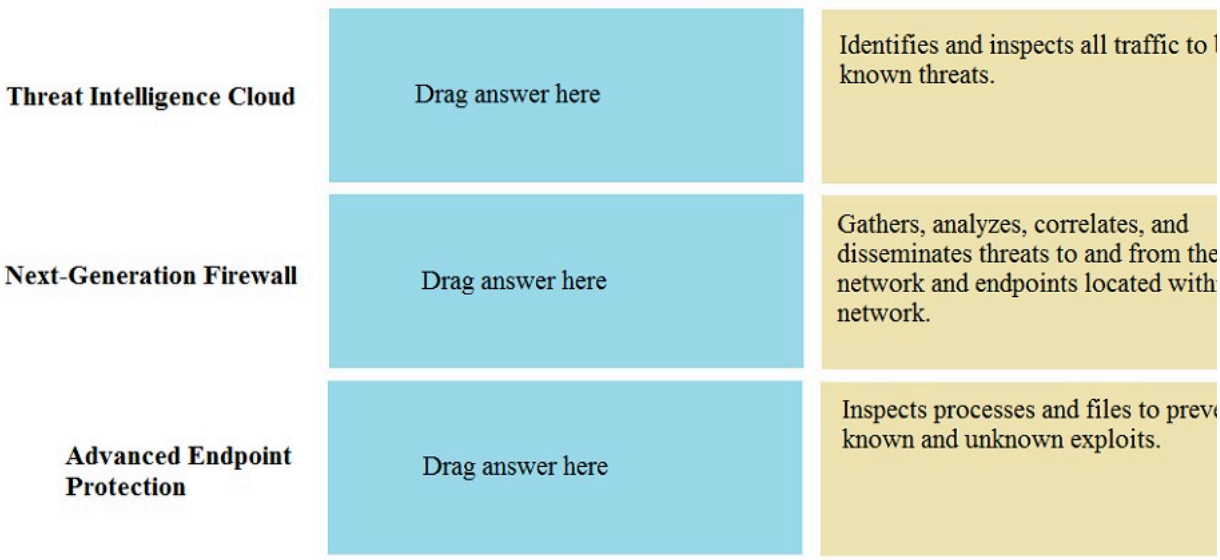
Palo Alto Networks Certified Network Security Administrator

1. DRAG DROP (Drag and Drop is not supported)
Match the Palo Alto Networks Security Operating Platform architecture to its description.
Select and Place:



A. See Explanation section for answer.

Answer(s): A

---

2. Which plane on a Palo Alto Networks Firewall provides configuration, logging, and reporting functions on a separate processor?

A. management

B. network processing

C. data

D. security processing

Answer(s): A

---

3. A security administrator has configured App-ID updates to be automatically downloaded and installed. The company is currently using an application identified by
App-ID as SuperApp_base.
On a content update notice, Palo Alto Networks is adding new app signatures labeled SuperApp_chat and SuperApp_download, which will be deployed in 30 days.
Based on the information, how is the SuperApp traffic affected after the 30 days have passed?

A. All traffic matching the SuperApp_chat, and SuperApp_download is denied because it no longer matches the SuperApp-base application

B. No impact because the apps were automatically downloaded and installed

C. No impact because the firewall automatically adds the rules to the App-ID interface

D. All traffic matching the SuperApp_base, SuperApp_chat, and SuperApp_download is denied until the security administrator approves the applications

Answer(s): A

---

4. How many zones can an interface be assigned with a Palo Alto Networks firewall?

A. two

B. three

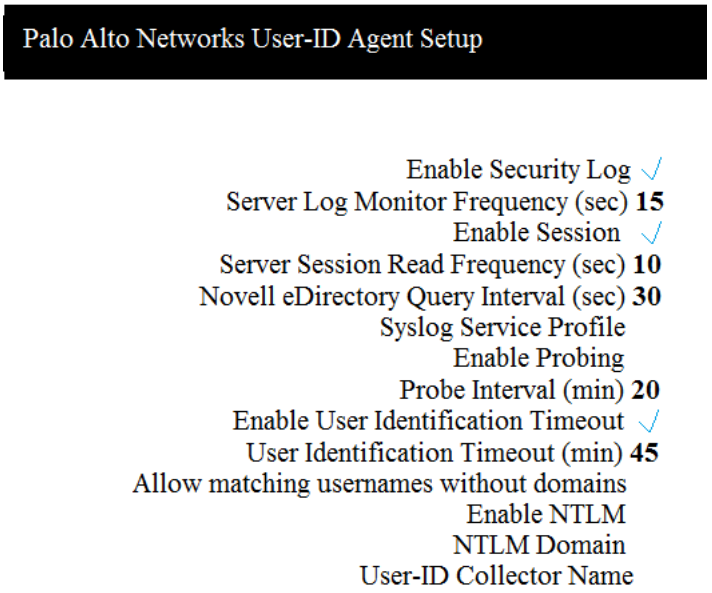
C. four

D. one

Answer(s): D

---

5. Which two configuration settings shown are not the default? (Choose two.)

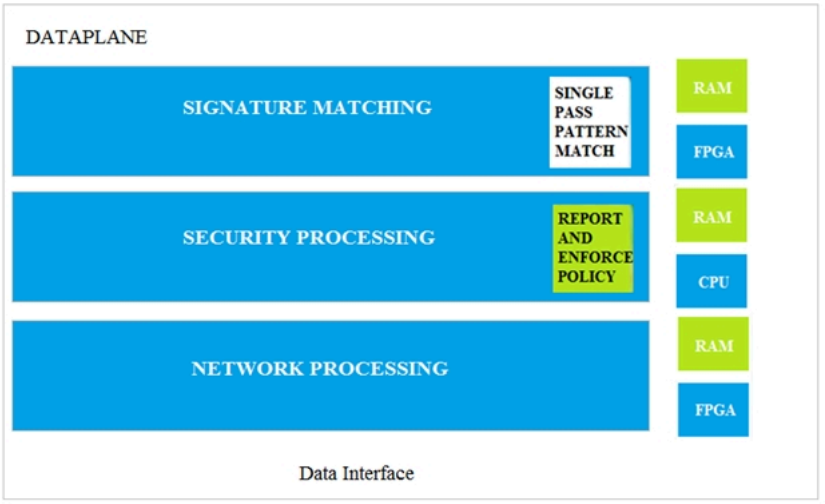


- [ ] A. Enable Security Log
- [ ] B. Server Log Monitor Frequency (sec)
- [ ] C. Enable Session
- [ ] D. Enable Probing

Answer(s): B C

---

6. Which dataplane layer of the graphic shown provides pattern protection for spyware and vulnerability exploits on a Palo Alto Networks Firewall?



A. Signature Matching

B. Network Processing

C. Security Processing

D. Data Interfaces

Answer(s): A

---

7. Which option shows the attributes that are selectable when setting up application filters?

A. Category, Subcategory, Technology, and Characteristic

B. Category, Subcategory, Technology, Risk, and Characteristic

C. Name, Category, Technology, Risk, and Characteristic

D. Category, Subcategory, Risk, Standard Ports, and Technology

Answer(s): B

---

8. Actions can be set for which two items in a URL filtering security profile? (Choose two.)

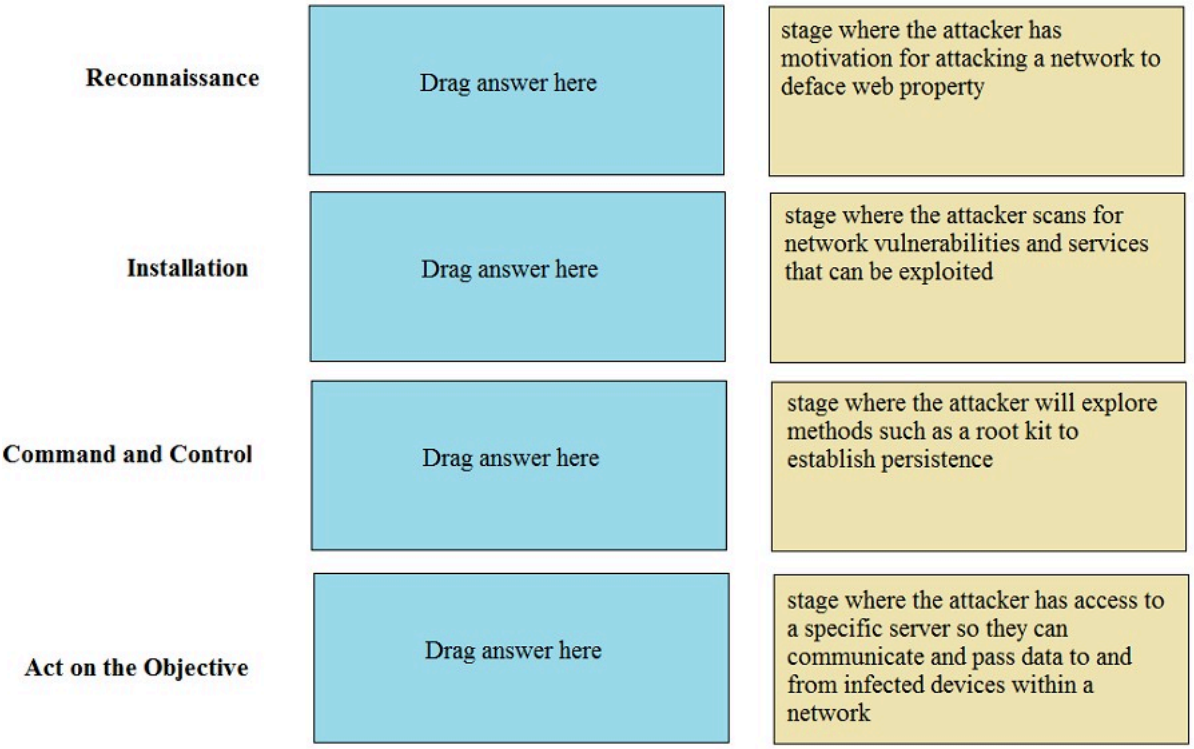
- [ ] A. Block List
- [ ] B. Custom URL Categories
- [ ] C. PAN-DB URL Categories
- [ ] D. Allow List

Answer(s): A D

---

9. DRAG DROP (Drag and Drop is not supported)
Match the Cyber-Attack Lifecycle stage to its correct description.

Select and Place:



A. See Explanation section for answer.

Answer(s): A

---

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

- ☐ A. Updated application content might 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.

Answer(s): C D

---

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

A. Windows session monitoring

B. passive server monitoring using the Windows-based agent

C. Captive Portal

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

Answer(s): C

---

12. An administrator needs to allow users to use their own office applications. How should the administrator configure the firewall to allow multiple applications in a dynamic environment?

A. Create an Application Filter and name it Office Programs, then filter it on the business-systems category, office-programs subcategory

B. Create an Application Group and add business-systems to it

C. Create an Application Filter and name it Office Programs, then filter it on the business-systems category

D. Create an Application Group and add Office 365, Evernote, Google Docs, and Libre Office

Answer(s): A

---

13. Which statement is true regarding a Best Practice Assessment?

A. The BPA tool can be run only on firewalls

B. It provides a percentage of adoption for each assessment area

C. The assessment, guided by an experienced sales engineer, helps determine the areas of greatest risk where you should focus prevention activities

D. It provides a set of questionnaires that help uncover security risk prevention gaps across all areas of network and security architecture

Answer(s): B

---

14. Employees are shown an application block page when they try to access YouTube. Which security policy is blocking the YouTube application?

			Source		Destination			
	Name	**Type**	**Zone**	**Address**	**Zone**	**Address**	**Application**	**Service**
1	Deny Google	universal	Inside	any	Outside	any	google-docs-base	application-
2	allowed-security serv..	universal	Inside	any	Outside	any	snmpv3 ssh ssl	application-
3	intrazone-default	intrazone	any	any	(intrazone)	any	any	any
4	interzone-default	interzone	any	any	any	any	any	any

A. intrazone-default

B. Deny Google

C. allowed-security services

D. interzone-default

Answer(s): D

---

15. 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.

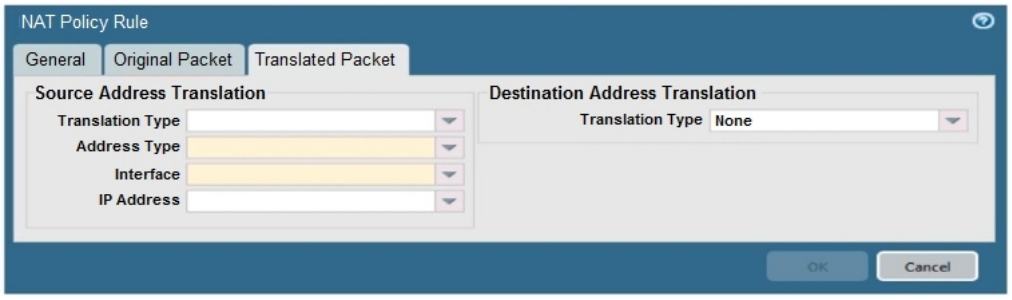
C. before it is matched to a Security policy rule.

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

Answer(s): D

---

16. When creating a Source NAT policy, which entry in the Translated Packet tab will display the options Dynamic IP and Port, Dynamic, Static IP, and None?



A. Translation Type

B. Interface

C. Address Type

D. IP Address

Answer(s): A

---

17. Which interface does not require a MAC or IP address?

A. Virtual Wire

B. Layer3

C. Layer2

D. Loopback

Answer(s): A

---

18. 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

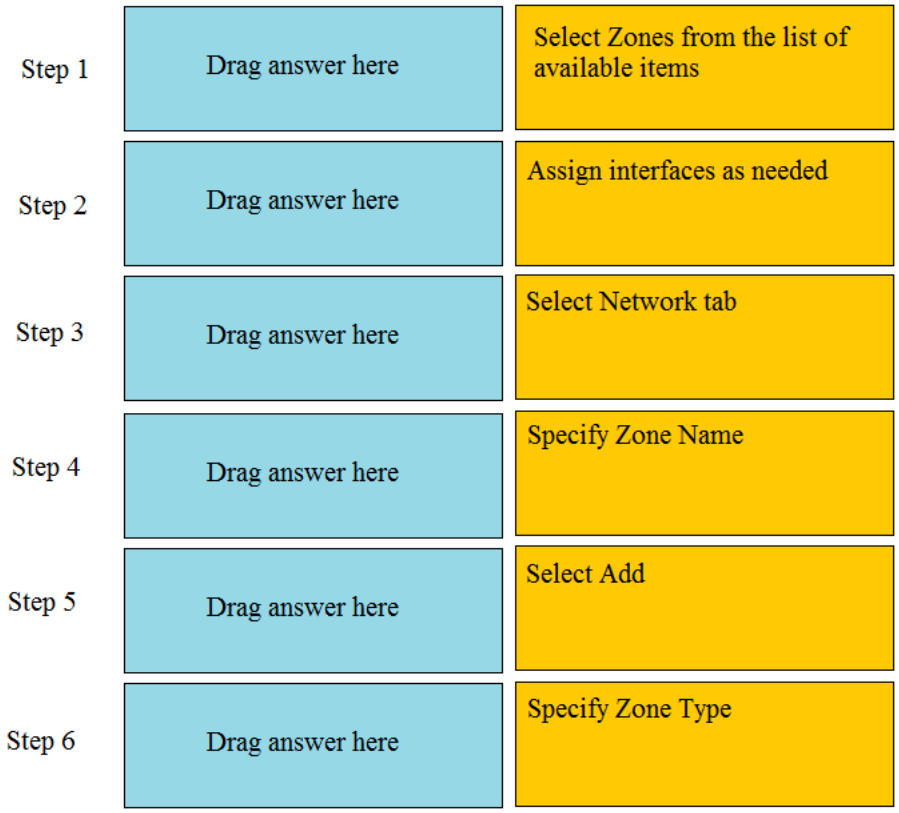
D. Rule Usage Filter > Hit Count > Unused in 90 days

Answer(s): D

---

19. DRAG DROP (Drag and Drop is not supported)
Order the steps needed to create a new security zone with a Palo Alto Networks firewall.

Select and Place:



A. See Explanation section for answer.

Answer(s): A

---

20. What are two differences between an implicit dependency and an explicit dependency in App-ID? (Choose two.)

- [ ] A. An implicit dependency does not require the dependent application to be added in the security policy
- [ ] B. An implicit dependency requires the dependent application to be added in the security policy
- [ ] C. An explicit dependency does not require the dependent application to be added in the security policy
- [ ] D. An explicit dependency requires the dependent application to be added in the security policy

Answer(s): A D
