PCNSA.VCEplus.premium.exam.50q

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

PCNSA

Palo Alto Networks Certified Network Security Administrator

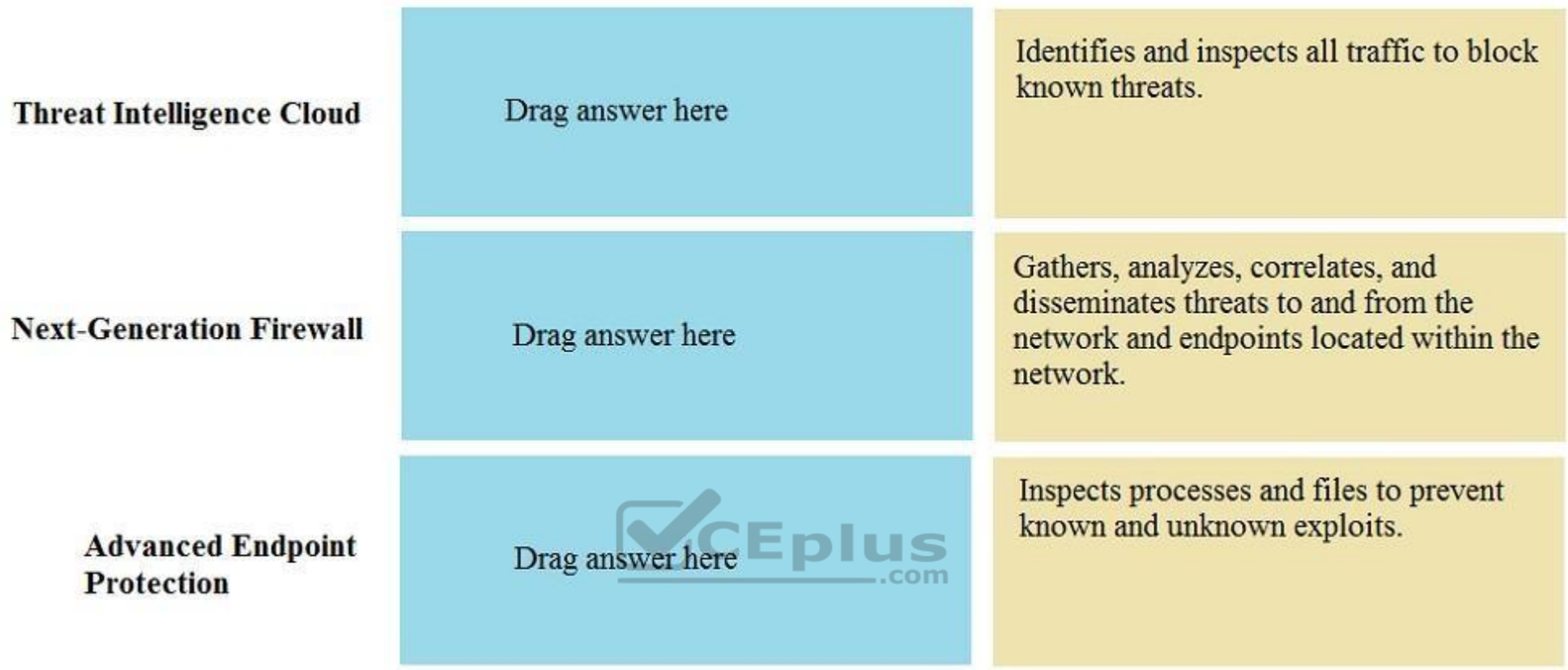
Version 1.0

Exam A

QUESTION 1
DRAG DROP

Match the Palo Alto Networks Security Operating Platform architecture to its description.

Select and Place:



Correct Answer:

Threat Intelligence Cloud	Gathers, analyzes, correlates, and disseminates threats to and from the network and endpoints located within the network.	Identifies and inspects all traffic to block known threats.
Next-Generation Firewall	Identifies and inspects all traffic to block known threats.	Gathers, analyzes, correlates, and disseminates threats to and from the network and endpoints located within the network.
Advanced Endpoint Protection	Inspects processes and files to prevent known and unknown exploits.	Inspects processes and files to prevent known and unknown exploits.

Section: (none)
Explanation

Explanation/Reference:

QUESTION 2 Which firewall plane provides configuration, logging, and reporting functions on a separate processor?

A. control
B. network processingC. data
D. security processing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

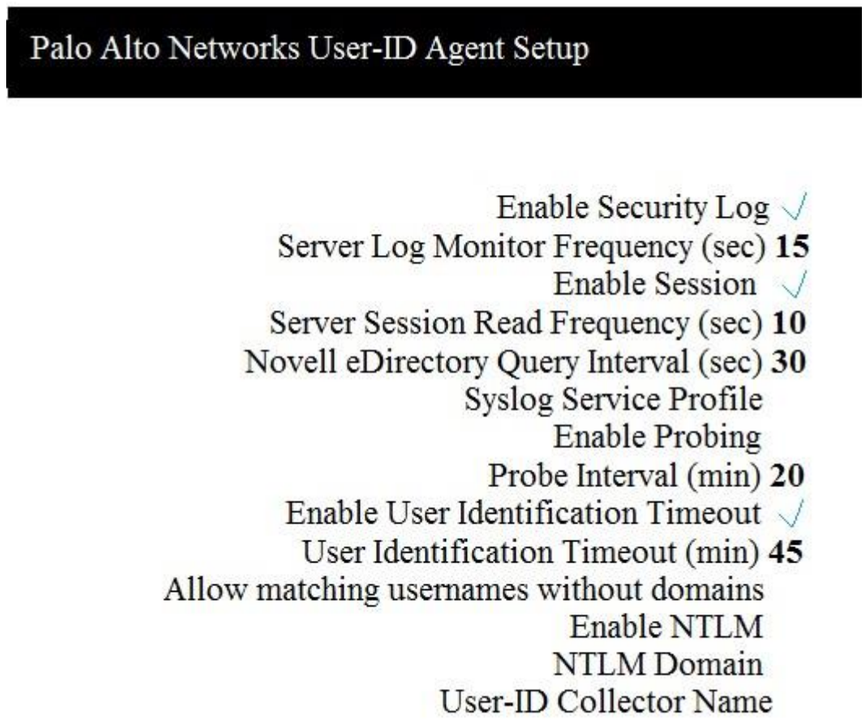
QUESTION 4 How many zones can an interface be assigned with a Palo Alto Networks firewall?

A. two
B. three
C. four
D. one

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface-help/network/network-zones/security-zone-overview

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



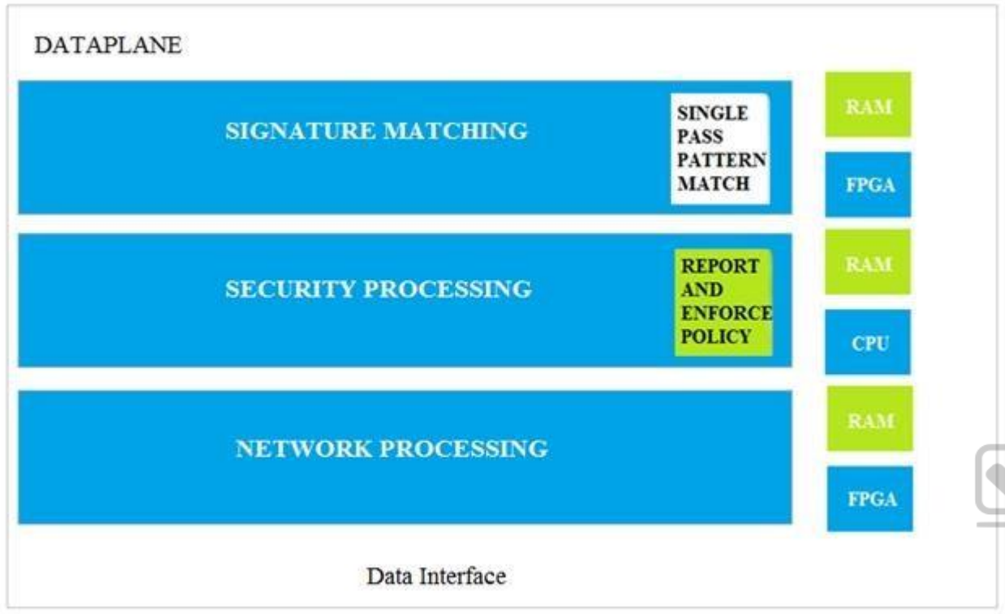
A. Enable Security Log
B. Server Log Monitor Frequency (sec)
C. Enable Session

D. Enable Probing

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-web-interface-help/user-identification/device-user-identification-user-mapping/enable-server-monitoring

QUESTION 6
Which data-plane processor layer of the graphic shown provides uniform matching for spyware and vulnerability exploits on a Palo Alto Networks Firewall?



A. Signature Matching
B. Network ProcessingC. Security Processing
D. Security Matching

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 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
Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-web-interface-help/objects/objects-application-filters

QUESTION 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

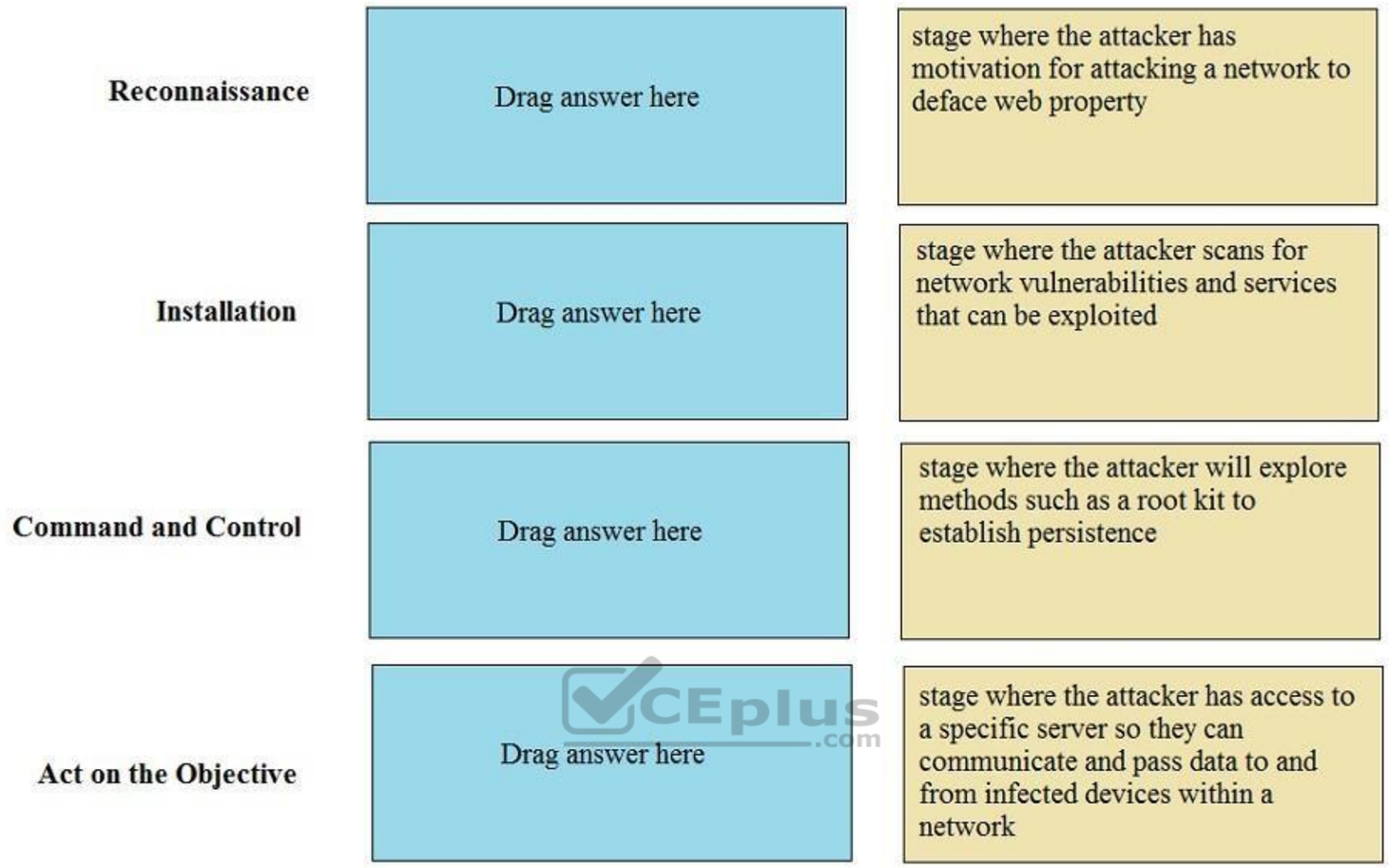
Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
DRAG DROP

Match the Cyber-Attack Lifecycle stage to its correct description.

Select and Place:



Correct Answer:

Reconnaissance	stage where the attacker scans for network vulnerabilities and services that can be exploited	stage where the attacker has motivation for attacking a network to deface web property
Installation	stage where the attacker will explore methods such as a root kit to establish persistence	stage where the attacker scans for network vulnerabilities and services that can be exploited
Command and Control	stage where the attacker has access to a specific server so they can communicate and pass data to and from infected devices within a network	stage where the attacker will explore methods such as a root kit to establish persistence
Act on the Objective	stage where the attacker has motivation for attacking a network to deface web property	stage where the attacker has access to a specific server so they can communicate and pass data to and from infected devices within a network

Section: (none)
Explanation

Explanation/Reference:

QUESTION 10 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: CD
Section: (none)
Explanation

Explanation/Reference:

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

A. Windows session monitoring via a domain controller
B. passive server monitoring using the Windows-based agent
C. Captive Portal
D. passive server monitoring using a PAN-OS integrated User-ID agent

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 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 data
C. The assessment, guided by an experienced sales engineer, helps determine the areas of greatest risk where you should focus prevention activitiesD. It provides a set of questionnaires that help uncover security risk prevention gaps across all areas of network and security architecture

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.paloaltonetworks.com/best-practices/8-1/data-center-best-practices/data-center-best-practice-security-policy/use-palo-alto-networks-assessment-and-review-tools

QUESTION 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**	**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:

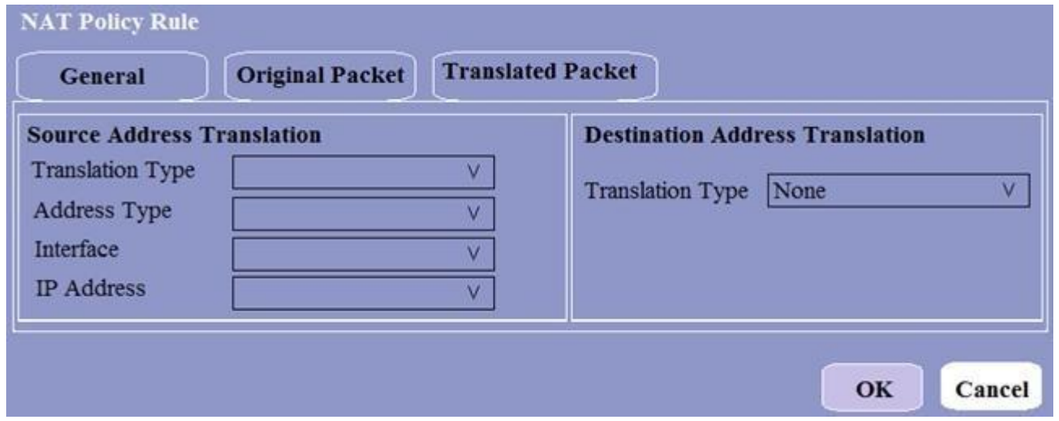
QUESTION 15 Complete the statement. A security profile can block or allow traffic.

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 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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
DRAG DROP

Order the steps needed to create a new security zone with a Palo Alto Networks firewall.

Select and Place:

Correct Answer:

Section: (none)
Explanation

Explanation/Reference:

QUESTION 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

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
Recently changes were made to the firewall to optimize the policies and the security team wants to see if those changes are helping. What is the quickest way to reset the hit counter to zero in all the security policy rules?

A. At the CLI enter the command reset rules and press Enter
B. Highlight a rule and use the **Reset Rule Hit Counter > Selected Rules** for each rule
C. Reboot the firewall
D. Use the **Reset Rule Hit Counter > All Rules** option

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface-help/policies/policies-security/creating-and-managing-policies

QUESTION 22 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
Section: (none)
Explanation
Explanation/Reference:

Reference: https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClV0CAK

QUESTION 23
Which User-ID agent would be appropriate in a network with multiple WAN links, limited network bandwidth, and limited firewall management plane resources?

A. Windows-based agent deployed on the internal network
B. PAN-OS integrated agent deployed on the internal network
C. Citrix terminal server deployed on the internal network
D. Windows-based agent deployed on each of the WAN Links

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
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 25
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 command-and-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 26
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 27 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. 1-4-3-2C. 3-1-2-4
D. 1-3-2-4

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
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 29
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:

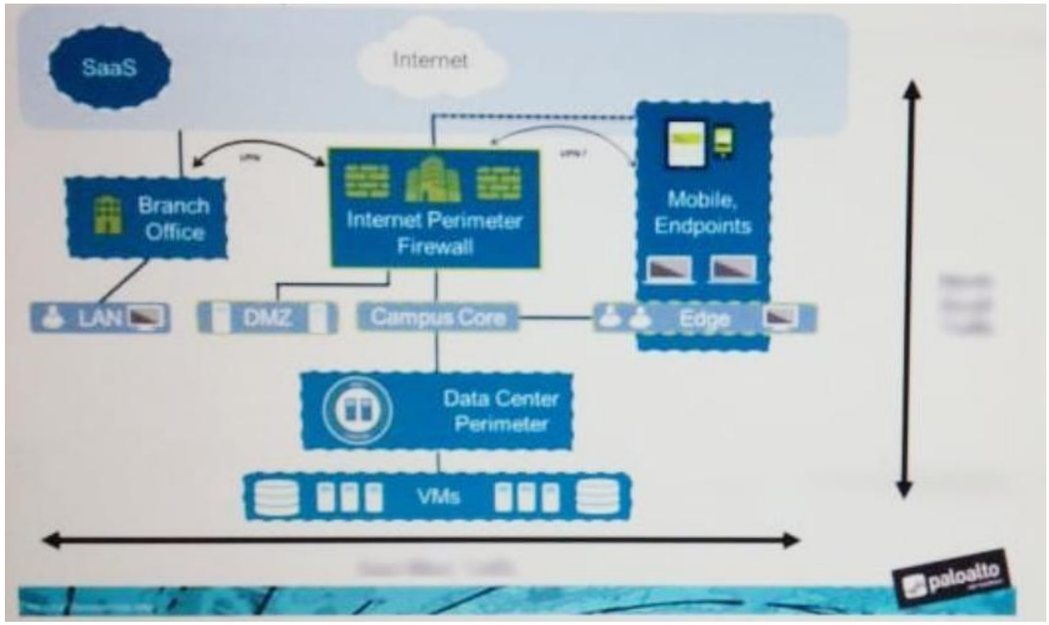
QUESTION 30
Which license must an Administrator acquire prior to downloading Antivirus Updates for use with the firewall?

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 31
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?

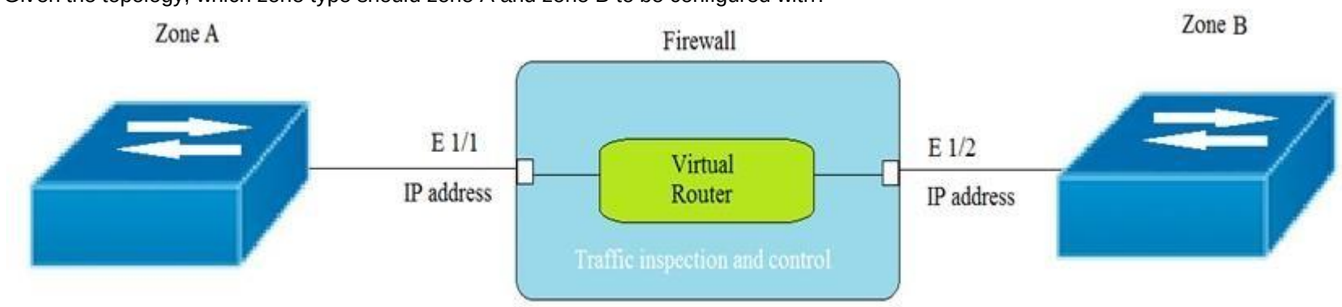


A. branch office traffic
B. north-south traffic
C. perimeter traffic
D. east-west traffic

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
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 33 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 34 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 35
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 36 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/administrative-privileges?PageSpeed=noscript

QUESTION 37 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 38
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 39
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
C. domain controller monitoring

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
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:

QUESTION 41
Given the image, which two options are true about the Security policy rules. (Choose two.)

				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

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 42 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

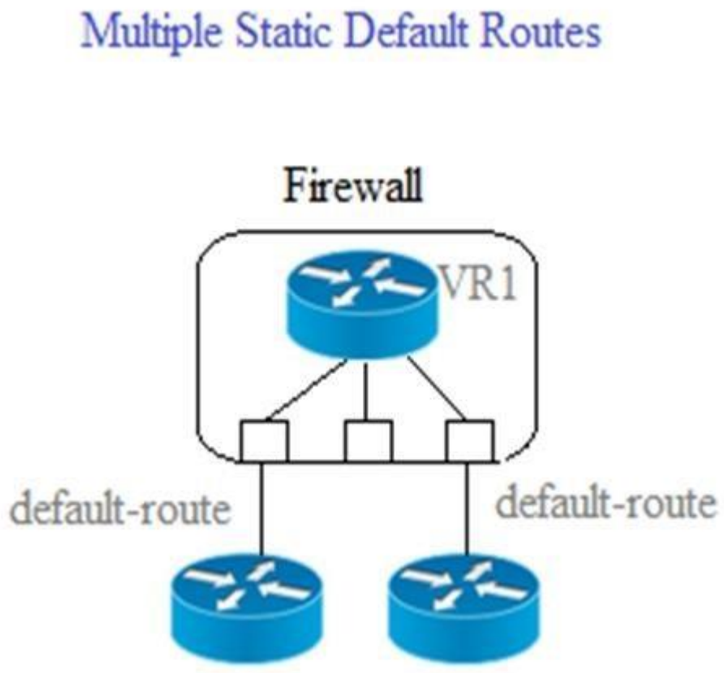
QUESTION 43
Which Palo Alto Networks firewall security platform provides network security for mobile endpoints by inspecting traffic deployed as internet gateways?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

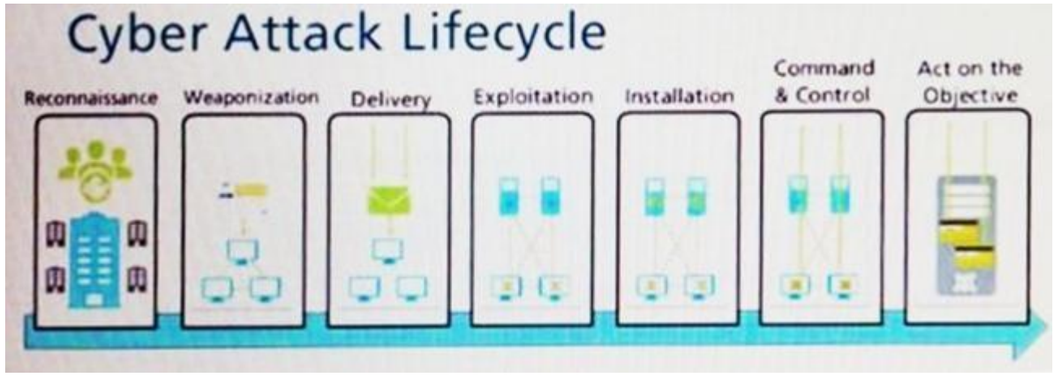
QUESTION 44
Given the scenario, which two statements are correct regarding multiple static default routes? (Choose two.)



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 45
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 46 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 47
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:

QUESTION 48
Which two Palo Alto Networks security management tools provide a consolidated creation of policies, centralized management and centralized threat intelligence. (Choose two.)

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

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49 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
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.paloaltonetworks.com/best-practices/8-1/data-center-best-practices/data-center-best-practice-security-policy/use-palo-alto-networks-assessment-and-review-tools

QUESTION 50
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
Section: (none)
Explanation

Explanation/Reference: