B. Data Filtering profile applied to outbound Security policy rules.
C. Antivirus profile applied to inbound Security policy rules.
D. Vulnerability Protection profile applied to outbound Security policy rules.

Correct Answer: C

QUESTION 119
What is the main function of the Test Policy Match function?

A. verify that policy rules from Expedition are valid
B. confirm that rules meet or exceed the Best Practice Assessment recommendations
C. confirm that policy rules in the configuration are allowing/denying the correct traffic
D. ensure that policy rules are not shadowing other policy rules

Correct Answer: D

QUESTION 120
What is the main function of Policy Optimizer?

A. reduce load on the management plane by highlighting combinable security rules
B. migrate other firewall vendors' security rules to Palo Alto Networks configuration
C. eliminate "Log at Session Start" security rules
D. convert port-based security rules to application-based security rules

Correct Answer: D

QUESTION 121
Which rule type is appropriate for matching traffic both within and between the source and destination zones?

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

Correct Answer: A

QUESTION 122
Which Security profile would you apply to identify infected hosts on the protected network using DNS traffic?

A. URL traffic
B. vulnerability protection
C. anti-spyware
D. antivirus

Correct Answer: C

QUESTION 123
What can be achieved by selecting a policy target prior to pushing policy rules from Panorama?

A. Doing so limits the templates that receive the policy rules
B. Doing so provides audit information prior to making changes for selected policy rules
C. You can specify the firewalls m a device group to which to push policy rules
D. You specify the location as pre can - or post-rules to push policy rules

Correct Answer: C

QUESTION 124
Which plane on a Palo alto networks firewall provides configuration logging and reporting functions on a separate processor?

A. data
B. network processing
C. management
D. security processing

Correct Answer: C

QUESTION 125
If using group mapping with Active Directory Universal Groups, what must you do when configuring the User-ID?

A. Create an LDAP Server profile to connect to the root domain of the Global Catalog server on port 3268 or 3269 for SSL
B. Configure a frequency schedule to clear group mapping cache
C. Configure a Primary Employee ID number for user-based Security policies
D. Create a RADIUS Server profile to connect to the domain controllers using LDAPS on port 636 or 389

Correct Answer: A
Explanation:
If you have Universal Groups, create an LDAP server profile to connect to the root domain of the Global Catalog server on port 3268 or 3269 for SSL, then create another LDAP server profile to connect to the root domain controllers on port 389. This helps ensure that users and group information is available for all domains and subdomains.

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/user-id/map-users-to-groups

QUESTION 126
Your company occupies one floor in a single building you have two active directory domain controllers on a single networks the firewall s management plane is only slightly utilized. Which user-ID agent sufficient in your network?

A. PAN-OS integrated agent deployed on the firewall
B. Windows-based agent deployed on the internal network a domain member
C. Citrix terminal server agent deployed on the network
D. Windows-based agent deployed on each domain controller

Correct Answer: D

QUESTION 127
Which license is required to use the Palo Alto Networks built-in IP address EDLs?

A. DNS Security
B. Threat Prevention
C. WildFire
D. SD-Wan

Correct Answer: B

QUESTION 128
What is the correct process tor creating a custom URL category?

A. Objects > Security Profiles > URL Category > Add
B. Objects > Custom Objects > URL Filtering > Add
C. Objects > Security Profiles > URL Filtering > Add
D. Objects > Custom Objects > URL Category > Add

Correct Answer: D

QUESTION 129
Which statement is true regarding a Prevention Posture Assessment?

A. The Security Policy Adoption Heatmap component filters the information by device groups, serial numbers, zones, areas of architecture, and other categories
B. It provides a set of questionnaires that help uncover security risk prevention gaps across all areas of network and security architecture
C. It provides a percentage of adoption for each assessment area
D. It performs over 200 security checks on Panorama/firewall for the assessment

Correct Answer: B

QUESTION 130
The compliance officer requests that all evasive applications need to be blocked on all perimeter firewalls out to the internet The firewall is configured with two zones:

1. trust for internal networks
2. untrust to the internet

Based on the capabilities of the Palo Alto Networks NGFW, what are two ways to configure a security policy using App-ID to comply with this request? (Choose two)

A. Create a deny rule at the top of the policy from trust to untrust over any service and select evasive as the application
B. Create a deny rule at the top of the policy from trust to untrust with service application-default and select evasive as the application.
C. Create a deny rule at the top of the policy from trust to untrust over any service and add an application filter with the evasive characteristic.
D. Create a deny rule at the top of the policy from trust to untrust with service application-default and add an application filter with the evasive characteristic

Correct Answer: D

QUESTION 131
What are three differences between security policies and security profiles? (Choose three.)

A.   Security policies are attached to security profiles
B.   Security profiles are attached to security policies
C.   Security profiles should only be used on allowed traffic
D.   Security profiles are used to block traffic by themselves
E.   Security policies can block or allow traffic

Correct Answer: BCE

QUESTION 132
Which type of administrative role must you assign to a firewall administrator account, if the account must include a custom set of firewall permissions?

A.   SAML
B.   Multi-Factor Authentication
C.   Role-based
D.   Dynamic

Correct Answer: C

QUESTION 133
You receive notification about new malware that is being used to attack hosts The malware exploits a software bug in a common application. Which Security Profile detects and blocks access to this threat after you update the firewall's threat signature database?

A.   Data Filtering Profile applied to outbound Security policy rules
B.   Antivirus Profile applied to outbound Security policy rules
C.   Data Filtering Profile applied to inbound Security policy rules
D.   Vulnerability Profile applied to inbound Security policy rules

Correct Answer: B

QUESTION 134
Given the network diagram, traffic should be permitted for both Trusted and Guest users to access general Internet and DMZ servers using SSH, web-browsing and SSL applications. Which policy achieves the desired results?
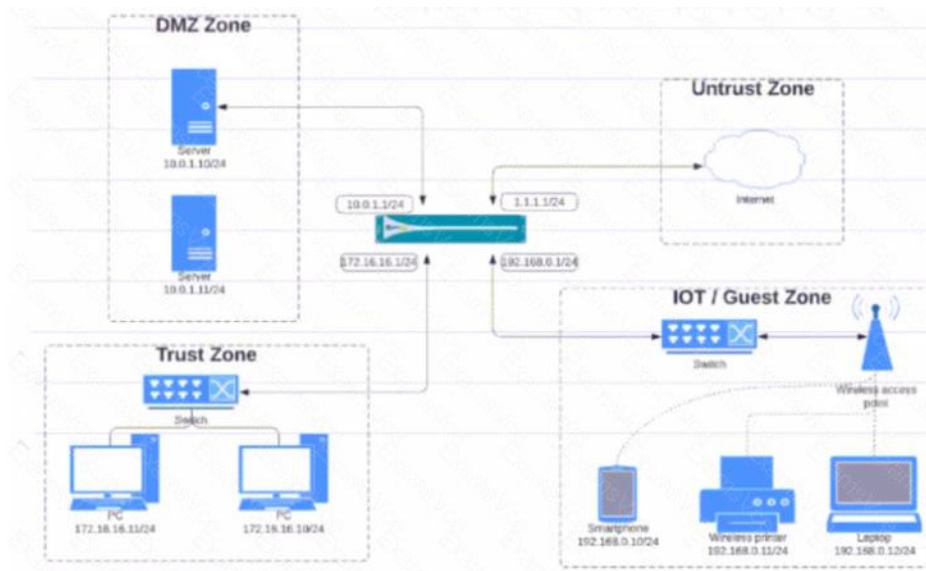
A.

NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS
				Source				**Destina**
04-A	none	universal	IOT-Guest	172.16.16.0/24	any	any	DMZ	any
			Trust	192.168.0.0/24			Untrust	

B.

NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS
03-A	none	universal	IOT-Guest	172.16.16.0/24	any	any	DMZ	1.1.1.0/
			Trust	192.168.0.0/24			Untrust	10.0.1.0

C.

NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS
				Source				**Destina**
02-A	none	universal	IOT-Guest	172.16.18.0/24	any	any	DMZ	any
			Trust	192.168.0.0/24			Untrust	

D.

NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS
				Source				**Destina**
01-A	none	universal	IOT-Guest	10.0.1.0/24	any	any	DMZ	1.1.1.0/2
			Trust	172.16.16.0/12			Untrust	192.168

Correct Answer: C
QUESTION 135
In which profile should you configure the DNS Security feature?

A.   URL Filtering Profile
B.   Anti-Spyware Profile
C.   Zone Protection Profile
D.   Antivirus Profile

Correct Answer: B

QUESTION 136
Which path is used to save and load a configuration with a Palo Alto Networks firewall?