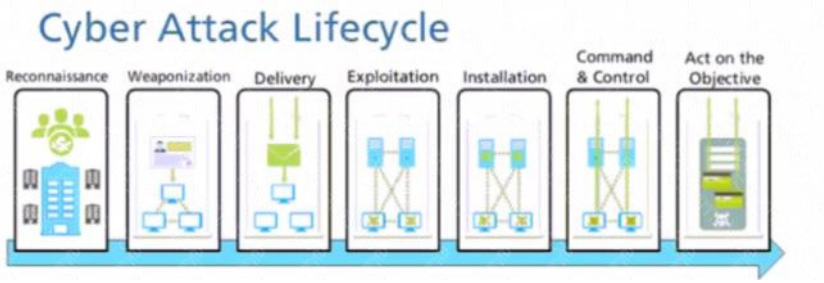


A. Exploitation
B. Installation
C. Reconnaissance
D. Act on the Objective

Correct Answer: A

QUESTION 103
Which two settings allow you to restrict access to the management interface? (Choose two)

A. enabling the Content-ID filter
B. administrative management services
C. restricting HTTP and telnet using App-ID
D. permitted IP addresses

Correct Answer: AC

QUESTION 104
Which two rule types allow the administrator to modify the destination zone? (Choose two)

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

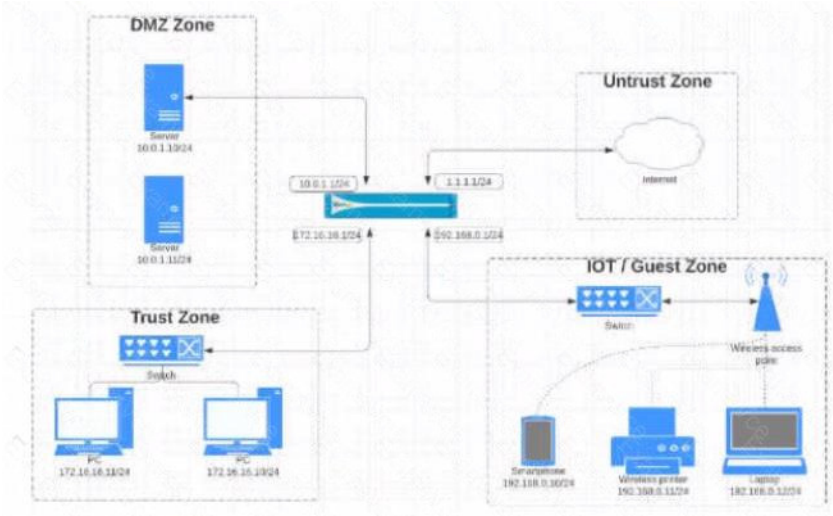
Correct Answer: AC

QUESTION 105
Which three types of authentication services can be used to authenticate user traffic flowing through the firewalls data plane? (Choose three)

A. TACACS
B. SAML2
C. SAML10
D. Kerberos
E. TACACS+

Correct Answer: ABD

QUESTION 106
View the diagram. What is the most restrictive yet fully functional rule to allow general Internet and SSH traffic into both the DMZ and Untrust/Internet zones from each of the IOT/Guest and Trust Zones?



A.

Source				Destination						
ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	URL CATEGORY	ACTION
172.16.16.0/24 192.168.0.0/24	any	any	DMZ Untrust	1.1.1.0/24 10.0.1.0/24	any	ssh ssl web-browsing	application-default	any	Allow

B.

Source				Destination						
ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	URL CATEGORY	ACTION
10.0.1.0/24 172.16.16.0/12	any	any	DMZ Untrust	1.1.1.0/24 192.168.0.0/24	any	ssh ssl web-browsing	application-default	any	Allow

C.

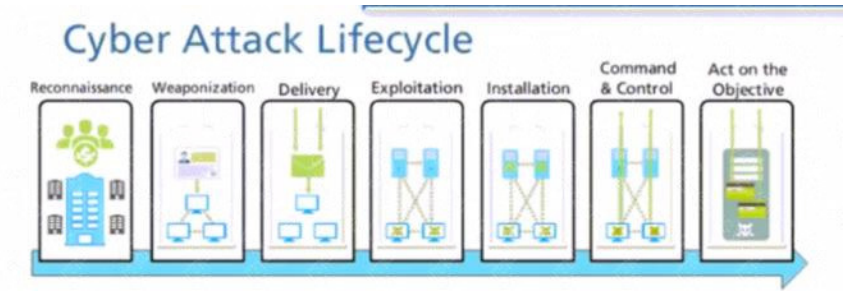
Source				Destination						
ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	URL CATEGORY	ACTION
172.16.16.0/24 192.168.0.0/24	any	any	DMZ Untrust	any	any	ssh ssl web-browsing	application-default	any	Allow

D.

Source				Destination						
ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	URL CATEGORY	ACTION
172.16.16.0/24 192.168.0.0/24	any	any	DMZ Untrust	any	any	ssh ssl web-browsing	application-default	any	Allow

Correct Answer: C

QUESTION 107
At which stage of the cyber-attack lifecycle would the attacker attach an infected PDF file to an email?



A. delivery
B. command and control
C. explotation
D. reinsurance
E. installation

Correct Answer: A

QUESTION 108
A Security Profile can block or allow traffic at which point?

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

Correct Answer: A

QUESTION 109
Which five Zero Trust concepts does a Palo Alto Networks firewall apply to achieve an integrated approach to prevent threats? (Choose five.)

A. User identification
B. Filtration protection
C. Vulnerability protection
D. Antivirus
E. Application identification
F. Anti-spyware
Correct Answer: ACDEF

QUESTION 110
Which license must an Administrator acquire prior to downloading Antivirus Updates for use with the firewall?

A. Threat Prevention License
B. Threat Implementation License
C. Threat Environment License
D. Threat Protection License

Correct Answer: A

QUESTION 111
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, the 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

Correct Answer: A
Explanation:
An application filter is an object that dynamically groups applications based on application attributes that you define, including category, subcategory, technology, risk factor, and characteristic. This is useful when you want to safely enable access to applications that you do not explicitly sanction, but that you want users to be able to access. For example, you may want to enable employees to choose their own office programs (such as Evernote, Google Docs, or Microsoft Office 365) for business use. To safely enable these types of applications, you could create an application filter that matches on the Category business-systems and the Subcategory office-programs. As new applications office programs emerge and new App-IDs get created, these new applications will automatically match the filter you defined; you will not have to make any additional changes to your policy rulebase to safely enable any applicatio n that matches the attributes you defined for the filter.

https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/app-id/use-application-objects-in-policy/create-an-application-filter.html

QUESTION 112
Which interface type can use virtual routers and routing protocols?

A. Tap
B. Layer3
C. Virtual Wire
D. Layer2

Correct Answer: B

QUESTION 113
What must be configured before setting up Credential Phishing Prevention?

A. Anti Phishing Block Page
B. Threat Prevention
C. Anti Phishing profiles
D. User-ID

Correct Answer: A
Explanation:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/threat-prevention/prevent-credential-phishing/set-up-credential-phishing-prevention

QUESTION 114
How is the hit count reset on a rule?

A. select a security policy rule, right click Hit Count > Reset
B. with a dataplane reboot
C. Device > Setup > Logging and Reporting Settings > Reset Hit Count
D. in the CLI, type command reset hitcount <POLICY-NAME>

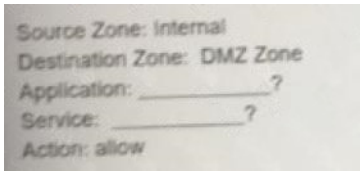
Correct Answer: A

QUESTION 115
Which file is used to save the running configuration with a Palo Alto Networks firewall?

A. running-config.xml
B. run-config.xml
C. running-configuration.xml
D. run-configuratin.xml

Correct Answer: A

QUESTION 116
All users from the internal zone must be allowed only Telnet access to a server in the DMZ zone. Complete the two empty fields in the Security Policy rules that permits only this type of access. (Choose two.)



A. Service = "any"
B. Application = "Telnet"
C. Service - "application-default"
D. Application = "any"

Correct Answer: BC
QUESTION 117
Which protocol used to map username to user groups when user-ID is configured?

A. SAML
B. RADIUS
C. TACACS+
D. LDAP

Correct Answer: D

QUESTION 118
You receive notification about new malware that infects hosts through malicious files transferred by FTP. Which Security profile detects and protects your internal networks from this threat after you update your firewall's threat signature database?

A. URL Filtering profile applied to inbound Security policy rules.