PCNSA.exam.26q

Number: PCNSA
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

Palo ALTO PCNSA

Palo Alto Networks Certified Network Security Administrator

Exam A

QUESTION 1
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	URL Category	Action	Profile
1	Deny Google	Universal	Inside	Any	Outside	Any	Google-docs-base	Application-d	Any	Deny	None
2	Allowed-security serv...	Universal	Inside	Any	Outside	Any	Snmpv3 Ssh ssl	Application-d	Any	Allow	None
3	Intrazone-default	Intrazone	Any	Any	(intrazone)	Any	Any	Any	Any	Allow	None
4	Interzone-default	Interzone	Any	Any	Any	Any	Any	Any	Any	Deny	None

A. intrazone-default
B. Deny Google
C. allowed-security services
D. interzone-default

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
Complete the statement. A security profile can block or allow traffic.

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4

An administrator receives a global notification for a new malware that infects hosts. The infection will result in the infected host attempting to contact a commandand-control (C2) server. Which two security profile components will detect and prevent this threat after the firewall's signature database has been updated?
(Choose two.)

A. vulnerability protection profile applied to outbound security policies
B. anti-spyware profile applied to outbound security policies
C. antivirus profile applied to outbound security policies
D. URL filtering profile applied to outbound security policies

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-admin/policy/create-best-practice-security-profiles

QUESTION 5

In which stage of the Cyber-Attack Lifecycle would the attacker inject a PDF file within an email?

A. Weaponization
B. Reconnaissance
C. Installation
D. Command and Control
E. Exploitation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6

Identify the correct order to configure the PAN-OS integrated USER-ID agent.

3. add the service account to monitor the server(s)
2. define the address of the servers to be monitored on the firewall
4. commit the configuration, and verify agent connection status
1. create a service account on the Domain Controller with sufficient permissions to execute the User- ID agent

A. 2-3-4-1
B. 1-4-3-2
C. 3-1-2-4
D. 1-3-2-4

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
Users from the internal zone need to be allowed to Telnet into a server in the DMZ zone.
Complete the security policy to ensure only Telnet is allowed.
Security Policy: Source Zone: Internal to DMZ Zone _____services “Application defaults”, and action = Allow

A. Destination IP: 192.168.1.123/24
B. Application = ‘Telnet’
C. Log Forwarding
D. USER-ID = ‘Allow users in Trusted’

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
Based on the security policy rules shown, ssh will be allowed on which port?

			Source		Destination						
	Name	Type	Zone	Address	Zone	Address	Application	Service	URL Category	Action	Profile
1	Deny Google	Universal	Inside	Any	Outside	Any	Google-docs-base	Application-d	Any	Deny	None
2	Allowed-security serv...	Universal	Inside	Any	Outside	Any	Snmpv3 Ssh ssl	Application-d	Any	Allow	None
3	Intrazone-default	Intrazone	Any	Any	(intrazone)	Any	Any	Any	Any	Allow	None
4	Interzone-default	Interzone	Any	Any	Any	Any	Any	Any	Any	Deny	None

A. 80
B. 53
C. 22
D. 23

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

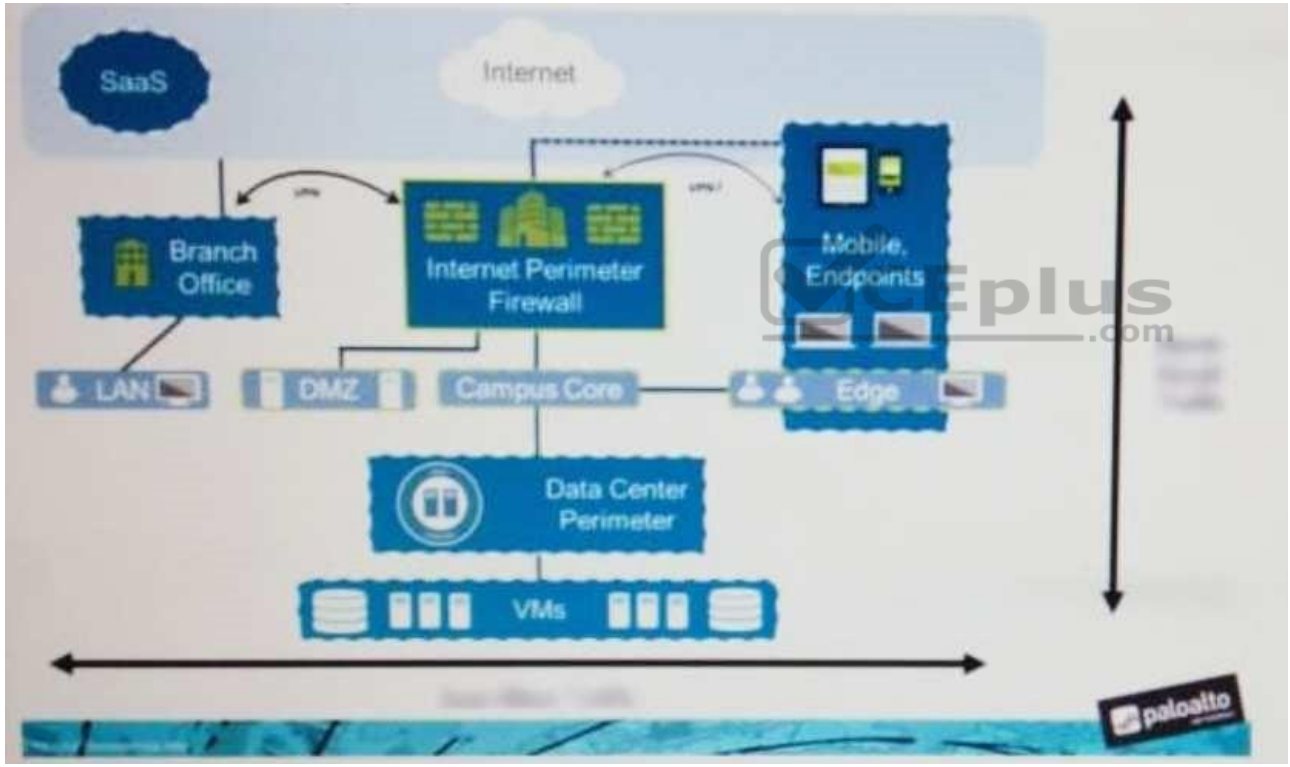
QUESTION 9
Which license must an Administrator acquire prior to downloading Antivirus Updates for use with the firewall?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/threat-prevention/set-up-antivirus-anti-spyware-and-vulnerability-protection.html

QUESTION 10
An administrator notices that protection is needed for traffic within the network due to malicious lateral movement activity. Based on the image shown, which traffic would the administrator need to monitor and block to mitigate the malicious activity?

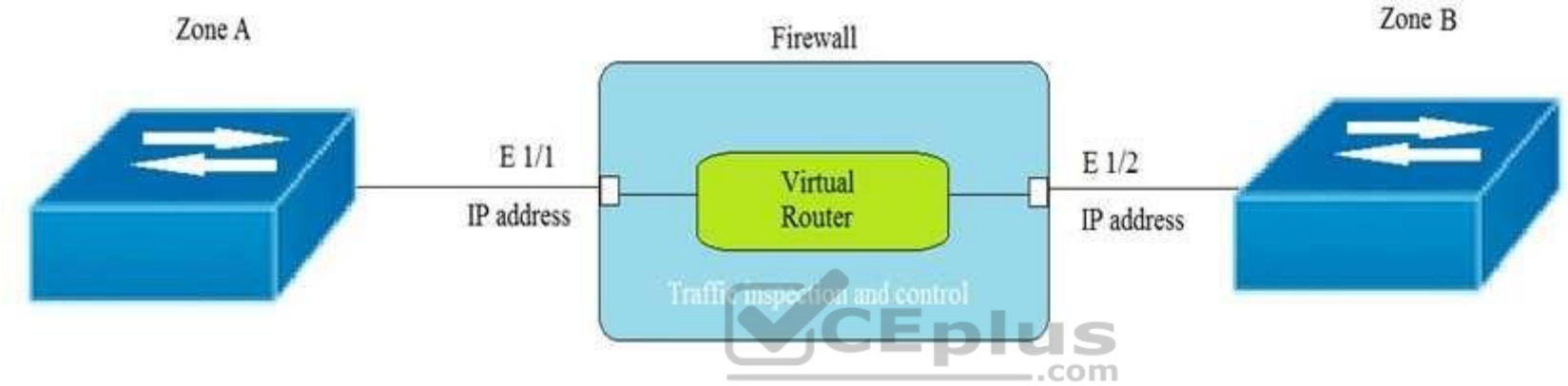


A. branch office traffic
B. north-south traffic
C. perimeter traffic D. east-west traffic

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
Given the topology, which zone type should zone A and zone B to be configured with?



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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
To use Active Directory to authenticate administrators, which server profile is required in the authentication profile?
A. domain controller
B. TACACS+

C. LDAP
D. RADIUS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
Which interface type is used to monitor traffic and cannot be used to perform traffic shaping?

A. Layer 2
B. Tap
C. Layer 3
D. Virtual Wire

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
Which administrator type provides more granular options to determine what the administrator can view and modify when creating an administrator account?

A. Root
B. Dynamic
C. Role-based
D. Superuser

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
Which administrator type utilizes predefined roles for a local administrator account?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-cli-quick-start/get-started-with-the-cli/give-administrators-access-to-the-cli/administrativeprivileges?PageSpeed=noscript

QUESTION 16
Which two security profile types can be attached to a security policy? (Choose two.)

A. antivirus
B. DDoS protection
C. threat
D. vulnerability

Correct Answer: AD

Section: (none)
Explanation
Explanation/Reference:
Reference: https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/policy/security-profiles

QUESTION 17
The CFO found a USB drive in the parking lot and decide to plug it into their corporate laptop. The USB drive had malware on it that loaded onto their computer and then contacted a known command and control (CnC) server, which ordered the infected machine to begin Exfiltrating data from the laptop.

Which security profile feature could have been used to prevent the communication with the CnC server?

A. Create an anti-spyware profile and enable DNS Sinkhole
B. Create an antivirus profile and enable DNS Sinkhole
C. Create a URL filtering profile and block the DNS Sinkhole category
D. Create a security policy and enable DNS Sinkhole

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-web-interface-help/objects/objects-security-profiles-anti-spyware-profile

QUESTION 18
Which user mapping method could be used to discover user IDs in an environment with multiple Windows domain controllers?

A. Active Directory monitoring
B. Windows session monitoring
C. Windows client probing
D. domain controller monitoring

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
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
Section: (none)
Explanation

Explanation/Reference:

				Source				Destination		Rule Usage						
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Hit Count	Last Hit	First Hit	Application	Service	Action	Profile
1	Allow Office Programs	None	Universal	Inside	Any	Any	Any	Outside	Any	-	-	-	Office-program	Application-d...	Allow	None
2	Allow FTP to web ser..	None	Universal	Inside	Any	Any	Any	Outside	ftp-server	-	-	-	any	ftp-service..	Allow	None
3	Allow Social Networkin..	None	Universal	Inside	Any	Any	Any	Outside	Any	-	-	-	facebook	Application-d...	Allow	None

QUESTION 20
Given the image, which two options are true about the Security policy rules. (Choose two.)

A. The Allow Office Programs rule is using an Application Filter
B. In the Allow FTP to web server rule, FTP is allowed using App-ID
C. The Allow Office Programs rule is using an Application Group
D. In the Allow Social Networking rule, allows all of Facebook's functions

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
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
Section: (none)
Explanation

Explanation/Reference:
Reference: https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClomCAC

QUESTION 22
Which Palo Alto Networks firewall security platform provides network security for mobile endpoints by inspecting traffic deployed as internet gateways?

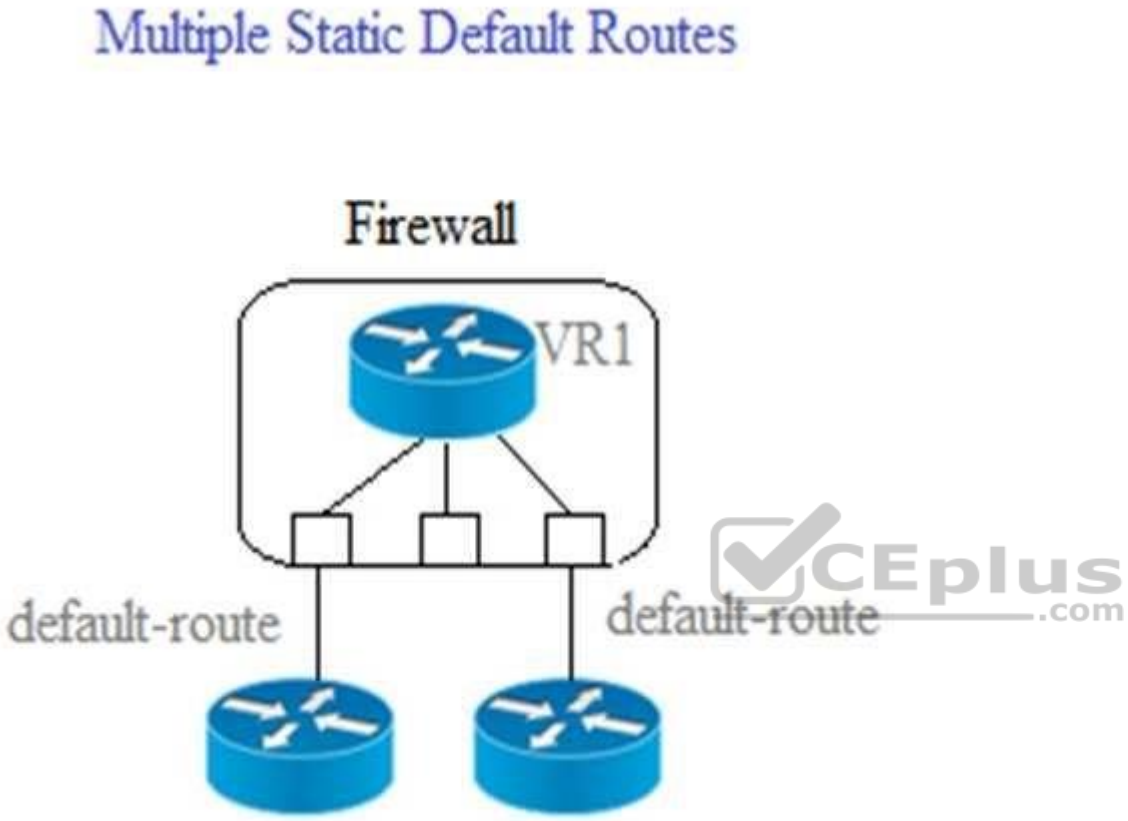
A. GlobalProtect
B. AutoFocus
C. Aperture
D. Panorama

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23

Given the scenario, which two statements are correct regarding multiple static default routes? (Choose two.)



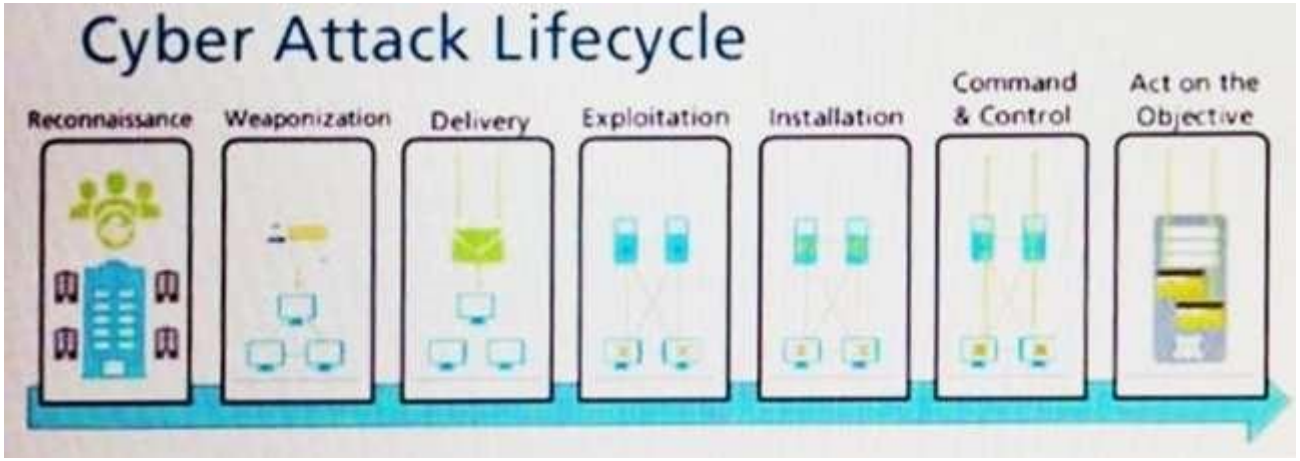
A. Path monitoring does not determine if route is useable
B. Route with highest metric is actively used
C. Path monitoring determines if route is useable
D. Route with lowest metric is actively used

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24

Given the Cyber-Attack Lifecycle diagram, identify the stage in which the attacker can initiate malicious code against a targeted machine.



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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25

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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
In the example security policy shown, which two websites would be blocked? (Choose two.)

	Name	Tags	Zone	Address	Zone	Address	Application	Service	URL Category	Action	Profile
1	Block-Sites	outbound	Inside	Any	Outside	Any	Any	any	Social-networking	Deny	None

A. LinkedIn
B. Facebook
C. YouTube
D. Amazon

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference: