?

A. A. Device > Dynamic Updates > Review App-IDs

B. B. Objects > Dynamic Updates > Review App-IDs

C. C. Objects > Dynamic Updates > Review Policies

D. D. Device > Dynamic Updates > Review Policies

Answer(s): D

---

3. Question #: 317
Topic #: 1
Which three management interface settings must be configured for functional dynamic updates and administrative access on a Palo Alto Networks firewall? (Choose three.)

A. A. NTP

B. B. IP address

C. C. MTU

D. D. DNS server

E. E. service routes

Answer(s): A B D

---

4. Question #: 186
Topic #: 1
A coworker found a USB labeled “confidential in the parking lot. They inserted the drive and it infected their corporate laptop with unknown malware The malware caused the laptop to begin infiltrating corporate data.
Which Security Profile feature could have been used to detect the malware on the laptop?

A. A. DNS Sinkhole

B. B. WildFire Analysis

C. C. Antivirus

D. D. DoS Protection

Answer(s): C

---

5. Question #: 170
Topic #: 1
Starting with PAN-OS version 9.1, application dependency information is now reported in which two locations? (Choose two.)

A. A. on the App Dependency tab in the Commit Status window

B. B. on the Policy Optimizer’s Rule Usage page

C. C. on the Application tab in the Security Policy Rule creation window

D. D. on the Objects > Applications browser pages

Answer(s): A C

---

6. Question #: 168
Topic #: 1
Refer to the exhibit. An administrator is using DNAT to map two servers to a single public IP address. Traffic will be steered to the specific server based on the application, where Host A (10.1.1.100) receives HTTP traffic and Host B (10.1.1.101) receives SSH traffic.

A. Which two Security policy rules will accomplish this configuration? (Choose two.)

Answer(s): A C

---

7. Question #: 356
Topic #: 1
What are three DNS policy actions? (Choose three.)

A. A. Block

B. B. Allow

C. C. Strict

D. D. Sinkhole

E. E. Alert

Answer(s): A B

---

8. Question #: 355
Topic #: 1
When configuring a security policy, what is a best practice for User-ID?

A. A. Use only one method for mapping IP addresses to usernames.

B. B. Allow the User-ID agent in zones where agents are not monitoring services.

C. C. Limit User-ID to users registered in an Active Directory server.

D. D. Deny WMI traffic from the User-ID agent to any external zone.

Answer(s): D

---

9. Question #: 406
Topic #: 1
What are three configurable interface types for a data-plane ethernet interface? (Choose three.)

A. A. VWire

B. B. Layer 2

C. C. Management

D. D. HSCI

E. E. Layer 3

Answer(s): A B E

---

10. Question #: 209
Topic #: 1
What are three valid information sources that can be used when tagging users to dynamic user groups? (Choose three.)

A. A. firewall logs

B. B. custom API scripts

C. C. Security Information and Event Management Systems (SIEMS), such as Splunk

D. D. biometric scanning results from iOS devices

E. E. DNS Security service

Answer(s): A B C

---

11. Question #: 208
Topic #: 1
What are the three DNS Security categories available to control DNS traffic? (Choose three.)

A. A. Parked Domains

B. B. Spyware Domains

C. C. Vulnerability Domains

D. D. Phishing Domains

E. E. Malware Domains

Answer(s): A D E

---

12. Question #: 350
Topic #: 1
Where can you apply URL Filtering policy in a Security policy rule?

A. A. Within the applications selection

B. B. Within a destination address

C. C. Within a service type

D. D. Within the actions tab

Answer(s): D

---

13. Question #: 15
Topic #: 1
Choose the option that correctly completes this statement. A Security Profile can block or allow traffic _____.

A. A. on either the data place or the management plane.

B. B. after it is matched by a security policy rule that allows traffic.

C. C. before it is matched to a Security policy rule.

D. D. after it is matched by a security policy rule that allows or blocks traffic.

Answer(s): B

---

14. Question #: 11
Topic #: 1
Which User-ID mapping method should be used for an environment with users that do not authenticate to Active Directory?

A. A. Windows session monitoring

B. B. passive server monitoring using the Windows-based agent

C. C. Captive Portal

D. D. passive server monitoring using a PAN-OS integrated User-ID agent

Answer(s): C

---

15. Question #: 271
Topic #: 1
An administrator manages a network with 300 addresses that require translation. The administrator configured NAT with an address pool of 240 addresses and found that connections from addresses that needed new translations were being dropped.

A. Which type of NAT was configured?

Answer(s): A

---

16. Question #: 288
Topic #: 1
By default, which action is assigned to the interzone-default rule?

A. A. Allow

B. B. Deny

C. C. Reset-client

D. D. Reset-server

Answer(s): D

---

17. Question #: 284
Topic #: 1
An administrator configured a Security policy rule with an Antivirus Security profile. The administrator did not change the action for the profile.

A. If a virus gets detected, how will the firewall handle the traffic?

Answer(s): D

---

18. Question #: 298
Topic #: 1

Which rule type is appropriate for matching traffic occurring within a specified zone?

A. A. Universal

B. B. Shadowed

C. C. Intrazone

D. D. Interzone

Answer(s): C

---

19. Question #: 295
Topic #: 1
What must exist in order for the firewall to route traffic between Layer 3 interfaces?

A. A. Virtual router

B. B. Virtual wires

C. C. Traffic Distribution profile

D. D. VLANs

Answer(s): A

---

20. Question #: 291
Topic #: 1
Where within the firewall GUI can all existing tags be viewed?

A. A. Policies > Tags

B. B. Network > Tags

C. C. Objects > Tags

D. D. Monitor > Tags

Answer(s): C