bandwidth needed to support mission-critical applications. Given the scenario, which type of User-ID agent is considered a best practice by Palo Alto Networks?

A. Windows-based agent on a domain controller
B. Captive Portal
C. Citrix terminal server with adequate data-plane resources
D. PAN-OS integrated agent

Correct Answer: A

QUESTION 81
Assume that traffic matches a Security policy rule but the attached Security Profiles is configured to block matching traffic. Which statement accurately describes how the firewall will apply an action to matching traffic?

A. If it is an allowed rule, then the Security Profile action is applied last
B. If it is a block rule then the Security policy rule action is applied last
C. If it is an allow rule then the Security policy rule is applied last
D. If it is a block rule then Security Profile action is applied last

Correct Answer: A

QUESTION 82
Which two statements are correct about App-ID content updates? (Choose two.)

A. Updated application content may change how security policy rules are enforced
B. After an application content update, new applications must be manually classified prior to use
C. Existing security policy rules are not affected by application content updates
D. After an application content update, new applications are automatically identified and classified

Correct Answer: AD

QUESTION 83
What in the minimum frequency for which you can configure the firewall too check for new wildfire antivirus signatures?

A. every 5 minutes
B. every 1 minute
C. every 24 hours
D. every 30 minutes

Correct Answer: B

QUESTION 84
Complete the statement. A security profile can block or allow traffic_____.

A. on unknown-tcp or unknown-udp traffic
B. after it is matched by a security policy that allows traffic
C. before it is matched by a security policy
D. after it is matched by a security policy that allows or blocks traffic

Correct Answer: B
Explanation:
Security profiles are objects added to policy rules that are configured with an action of allow.

QUESTION 85
A company moved its old port-based firewall to a new Palo Alto Networks NGFW 60 days ago.
Which utility should the company use to identify out-of-date or unused rules on the firewall?

A. Rule Usage Filter > No App Specified
B. Rule Usage Filter >Hit Count > Unused in 30 days
C. Rule Usage Filter > Unused Apps
D. Rule Usage Filter > Hit Count > Unused in 90 days

Correct Answer: D

QUESTION 86
Which update option is not available to administrators?

A. New Spyware Notifications
B. New URLs
C. New Application Signatures
D. New Malicious Domains
E. New Antivirus Signatures

Correct Answer: B

QUESTION 87
Which two features can be used to tag a user name so that it is included in a dynamic user
group? (Choose two)

A. XML API
B. log forwarding auto-tagging
C. GlobalProtect agent
D. User-ID Windows-based agent

Correct Answer: AD
Explanation:
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/url-filtering/url-filtering-concepts/url-
filtering-profile-actions

QUESTION 88
At which point in the app-ID update process can you determine if an existing policy rule is
affected by an app-ID update?

A. after clicking Check New in the Dynamic Update window
B. after connecting the firewall configuration
C. after downloading the update
D. after installing the update

Correct Answer: A

QUESTION 89
Starting with PAN_OS version 9.1 which new type of object is supported for use within the user field of a security policy rule?

A. local username
B. dynamic user group
C. remote username
D. static user group

Correct Answer: B

QUESTION 90
Which service protects cloud-based applications such as Dropbox and Salesforce by administering permissions and scanning files for sensitive information?

A. Aperture
B. AutoFocus
C. Parisma SaaS
D. GlobalProtect

Correct Answer: C

QUESTION 91
Which action would an administrator take to ensure that a service object will be available only to the selected device group?

A. create the service object in the specific template
B. uncheck the shared option
C. ensure that disable override is selected
D. ensure that disable override is cleared

Correct Answer: D
Explanation:
https://docs.paloaltonetworks.com/panorama/9-0/panorama-admin/manage-firewalls/manage-device-groups/create-objects-for-use-in-shared-or-device-group-policy

QUESTION 92
Choose the option that correctly completes this statement. A Security Profile can block or allow traffic _____.

A. on either the data place or the management plane.
B. after it is matched by a security policy rule that allows traffic.
C. before it is matched to a Security policy rule.
D. after it is matched by a security policy rule that allows or blocks traffic.

Correct Answer: B

QUESTION 93
Your company requires positive username attribution of every IP address used by wireless devices to support a new compliance requirement. You must collect IP-to-user mappings as soon

as possible with minimal downtime and minimal configuration changes to the wireless devices themselves. The wireless devices are from various manufactures. Given the scenario, choose the option for sending IP-to-user mappings to the NGFW.

A. syslog
B. RADIUS
C. UID redistribution
D. XFF headers

Correct Answer: A

QUESTION 94
Which two statements are true for the DNS security service introduced in PAN-OS version 10.0?

A. It functions like PAN-DB and requires activation through the app portal.
B. It removes the 100K limit for DNS entries for the downloaded DNS updates.
C. IT eliminates the need for dynamic DNS updates.
D. IT is automatically enabled and configured.

Correct Answer: AB

QUESTION 95
Which type of security rule will match traffic between the Inside zone and Outside zone, within the Inside zone, and within the Outside zone?

A. global
B. intrazone
C. interzone
D. universal

Correct Answer: D
Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClomCAC

QUESTION 96
Which administrator type utilizes predefined roles for a local administrator account?

A. Superuser
B. Role-based
C. Dynamic
D. Device administrator

Correct Answer: C

QUESTION 97
Which firewall plane provides configuration, logging, and reporting functions on a separate processor?

A. control
B. network processing
C. data

D. security processing

Correct Answer: A

QUESTION 98
When creating a custom URL category object, which is a valid type?

A. domain match
B. host names
C. wildcard
D. category match

Correct Answer: D

QUESTION 99
Which interface type is part of a Layer 3 zone with a Palo Alto Networks firewall?

A. Management
B. High Availability
C. Aggregate
D. Aggregation

Correct Answer: C

QUESTION 100
Which two App-ID applications will need to be allowed to use Facebook-chat? (Choose two.)

A. facebook
B. facebook-chat
C. facebook-base
D. facebook-email

Correct Answer: BC

QUESTION 101
Which two firewall components enable you to configure SYN flood protection thresholds?
(Choose two.)

A. QoS profile
B. DoS Protection profile
C. Zone Protection profile
D. DoS Protection policy

Correct Answer: BC

QUESTION 102
Given the cyber-attack lifecycle diagram identify the stage in which the attacker can run malicious
code against a vulnerability in a targeted machine.