Number: PCNSA
Passing Score: 800
Time Limit: 120
File Version: 7.0

Exam Code: PCNSA
Exam Name: Palo Alto Networks Certified Network Security Administrator

Exam A

QUESTION 1
How does an administrator schedule an Applications and Threats dynamic update while delaying installation of the update for a certain amount of time?

A. Disable automatic updates during weekdays
B. Automatically "download and install" but with the "disable new applications" option used
C. Automatically "download only" and then install Applications and Threats later, after the administrator approves the update
D. Configure the option for "Threshold"

Correct Answer: D
Section:

QUESTION 2
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.
B. Data Filtering profile applied to outbound Security policy rules.
C. Antivirus profile applied to inbound Security policy rules.
D. Vulnerability Prote ction profile applied to outbound Security policy rules.

Correct Answer: C
Section:
Explanation:
Reference:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/security-profiles

QUESTION 3
URL categories can be used as match criteria on which two policy types? (Choose two.)

A. authentication
B. decryption
C. application override
D. NAT

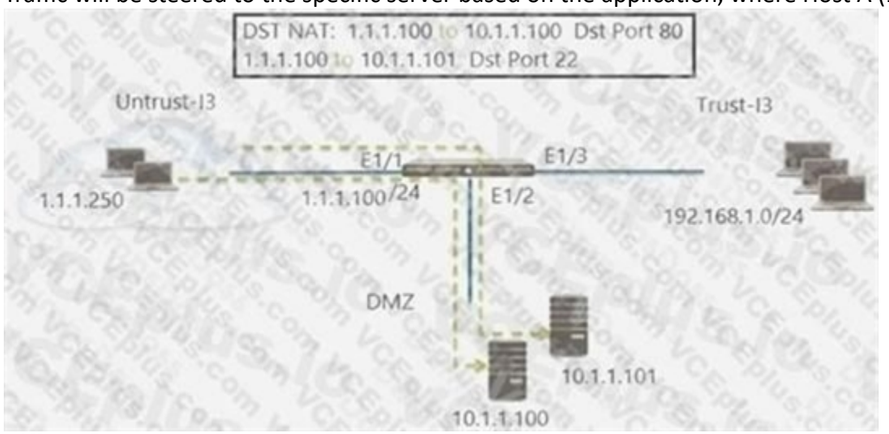
Correct Answer: A, B
Section:
Explanation:
Reference: https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/url-filtering/url-filteringconcepts/url-category-as-policy-match-criteria.html

QUESTION 4
Given the screenshot, what are two correct statements about the logged traffic? (Choose two.)

A. The web session was unsuccessfully decrypted.
B. The traffic was denied by security profile.
C. The traffic was denied by URL filtering.
D. The web session was decrypted.

Correct Answer: C, D
Section:

QUESTION 5
Refer to the exhibit. An administrator is using DNAT to map two servers to a single public IP address.
Traffic will be steered to the specific server based on the application, where Host A (10.1.1.100) receives HTTP traffic and Host B (10.1.1.101) receives SSH traffic.

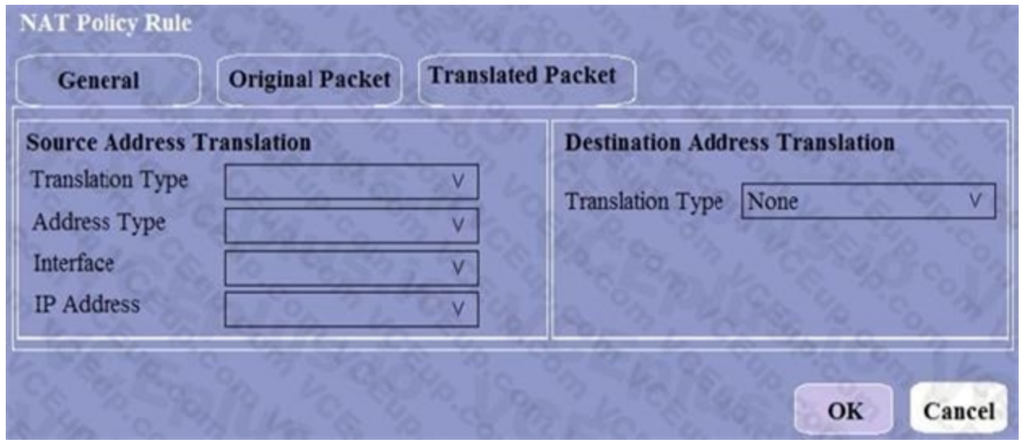


Which two Security policy rules will accomplish this configuration? (Choose two.)

A. Untrust (Any) to DMZ (1.1.1.100), ssh - Allow
B. Untrust (Any) to Untrust (10.1.1.1), web-browsing -Allow
C. Untrust (Any) to Untrust (10.1.1.1), ssh -Allow
D. Untrust (Any)to DMZ (10.1.1.100. 10.1.1.101), ssh, web-browsing-Allow
E. Untrust (Any) to DMZ (1.1.1.100), web-browsing - Allow

Correct Answer: A, E
Section:

QUESTION 6
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:

QUESTION 7
Which interface does not require a MAC or IP address?

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

Correct Answer: A
Section:

QUESTION 8
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:

QUESTION 9
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: A, D
Section:

QUESTION 10
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:
Explanation:
References:

QUESTION 11
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: B, C
Section:

QUESTION 12
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:
Explanation:
Another reason to choose the Windows agent over the integrated PAN-OS agent is to save processing cycles on the firewall's management plane.

QUESTION 13
Your company requires positive username attribution of every IP address used by wireless devices to support a new compliance requirement. You must collect IP ñto-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:

QUESTION 14
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: B, D
Section:
Explanation:
References:

QUESTION 15
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:

QUESTION 16
Identify the correct order to configure the PAN-OS integrated USER-ID agent.

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

F. 1-4-3-2
G. 3-1-2-4
H. 1-3-2-4

Correct Answer: D
Section:

QUESTION 17
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:

QUESTION 18
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:

QUESTION 19
Which prevention technique will prevent attacks based on packet count?

A. zone protection profile
B. URL filtering profile
C. antivirus profile
D. vulnerability profile

Correct Answer: A
Section:

QUESTION 20
Which interface type can use virtual routers and routing protocols?

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

Correct Answer: B
Section:

QUESTION 21
Which URL profiling action does not generate a log entry when a user attempts to access that URL?

A. Override
B. Allow
C. Block
D. Continue

Correct Answer: B
Section:
Explanation:
References:

QUESTION 22
An internal host wants to connect to servers of the internet through using source NAT.
Which policy is required to enable source NAT on the firewall?

A. NAT policy with source zone and destination zone specified
B. post-NAT policy with external source and any destination address
C. NAT policy with no source of destination zone selected
D. pre-NAT policy with external source and any destination address

Correct Answer: A
Section:

QUESTION 23
Which security profile will provide the best protection against ICMP floods, based on individual combinations of a packet`s source and destination IP address?

A. DoS protection
B. URL filtering
C. packet buffering
D. anti-spyware

Correct Answer: A
Section:

QUESTION 24
Which path in PAN-OS 10.0 displays the list of port-based security policy rules?

A. Policies> Security> Rule Usage> No App Specified
B. Policies> Security> Rule Usage> Port only specified
C. Policies> Security> Rule Usage> Port-based Rules
D. Policies> Security> Rule Usage> Unused Apps

Correct Answer: A
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/app-id/security-policy-ruleoptimization/migrate-port-based-to-app-id-based-security-policy-rules.html

QUESTION 25
Which two components are utilized within the Single-Pass Parallel Processing architecture on a Palo Alto Networks Firewall? (Choose two.)

A. Layer-ID
B. User-ID
C. QoS-ID
D. App-ID

Correct Answer: B, D
Section:

QUESTION 26
Which path is used to save and load a configuration with a Palo Alto Networks firewall?

A. Device>Setup>Services
B. Device>Setup>Management
C. Device>Setup>Operations
D. Device>Setup>Interfaces

Correct Answer: C
Section:

QUESTION 27
Which action related to App-ID updates will enable a security administrator to view the existing security policy rule that matches new application signatures?

A. Review Policies
B. Review Apps
C. Pre-analyze
D. Review App Matches

Correct Answer: A

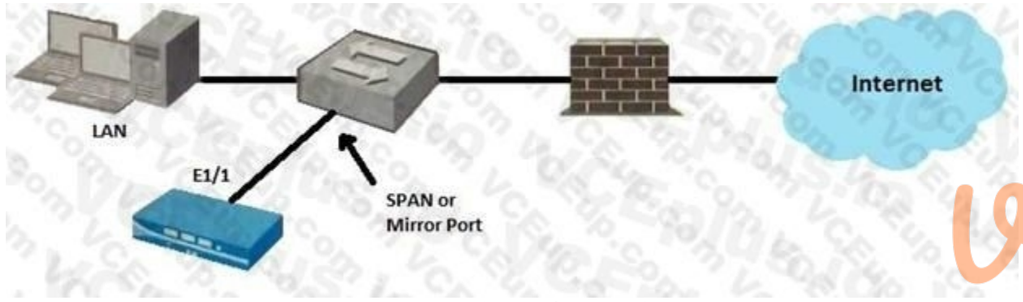
Section:
Explanation:
References:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/app-id/manage-new-app-idsintroduced-incontent-releases/review-new-app-id-impact-on- existing-policy-rules

QUESTION 28
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
Section:

QUESTION 29



Given the topology, which zone type should interface E1/1 be configured with?

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

Correct Answer: A
Section:

QUESTION 30
Which interface type is part of a Layer 3 zone with a Palo Alto Networks firewall?

A. Management
B. High Availability
C. Aggregate
D. Aggregation

Correct Answer: C
Section:

QUESTION 31

Which security policy rule would be needed to match traffic that passes between the Outside zone and Inside zone, but does not match traffic that passes within the zones?

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

Correct Answer: B
Section:

QUESTION 32
Based on the show security policy rule would match all FTP traffic from the inside zone to the outside zone?

A. internal-inside-dmz
B. engress outside
C. inside-portal
D. intercone-default

Correct Answer: B
Section:

QUESTION 33
Which the app-ID application will you need to allow in your security policy to use facebook-chat?

A. facebook-email
B. facebook-base
C. facebook
D. facebook-chat

Correct Answer: B, D
Section:

QUESTION 34
Which type security policy rule would match traffic flowing between the inside zone and outside zone within the inside zone and within the outside zone?

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

Correct Answer: B
Section:

QUESTION 35
Based on the screenshot presented which column contains the link that when clicked opens a window to display all applications matched to the policy rule?

A. Apps Allowed
B. Name
C. Apps Seen
D. Service

Correct Answer: C
Section:

QUESTION 36
In a security policy what is the quickest way to rest all policy rule hit counters to zero?

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

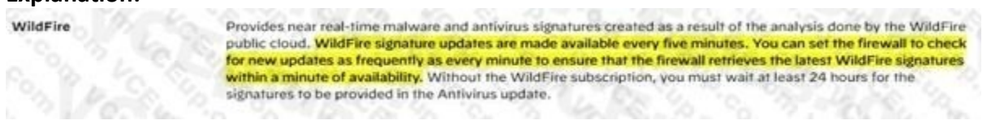
Correct Answer: C
Section:

QUESTION 37
What in the minimum frequency for which you can configure the firewall too check for new wildfire antivirus signatures?

A. every 5 minutes
B. every 1 minute
C. every 24 hours
D. every 30 minutes

Correct Answer: B

Section:
Explanation:



QUESTION 38
What do dynamic user groups you to do?

A. create a QoS policy that provides auto-remediation for anomalous user behavior and malicious activity
B. create a policy that provides auto-sizing for anomalous user behavior and malicious activity
C. create a policy that provides auto-remediation for anomalous user behavior and malicious activity
D. create a dynamic list of firewall administrators

Correct Answer: C
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/user-id-features/dynamicusergroups#:~:text=Dynamic%20user%20groups%20help%20you,activity%20while%20maintaining%20user%20visibility.

QUESTION 39
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
Section:

QUESTION 40
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
Section:
Explanation:
Reference:
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/user-id/map-ip-addresses-tousers/configureuser-mapping-using-the-windows-user-id- agent/configure-the-windows-based-userid-agent-for-usermapping.html

QUESTION 41
At which point in the app-ID update process can you determine if an existing policy rule is affected by an app-ID update?

A. after clicking Check New in the Dynamic Update window
B. after connecting the firewall configuration
C. after downloading the update
D. after installing the update

Correct Answer: A
Section:
Explanation:
Reference: https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interfacehelp/device/device-dynamicupdates

QUESTION 42
Which Palo Alto network security operating platform component provides consolidated policy creation and centralized management?

A. Prisma SaaS
B. Panorama
C. AutoFocus
D. GlobalProtect

Correct Answer: B
Section:

QUESTION 43
Which type firewall configuration contains in-progress configuration changes?

A. backup
B. running
C. candidate
D. committed

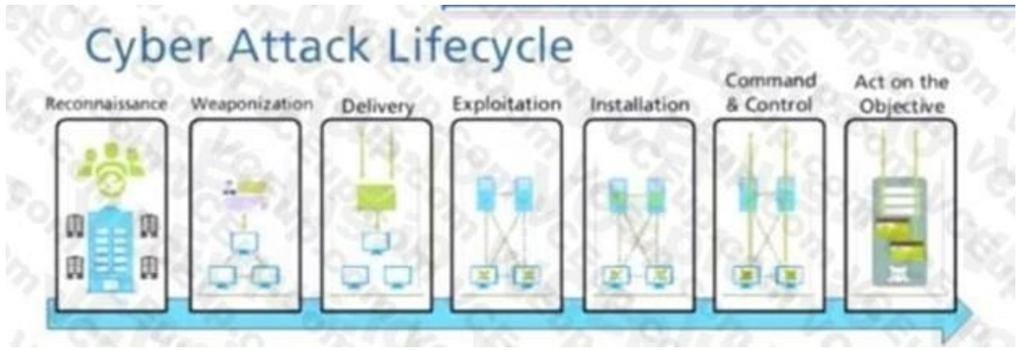
Correct Answer: C
Section:

QUESTION 44
Which link in the web interface enables a security administrator to view the security policy rules that match new application signatures?

A. Review Apps
B. Review App Matches
C. Pre-analyze
D. Review Policies

Correct Answer: D
Section:

QUESTION 45
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
Section:

QUESTION 46
How frequently can wildfire updates be made available to firewalls?

A. every 15 minutes
B. every 30 minutes
C. every 60 minutes
D. every 5 minutes

Correct Answer: D
Section:

QUESTION 47
Which data flow direction is protected in a zero trust firewall deployment that is not protected in a perimeter-only firewall deployment?

A. outbound
B. north south
C. inbound
D. east west

Correct Answer: D
Section:

QUESTION 48
How do you reset the hit count on a security policy rule?

A. First disable and then re-enable the rule.

B. Reboot the data-plane.
C. Select a Security policy rule, and then select Hit Count > Reset.
D. Type the CLI command reset hitcount <POLICY-NAME>.

Correct Answer: C
Section:

QUESTION 49
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
Section:

QUESTION 50
Based on the graphic which statement accurately describes the output shown in the server monitoring panel?

A. The User-ID agent is connected to a domain controller labeled lab-client.
B. The host lab-client has been found by the User-ID agent.
C. The host lab-client has been found by a domain controller.
D. The User-ID agent is connected to the firewall labeled lab-client.

Correct Answer: A
Section:

QUESTION 51

Which three configuration settings are required on a Palo Alto networks firewall management interface?

A. default gateway
B. netmask
C. IP address
D. hostname
E. auto-negotiation

Correct Answer: A, B, C
Section:
Explanation:
Reference:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClN7CAK

QUESTION 52
Which Palo Alto networks security operating platform service protects cloud-based application such as Dropbox and salesforce by monitoring permissions and shared and scanning files for Sensitive information?

A. Prisma SaaS
B. AutoFocus
C. Panorama
D. GlobalProtect

Correct Answer: A
Section:

QUESTION 53
Which statements is true regarding a Heatmap report?

A. When guided by authorized sales engineer, it helps determine te areas of greatest security risk.
B. It provides a percentage of adoption for each assessment area.
C. It runs only on firewall.
D. 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:
Explanation:
Reference: https://live.paloaltonetworks.com/t5/best-practice-assessment-blogs/the-best-practiceassessment-bpa-tool-for-ngfw-and-panorama/ba-p/248343

QUESTION 54
Starting with PAN_OS version 9.1 which new type of object is supported for use within the user field of a security policy rule?

A. local username
B. dynamic user group
C. remote username
D. static user group

Correct Answer: B

Section:

QUESTION 55
Which two statements are true for the DNS security service introduced in PAN-OS version 10.0?

A. It functions like PAN-DB and requires activation through the app portal.
B. It removes the 100K limit for DNS entries for the downloaded DNS updates.
C. IT eliminates the need for dynamic DNS updates.
D. IT is automatically enabled and configured.

Correct Answer: A, B
Section:

QUESTION 56
Which three statement describe the operation of Security Policy rules or Security Profiles? (Choose three)

A. Security policy rules inspect but do not block traffic.
B. Security Profile should be used only on allowed traffic.
C. Security Profile are attached to security policy rules.
D. Security Policy rules are attached to Security Profiles.
E. Security Policy rules can block or allow traffic.

Correct Answer: B, C, E
Section:

QUESTION 57
Based on the screenshot what is the purpose of the included groups?

	Name	Type	Source Zone	Source Address	Source User	Destination Zone	Destination Address	Application	Service	Action
1	allow-it	universal	inside	any	it	dmz	any	it-tools	application-default	Allow

A. They are only groups visible based on the firewall's credentials.
B. They are used to map usernames to group names.
C. They contain only the users you allow to manage the firewall.
D. They are groups that are imported from RADIUS authentication servers.

Correct Answer: B
Section:
Explanation:
Reference:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/user-id/map-users-to-groups.html

QUESTION 58
What is an advantage for using application tags?

A. They are helpful during the creation of new zones
B. They help with the design of IP address allocations in DHCP.

C. They help content updates automate policy updates
D. They help with the creation of interfaces

Correct Answer: C
Section:

QUESTION 59
Which operations are allowed when working with App-ID application tags?

A. Predefined tags may be deleted.
B. Predefined tags may be augmented by custom tags.
C. Predefined tags may be modified.
D. Predefined tags may be updated by WildFire dynamic updates.

Correct Answer: B
Section:

QUESTION 60
You need to allow users to access the officeñsuite application of their choice. How should you configure the firewall to allow access to any office-suite application?

A. Create an Application Group and add Office 365, Evernote Google Docs and Libre Office
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 office programs subcategory.
D. Create an Application Filter and name it Office Programs then filter on the business-systems category.

Correct Answer: C
Section:

QUESTION 61
An administrator wishes to follow best practices for logging traffic that traverses the firewall Which log setting is correct?

A. Disable all logging
B. Enable Log at Session End
C. Enable Log at Session Start
D. Enable Log at both Session Start and End

Correct Answer: B
Section:
Explanation:
Reference:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Clt5CAC

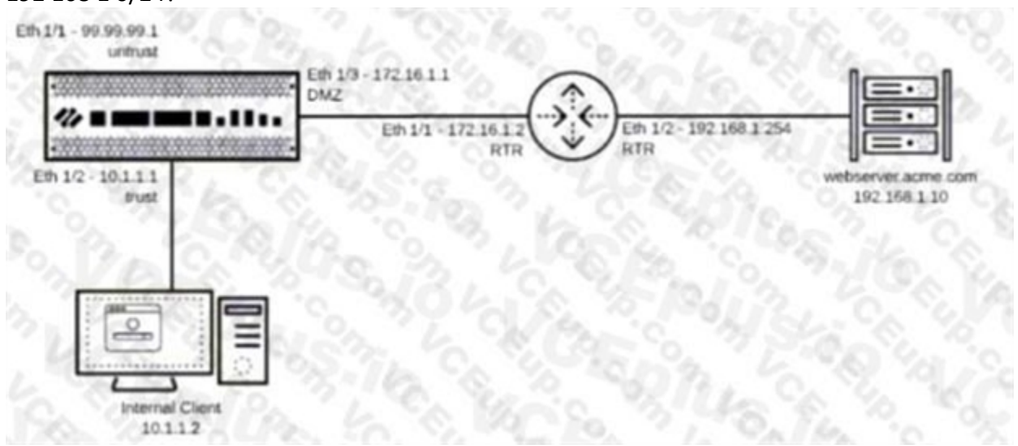
QUESTION 62
Assume that traffic matches a Security policy rule but the attached Security Profiles is configured to block matching traffic Which statement accurately describes how the firewall will apply an action to matching traffic?

A. If it is an allowed rule, then the Security Profile action is applied last
B. If it is a block rule then the Security policy rule action is applied last

C. If it is an allow rule then the Security policy rule is applied last
D. If it is a block rule then Security Profile action is applied last

Correct Answer: A
Section:

QUESTION 63
You have been tasked to configure access to a new web server located in the DMZ Based on the diagram what configuration changes are required in the NGFW virtual router to route traffic from the 10 1 1 0/24 network to 192 168 1 0/24?



A. Add a route with the destination of 192 168 1 0/24 using interface Eth 1/3 with a next-hop of 192.168 1.10
B. Add a route with the destination of 192 168 1 0/24 using interface Eth 1/2 with a next-hop of 172.16.1.2
C. Add a route with the destination of 192 168 1 0/24 using interface Eth 1/3 with a next-hop of 172.16.1.2
D. Add a route with the destination of 192 168 1 0/24 using interface Eth 1/3 with a next-hop of 192.168.1.254

Correct Answer: C
Section:

QUESTION 64
An administrator wants to prevent access to media content websites that are risky Which two URL categories should be combined in a custom URL category to accomplish this goal? (Choose two)

A. streaming-media
B. high-risk
C. recreation-and-hobbies
D. known-risk

Correct Answer: A, C
Section:

QUESTION 65
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
Section:

QUESTION 66
Given the cyber-attack lifecycle diagram identify the stage in which the attacker can run malicious code against a vulnerability in a targeted machine.

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

Correct Answer: A
Section:

QUESTION 67
Assume a custom URL Category Object of "NO-FILES" has been created to identify a specific website How can file uploading/downloading be restricted for the website while permitting general browsing access to that website?

A. Create a Security policy with a URL Filtering profile that references the site access setting of continue to NO-FILES
B. Create a Security policy with a URL Filtering profile that references the site access setting of block to NO-FILES
C. Create a Security policy that references NO-FILES as a URL Category qualifier, with an appropriate Data Filtering profile
D. Create a Security policy that references NO-FILES as a URL Category qualifier, with an appropriate File Blocking profile

Correct Answer: B
Section:

QUESTION 68
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+

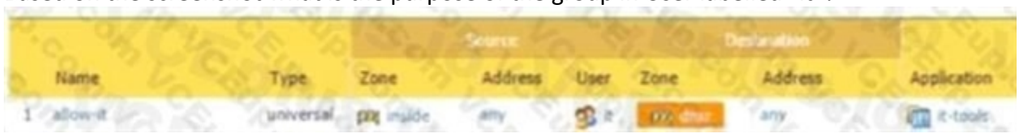
Correct Answer: A, B, D
Section:

QUESTION 69
Given the screenshot what two types of route is the administrator configuring? (Choose two)

A. default route
B. OSPF
C. BGP
D. static route

Correct Answer: A
Section:

QUESTION 70
Based on the screenshot what is the purpose of the group in User labelled "it"?



A. Allows users to access IT applications on all ports
B. Allows users in group "DMZ" lo access IT applications
C. Allows "any" users to access servers in the DMZ zone
D. Allows users in group "it" to access IT applications

Correct Answer: D

Section:

QUESTION 71
Which dynamic update type includes updated anti-spyware signatures?

A. Applications and Threats
B. GlobalProtect Data File
C. Antivirus
D. PAN-DB

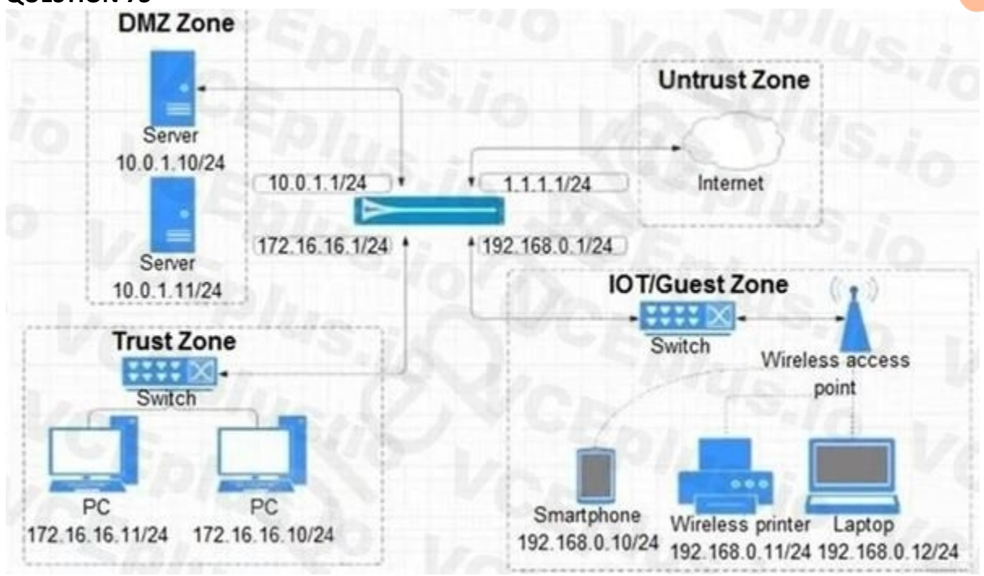
Correct Answer: A
Section:

QUESTION 72
Which URL Filtering Profile action does not generate a log entry when a user attempts to access a URL?

A. override
B. allow
C. block
D. continue

Correct Answer: B
Section:

QUESTION 73



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.

B.

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE		
03-A	none	universal	OT-Guest Trust	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	app

C.

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE		
04-A	none	universal	OT-Guest Trust	172.16.16.0/24 192.168.0.0/24	any	any	DMZ Untrust	any	any	ssh ssl web-browsing	app

D.

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE		
01-A	none	universal	OT-Guest Trust	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	app

E.

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE		
02-A	none	universal	OT-Guest Trust	172.16.18.0/24 192.168.0.0/24	any	any	DMZ Untrust	any	any	ssh ssl web-browsing	app

Correct Answer: B
Section:

QUESTION 74
Which action results in the firewall blocking network traffic without notifying the sender?

A. Deny
B. No notification
C. Drop
D. Reset Client

Correct Answer: C
Section:

QUESTION 75
Which type of profile must be applied to the Security policy rule to protect against buffer overflows illegal code execution and other attempts to exploit system flaws''

A. anti-spyware
B. URL filtering
C. vulnerability protection
D. file blocking

Correct Answer: C
Section:
Explanation:
Reference: https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interfacehelp/objects/objects-security-profiles-vulnerability-protection.html

QUESTION 76
An administrator is reviewing another administrator s Security policy log settings Which log setting configuration is consistent with best practices tor normal traffic?

A. Log at Session Start and Log at Session End both enabled
B. Log at Session Start disabled Log at Session End enabled
C. Log at Session Start enabled Log at Session End disabled
D. Log at Session Start and Log at Session End both disabled

Correct Answer: B
Section:

QUESTION 77
Which URL Filtering profile action would you set to allow users the option to access a site only if they provide a URL admin password?

A. override
B. authorization
C. authentication
D. continue

Correct Answer: B
Section:
Explanation:
Reference:
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/url-filtering/url-filtering-concepts/urlfilteringprofile-actions.html

QUESTION 78
Selecting the option to revert firewall changes will replace what settings?

A. the running configuration with settings from the candidate configuration
B. the device state with settings from another configuration
C. the candidate configuration with settings from the running configuration
D. dynamic update scheduler settings

Correct Answer: C
Section:

QUESTION 79
What is considered best practice with regards to committing configuration changes?

A. Disable the automatic commit feature that prioritizes content database installations before committing
B. Validate configuration changes prior to committing
C. Wait until all running and pending jobs are finished before committing
D. Export configuration after each single configuration change performed

Correct Answer: A
Section:

QUESTION 80
An administrator wants to prevent users from submitting corporate credentials in a phishing attack.
Which Security profile should be applied?

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

Correct Answer: B
Section:

QUESTION 81
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
Section:

QUESTION 82
Which two firewall components enable you to configure SYN flood protection thresholds? (Choose two.)

A. QoS profile
B. DoS Protection profile
C. Zone Protection profile
D. DoS Protection policy

Correct Answer: B, C
Section:
Explanation:
Reference:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/security-profiles

You can add security profiles that are commonly applied together to Create a Security Profile Group; this set of profiles can be treated as a unit and added to security policies in one step (or included in security policies by default, if you choose to set up a default security profile group).

PROFILE TYPE	DESCRIPTION
Antivirus Profiles	Antivirus profiles protect against viruses, worms, and trojans as well as spyware downloads. Using a stream-based malware prevention engine, which inspects traffic the moment the first packet is received, the Palo Alto Networks antivirus solution can provide protection for clients without significantly impacting the performance of the firewall. This profile scans for a wide variety of malware in executables, PDF files, HTML and JavaScript viruses, including support for scanning inside compressed files and data encoding schemes. If you have enabled Decryption on the firewall, the profile also enables scanning of decrypted content. The default profile inspects all of the listed protocol decoders for viruses, and generates alerts for SMTP, IMAP, and POP3 protocols while blocking for FTP, HTTP, and SMB protocols. You can configure the action for a decoder or Antivirus signature and specify how the firewall responds to a threat event: • **Default**—For each threat signature and Antivirus signature that is defined by Palo Alto Networks, a default action is specified internally. Typically, the default action is an alert or a

QUESTION 83
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
Section:
Explanation:
Reference:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-new-features/app-id-features/policyoptimizer.html

QUESTION 84
What does an administrator use to validate whether a session is matching an expected NAT policy?

A. system log
B. test command
C. threat log

D. config audit

Correct Answer: B
Section:
Explanation:
Reference:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClQSCA0

QUESTION 85
What is the purpose of the automated commit recovery feature?

A. It reverts the Panorama configuration.
B. It causes HA synchronization to occur automatically between the HA peers after a push from Panorama.
C. It reverts the firewall configuration if the firewall recognizes a loss of connectivity to Panorama after the change.
D. It generates a config log after the Panorama configuration successfully reverts to the last running configuration.

Correct Answer: C
Section:
Explanation:
Reference: https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/administerpanorama/enable-automated-commit-recovery.html

QUESTION 86
According to the best practices for mission critical devices, what is the recommended interval for antivirus updates?

A. by minute
B. hourly
C. daily
D. weekly

Correct Answer: C
Section:
Explanation:
Reference: https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/threat-prevention/bestpractices-for-content-and-threat-content-updates/best-practices-mission-critical.html

QUESTION 87
Which Security policy match condition would an administrator use to block traffic from IP addresses on the Palo Alto Networks EDL of Known Malicious IP Addresses list?

A. destination address
B. source address
C. destination zone
D. source zone

Correct Answer: B
Section:
Explanation:
Reference: https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/use-an-externaldynamic-list-in-policy/external-dynamic-list.html

QUESTION 88

Based on the graphic, what is the purpose of the SSL/TLS Service profile configuration option?


General Settings
Hostname
Domain
Accept DHCP server provided Hostname
Accept DHCP server provided Domain
Login Banner
Force Admins to Acknowledge Login Banner
SSL/TLS Service Profile
None
Time Zone
None
Locale
English
Date
Time
Latitude
Longitude
Automatically Acquire Commit Lock
Certificate Expiration Check
Use Hypervisor Assigned MAC Addresses
GTP Security
SCTP Security
Policy Rule Hit Count
OK
Cancel

A. It defines the SSUTLS encryption strength used to protect the management interface.
B. It defines the CA certificate used to verify the client's browser.
C. It defines the certificate to send to the client's browser from the management interface.
D. It defines the firewall's global SSL/TLS timeout values.

Correct Answer: C
Section:
Explanation:
Reference:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClFGCA0

QUESTION 89
An administrator is troubleshooting an issue with traffic that matches the intrazone-default rule, which is set to default configuration.
What should the administrator do?

A. change the logging action on the rule
B. review the System Log
C. refresh the Traffic Log
D. tune your Traffic Log filter to include the dates

Correct Answer: A
Section:

QUESTION 90
When is the content inspection performed in the packet flow process?

A. after the application has been identified
B. after the SSL Proxy re-encrypts the packet
C. before the packet forwarding process
D. before session lookup

Correct Answer: A
Section:
Explanation:
Reference:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClVHCA0

QUESTION 91
During the App-ID update process, what should you click on to confirm whether an existing policy rule is affected by an App-ID update?

A. check now
B. review policies
C. test policy match
D. download

Correct Answer: B

Section:
Explanation:
Reference: https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/app-id/manage-new-appids-introduced-in-content-releases/review-new-app-id-impact-on-existing-policy-rules

QUESTION 92
When creating a custom URL category object, which is a valid type?

A. domain match
B. host names
C. wildcard
D. category match

Correct Answer: D
Section:
Explanation:
Reference: https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interfacehelp/objects/objects-custom-objects-url-category.html

QUESTION 93
When HTTPS for management and GlobalProtect are enabled on the same interface, which TCP portis used for management access?

A. 80
B. 8443
C. 4443
D. 443

Correct Answer: C
Section:
Explanation:
Reference:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Cm8SCAS#:~:text=Details,using%20https%20on%20port%204443

QUESTION 94
What two authentication methods on the Palo Alto Networks firewalls support authentication and authorization for role-based access control? (Choose two.)

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

Correct Answer: A, B
Section:
Explanation:
Reference: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/firewalladministration/manage-firewall-administrators/administrative-authentication.html

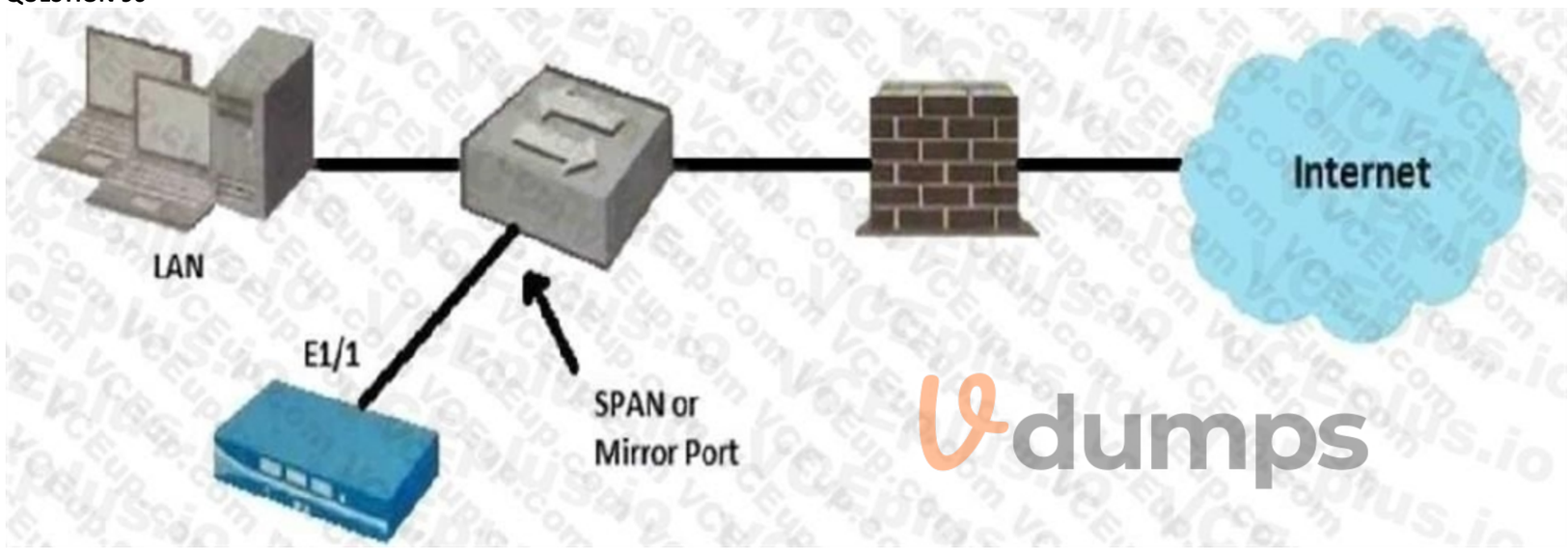
QUESTION 95
Choose the option that correctly completes this statement. A Security Profile can block or allow traffic _____.

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.

Correct Answer: B
Section:
Explanation:
Reference:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/security-policy.html

QUESTION 96



Given the topology, which zone type should you configure for firewall interface E1/1?

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

Correct Answer: A
Section:

QUESTION 97
Which two features can be used to tag a username so that it is included in a dynamic user group?
(Choose two.)

A. GlobalProtect agent
B. XML API
C. User-ID Windows-based agent
D. log forwarding auto-tagging

Correct Answer: B, C

Section:

QUESTION 98
For the firewall to use Active Directory to authenticate users, which Server Profile is required in the Authentication Profile?

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

Correct Answer: C
Section:
Explanation:
Reference:
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/authentication/configure-anauthenticationprofile-and-sequence

QUESTION 99
Which type of security policy rule will match traffic that flows between the Outside zone and inside zone, but would not match traffic that flows within the zones?

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

Correct Answer: C
Section:
Explanation:
Reference:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/software-and-contentupdates/dynamiccontentupdates.html#:~:text=WildFire%20signature%20updates%20are%20made,within%20a%20minute%20of%20availability

QUESTION 100
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
Section:
Explanation:
Reference:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/use-an-external-dynamic-listin-policy/builtin-edls.html#:~:text=With%20an%

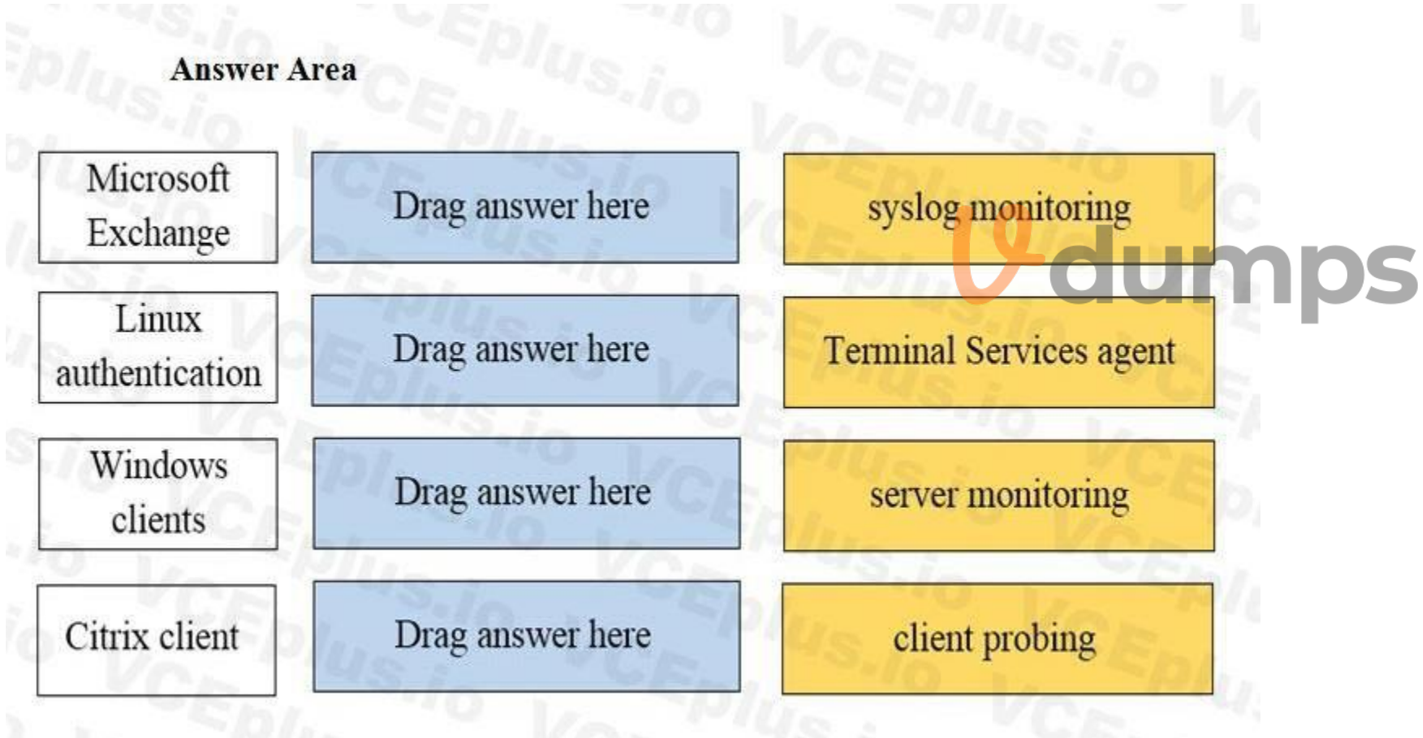
QUESTION 101
Which component is a building block in a Security policy rule?

A. decryption profile
B. destination interface
C. timeout (min)
D. application

Correct Answer: D
Section:
Explanation:
Reference:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/policies/policiessecurity/buildingblocks-in-a-security-policy-rule.html

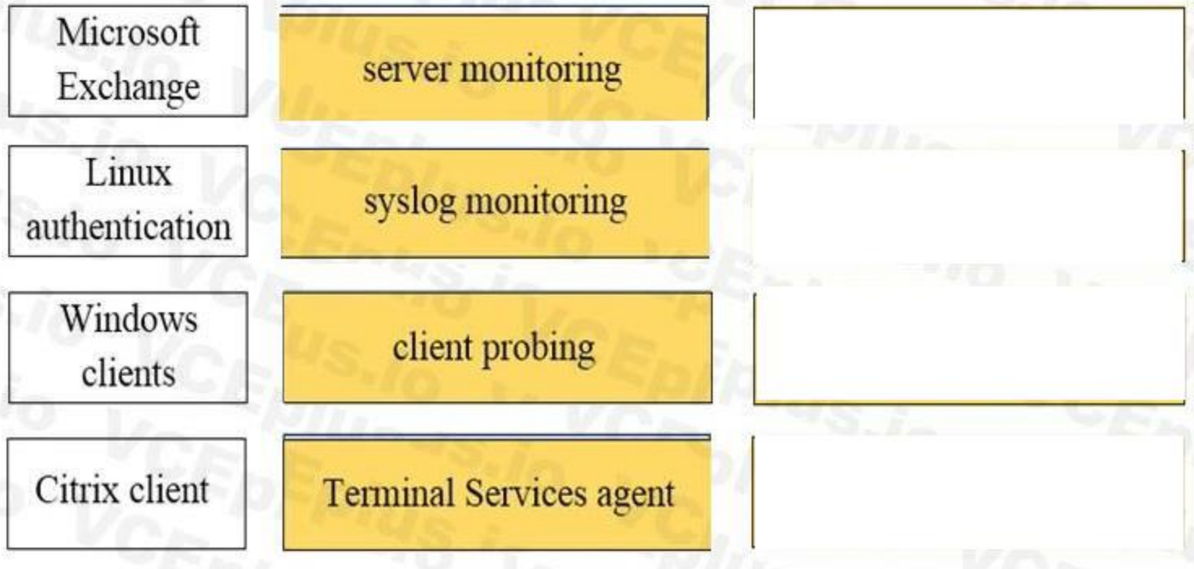
QUESTION 102
DRAG DROP
Match the network device with the correct User-ID technology.

Select and Place:



Correct Answer:

Answer Area

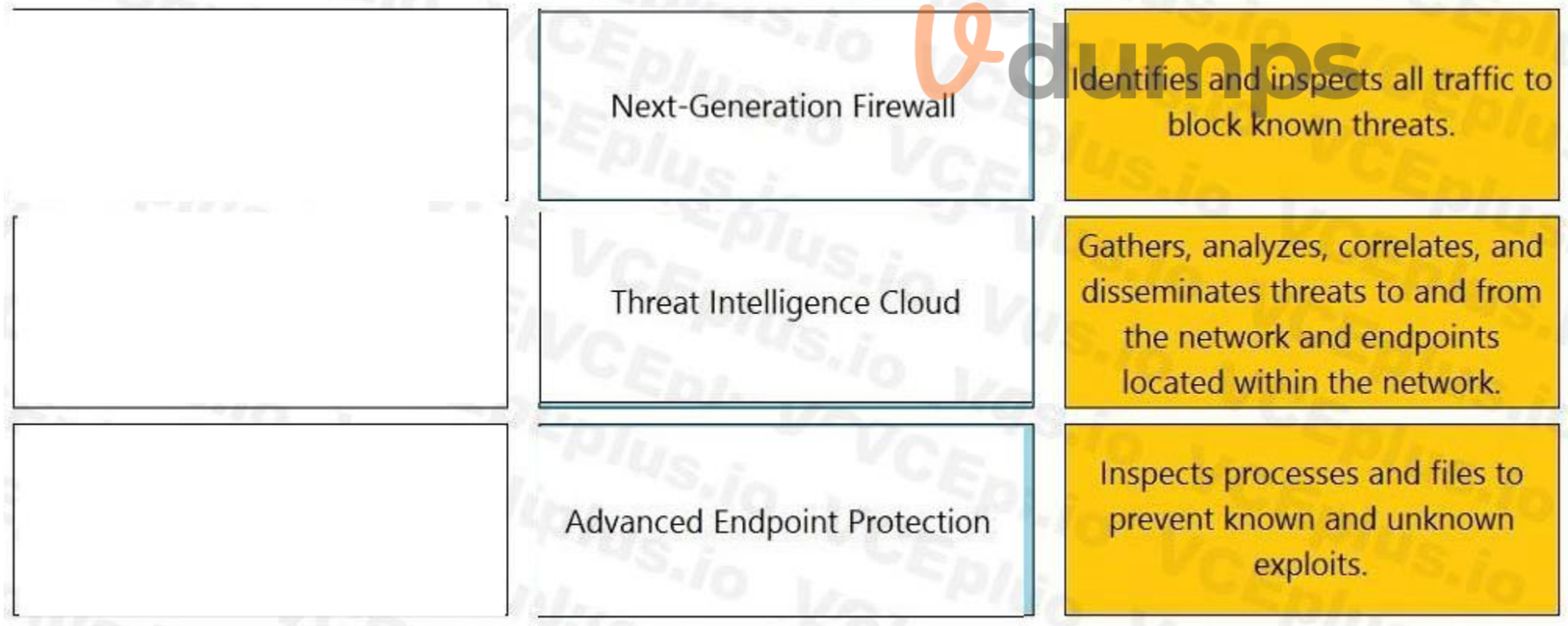


Section:
Explanation:

QUESTION 103
DRAG DROP
Match each feature to the DoS Protection Policy or the DoS Protection Profile.

Select and Place:

Correct Answer:

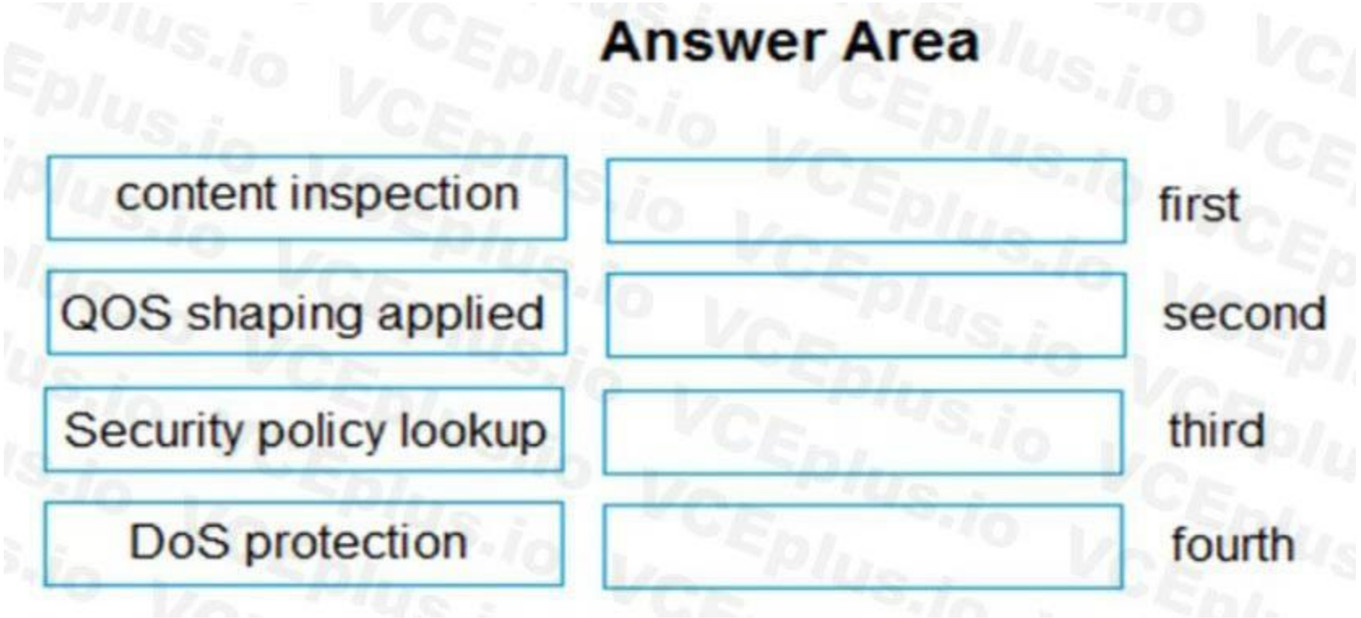


Section:
Explanation:

QUESTION 104
DRAG DROP

Place the following steps in the packet processing order of operations from first to last.

Select and Place:



Correct Answer:

Section:
Explanation:
Reference: https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClVHCA0

QUESTION 105
DRAG DROP

Place the steps in the correct packet-processing order of operations.

Select and Place:

Correct Answer:

Section:
Explanation:

QUESTION 106
What are three valid ways to map an IP address to a username? (Choose three.)

A. using the XML API
B. DHCP Relay logs
C. a user connecting into a GlobalProtect gateway using a GlobalProtect Agent
D. usernames inserted inside HTTP Headers
E. WildFire verdict reports

Correct Answer: A, C, D
Section:

QUESTION 107

Which object would an administrator create to enable access to all applications in the officeprograms subcategory?

A. application filter
B. URL category
C. HIP profile
D. application group

Correct Answer: A
Section:

QUESTION 108
An administrator would like to create a URL Filtering log entry when users browse to any gambling website. What combination of Security policy and Security profile actions is correct?

A. Security policy = drop, Gambling category in URL profile = allow
B. Security policy = deny. Gambling category in URL profile = block
C. Security policy = allow, Gambling category in URL profile = alert
D. Security policy = allow. Gambling category in URL profile = allow

Correct Answer: C
Section:

QUESTION 109
Which statement is true regarding NAT rules?

A. Static NAT rules have precedence over other forms of NAT.
B. Translation of the IP address and port occurs before security processing.
C. NAT rules are processed in order from top to bottom.
D. Firewall supports NAT on Layer 3 interfaces only.

Correct Answer: C
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/networking/nat/nat-policy-rules/nat-policy-overview

QUESTION 110
After making multiple changes to the candidate configuration of a firewall, the administrator would like to start over with a candidate configuration that matches the running configuration.
Which command in Device > Setup > Operations would provide the most operationally efficient way to accomplish this?

A. Import named config snapshot
B. Load named configuration snapshot
C. Revert to running configuration
D. Revert to last saved configuration

Correct Answer: C
Section:

QUESTION 111

An administrator is reviewing the Security policy rules shown in the screenshot below.
Which statement is correct about the information displayed?

A. Eleven rules use the "Infrastructure* tag.
B. The view Rulebase as Groups is checked.
C. There are seven Security policy rules on this firewall.
D. Highlight Unused Rules is checked.

Correct Answer: B
Section:

QUESTION 112
What are the two default behaviors for the intrazone-default policy? (Choose two.)

A. Allow
B. Logging disabled
C. Log at Session End
D. Deny

Correct Answer: A, B
Section:

QUESTION 113
What are two valid selections within an Antivirus profile? (Choose two.)

A. deny
B. drop
C. default
D. block-ip

Correct Answer: B, C
Section:

QUESTION 114
An administrator wants to create a NAT policy to allow multiple source IP addresses to be translated to the same public IP address. What is the most appropriate NAT policy to achieve this?

A. Dynamic IP and Port
B. Dynamic IP
C. Static IP
D. Destination

Correct Answer: A
Section:

QUESTION 115
Which action can be set in a URL Filtering Security profile to provide users temporary access to all websites in a given category using a provided password?

A. exclude
B. continue
C. hold
D. override

Correct Answer: D
Section:
Explanation:
The user will see a response page indicating that a password is required to allow access to websites inthe given category. With this option, the security administrator or help-desk person would provide apassword granting temporary access to all websites in the given category. A log entry is generated in theURL Filtering log. The Override webpage doesn't display properly on client systems configured to use aproxy server.

QUESTION 116
What is a function of application tags?

A. creation of new zones
B. application prioritization
C. automated referenced applications in a policy
D. IP address allocations in DHCP

Correct Answer: C
Section:

QUESTION 117
What are three Palo Alto Networks best practices when implementing the DNS Security Service?
(Choose three.)

A. Implement a threat intel program.
B. Configure a URL Filtering profile.
C. Train your staff to be security aware.
D. Rely on a DNS resolver.

E. Plan for mobile-employee risk

Correct Answer: A, B, D
Section:

QUESTION 118
An administrator is investigating a log entry for a session that is allowed and has the end reason of aged-out. Which two fields could help in determining if this is normal? (Choose two.)

A. Packets sent/received
B. IP Protocol
C. Action
D. Decrypted

Correct Answer: B, D
Section:

QUESTION 119
What does an application filter help you to do?

A. It dynamically provides application statistics based on network, threat, and blocked activity,
B. It dynamically filters applications based on critical, high, medium, low. or informational severity.
C. It dynamically groups applications based on application attributes such as category and subcategory.
D. It dynamically shapes defined application traffic based on active sessions and bandwidth usage.

Correct Answer: C
Section:

QUESTION 120
Prior to a maintenance-window activity, the administrator would like to make a backup of only the running configuration to an external location. What command in Device > Setup > Operations would provide the most operationally efficient way to achieve this outcome?

A. save named configuration snapshot
B. export device state
C. export named configuration snapshot
D. save candidate config

Correct Answer: A
Section:

QUESTION 121
Your company is highly concerned with their Intellectual property being accessed by unauthorized resources. There is a mature process to store and include metadata tags for all confidential documents.
Which Security profile can further ensure that these documents do not exit the corporate network?

A. File Blocking
B. Data Filtering
C. Anti-Spyware
D. URL Filtering

Correct Answer: B
Section:

QUESTION 122
An administrator wants to create a No-NAT rule to exempt a flow from the default NAT rule. What is the best way to do this?

A. Create a Security policy rule to allow the traffic.
B. Create a new NAT rule with the correct parameters and leave the translation type as None
C. Create a static NAT rule with an application override.
D. Create a static NAT rule translating to the destination interface.

Correct Answer: B
Section:

QUESTION 123
When creating a Panorama administrator type of Device Group and Template Admin, which two things must you create first? (Choose two.)

A. password profile
B. access domain
C. admin rote
D. server profile

Correct Answer: C, D
Section:

QUESTION 124
An administrator is troubleshooting traffic that should match the interzone-default rule. However, the administrator doesn't see this traffic in the traffic logs on the firewall. The interzone-default was never changed from its default configuration.
Why doesn't the administrator see the traffic?

A. Traffic is being denied on the interzone-default policy.
B. The Log Forwarding profile is not configured on the policy.
C. The interzone-default policy is disabled by default
D. Logging on the interzone-default policy is disabled

Correct Answer: D
Section:

QUESTION 125
An administrator is configuring a NAT rule
At a minimum, which three forms of information are required? (Choose three.)

A. name
B. source zone
C. destination interface
D. destination address
E. destination zone

Correct Answer: B, D, E
Section:

QUESTION 126
Which type of address object is www.paloaltonetworks.com?

A. IP range
B. IP netmask
C. named address
D. FQDN

Correct Answer: D
Section:

QUESTION 127
What are three characteristics of the Palo Alto Networks DNS Security service? (Choose three.)

A. It uses techniques such as DGA.DNS tunneling detection and machine learning.
B. It requires a valid Threat Prevention license.
C. It enables users to access real-time protections using advanced predictive analytics.
D. It requires a valid URL Filtering license.
E. It requires an active subscription to a third-party DNS Security service.

Correct Answer: A, B, C
Section:

QUESTION 128
What are the requirements for using Palo Alto Networks EDL Hosting Sen/ice?

A. any supported Palo Alto Networks firewall or Prisma Access firewall
B. an additional subscription free of charge
C. a firewall device running with a minimum version of PAN-OS 10.1
D. an additional paid subscription

Correct Answer: A
Section:

QUESTION 129
An administrator would like to block access to a web server, while also preserving resources and minimizing half-open sockets. What are two security policy actions the administrator can select? (Choose two.)

A. Reset server
B. Reset both
C. Drop
D. Deny

Correct Answer: A, C

Section:

QUESTION 130
An administrator would like to apply a more restrictive Security profile to traffic for file sharing applications. The administrator does not want to update the Security policy or object when new applications are released.
Which object should the administrator use as a match condition in the Security policy?

A. the Content Delivery Networks URL category
B. the Online Storage and Backup URL category
C. an application group containing all of the file-sharing App-IDs reported in the traffic logs
D. an application filter for applications whose subcategory is file-sharing

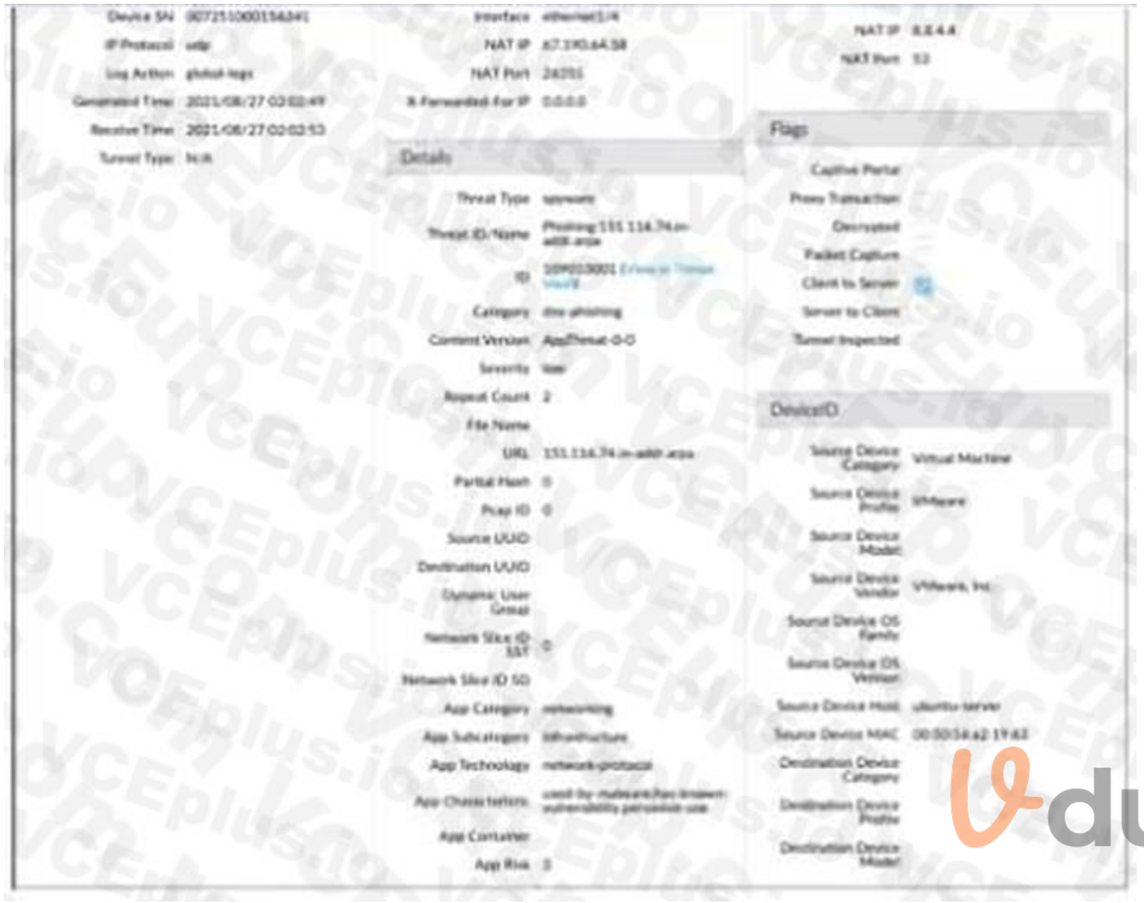
Correct Answer: D
Section:

QUESTION 131
A network administrator is required to use a dynamic routing protocol for network connectivity.
Which three dynamic routing protocols are supported by the NGFW Virtual Router for this purpose?
(Choose three.)

A. RIP
B. OSPF
C. IS-IS
D. EIGRP
E. BGP

Correct Answer: A, B, E
Section:

QUESTION 132
Given the detailed log information above, what was the result of the firewall traffic inspection?



A. It was blocked by the Vulnerability Protection profile action.
B. It was blocked by the Anti-Virus Security profile action.
C. It was blocked by the Anti-Spyware Profile action.
D. It was blocked by the Security policy action.

Correct Answer: C
Section:

QUESTION 133
Which three interface deployment methods can be used to block traffic flowing through the Palo Alto Networks firewall? (Choose three.)

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

Correct Answer: B, D, E
Section:

QUESTION 134
An administrator would like to protect against inbound threats such as buffer overflows and illegal code execution.
Which Security profile should be used?

A. Antivirus
B. URL filtering
C. Anti-spyware
D. Vulnerability protection

Correct Answer: C
Section:

QUESTION 135
Which statement best describes a common use of Policy Optimizer?

A. Policy Optimizer on a VM-50 firewall can display which Layer 7 App-ID Security policies have unused applications.
B. Policy Optimizer can add or change a Log Forwarding profile for each Security policy selected.
C. Policy Optimizer can display which Security policies have not been used in the last 90 days.
D. Policy Optimizer can be used on a schedule to automatically create a disabled Layer 7 App-ID Security policy for every Layer 4 policy that exists. Admins can then manually enable policies they want to keep and delete ones they want to remove.

Correct Answer: C
Section:

QUESTION 136
Which rule type is appropriate for matching traffic occurring within a specified zone?

A. Interzone
B. Universal
C. Intrazone
D. Shadowed

Correct Answer: C
Section:

QUESTION 137
What is a recommended consideration when deploying content updates to the firewall from Panorama?

A. Content updates for firewall A/P HA pairs can only be pushed to the active firewall.
B. Content updates for firewall A/A HA pairs need a defined master device.
C. Before deploying content updates, always check content release version compatibility.
D. After deploying content updates, perform a commit and push to Panorama.

Correct Answer: C
Section:

QUESTION 138

Which Security policy action will message a user's browser thai their web session has been terminated?

A. Reset server
B. Deny
C. Drop
D. Reset client

Correct Answer: B
Section:

QUESTION 139
An administrator configured a Security policy rule with an Antivirus Security profile. The administrator did not change the action (or the profile. If a virus gets detected, how wilt the firewall handle the traffic?

A. It allows the traffic because the profile was not set to explicitly deny the traffic.
B. It drops the traffic because the profile was not set to explicitly allow the traffic.
C. It uses the default action assigned to the virus signature.
D. It allows the traffic but generates an entry in the Threat logs.

Correct Answer: B
Section:

QUESTION 140
Selecting the option to revert firewall changes will replace what settings?

A. The running configuration with settings from the candidate configuration
B. The candidate configuration with settings from the running configuration
C. The device state with settings from another configuration
D. Dynamic update scheduler settings

Correct Answer: A
Section:

QUESTION 141
An administrator is updating Security policy to align with best practices.
Which Policy Optimizer feature is shown in the screenshot below?

	NAME	SERVICE	TRAFFIC (BYTES, 30 DAYS)	App Usage				MODIFIED	CREATED
				APPS ALLOWED	APPS SEEN	DAYS WITH NO NEW APPS	COMPARE		
55	Unexpected Traffic	application-default	1.7T	any	142	258	Compare	2022-01-06 18:30:02	2020-11-16
25	Outbound-Trust2	application-default	6.3G	any	26	447	Compare	2022-01-06 18:30:02	2020-11-16
29	CorObj6003	application-default	912.3M	any	2	448	Compare	2022-01-06 18:30:02	2020-11-16
20	2019-08-TrickBot E...	application-default	508.0M	any	18	448	Compare	2022-01-06 18:30:02	2020-11-16
31	CorObj-wf2	application-default	235.1M	any	1	448	Compare	2022-01-06 18:30:02	2020-11-16
32	GRE-EndPoint	application-default	140.8M	any	1	448	Compare	2022-01-06 18:30:02	2020-11-16
47	Workstation-appdef...	any	23.1M	any	5	448	Compare	2022-01-06 18:30:02	2020-11-16
27	CorObj6005	application-default	22.8M	any	2	448	Compare	2022-01-06 18:30:02	2020-11-16
30	Corobj-IRC	application-default	1.2M	any	1	446	Compare	2022-01-06 18:30:02	2020-11-16
28	CorObj6004	application-default	590.2k	any	1	445	Compare	2022-01-06 18:30:02	2020-11-16
17	LogSinkholeTraffic	application-default	0	any	2	452	Compare	2022-01-06 18:30:02	2020-11-16
24	Outbound-Trust	application-default	0	any	1	419	Compare	2022-01-06 18:30:02	2020-11-16

A. Rules without App Controls
B. New App Viewer
C. Rule Usage
D. Unused Unused Apps

Correct Answer: C
Section:

QUESTION 142
In which two types of NAT can oversubscription be used? (Choose two.)

A. Static IP
B. Destination NAT
C. Dynamic IP and Port (DIPP)
D. Dynamic IP

Correct Answer: C, D
Section:
Explanation:
Oversubscription is a feature that allows you to use more private IP addresses than public IP addresses for NAT. This means that multiple private IP addresses can share the same public IP address, as long as they use different ports. Oversubscription can be used in two types of NAT: Dynamic IP and Port (DIPP) and Dynamic IP. DIPP NAT translates both the source IP address and the source port number of the outgoing packets, and can have an oversubscription rate greater than 1. Dynamic IP NAT translates only the source IP address of the outgoing packets, and can have an oversubscription rate of 1 or less. Static IP and Destination NAT do not support oversubscription, as they require a one-to-one mapping between the private and public IP addresses.Reference:Source NAT,Configure NAT,NAT

QUESTION 143

Where in the PAN-OS GUI can an administrator monitor the rule usage for a specified period of time?

A. Objects > Schedules
B. Policies > Policy Optimizer
C. Monitor > Packet Capture
D. Monitor > Reports

Correct Answer: B
Section:
Explanation:
The Policy Optimizer is a feature in the PAN-OS GUI that allows an administrator to monitor the rule usage for a specified period of time, as well as optimize the security policies based on the traffic logs and recommendations. The Policy Optimizer can help the administrator to improve the security posture, reduce the attack surface, and simplify the policy management. The Policy Optimizer can be accessed from Policies > Policy Optimizer in the PAN-OS GUI.Reference:Policy Optimizer,View Policy Rule Usage,Updated Certifications for PAN-OS 10.1

QUESTION 144
Which security profile should be used to classify malicious web content?

A. URL Filtering
B. Antivirus
C. Web Content
D. Vulnerability Protection

Correct Answer: A
Section:
Explanation:
URL Filtering is a security profile that allows you to classify web content based on the URL category and reputation of the website. URL Filtering can help you block access to malicious web content, such as phishing, malware, or command and control sites, as well as enforce acceptable use policies for web browsing. URL Filtering uses the PAN-DB cloud service to provide up-to-date information on the URL categories and reputations of millions of websites. You can configure URL Filtering policies to allow, block, alert, continue, or override web requests based on the URL category and reputation, as well as customize the response pages and exceptions for different user groups.Reference:URL Filtering,Set Up a Basic Security Policy,Updated Certifications for PAN-OS 10.1

QUESTION 145
In order to attach an Antivirus, Anti-Spyware and Vulnerability Protection security profile to your Security Policy rules, which setting must be selected?

A. Policies > Security > Actions Tab > Select Group-Profiles as Profile Type
B. Policies > Security > Actions Tab > Select Default-Profiles as Profile Type
C. Policies > Security > Actions Tab > Select Profiles as Profile Type
D. Policies > Security > Actions Tab > Select Tagged-Profiles as Profile Type

Correct Answer: C
Section:
Explanation:
To enable the firewall to scan the traffic that it allows based on a Security policy rule, you must also attach Security Profiles ---including URL Filtering, Antivirus, Anti-Spyware, File Blocking, and WildFire Analysis---to each rule. To attach a Security Profile to a Security policy rule, you must select Profiles as the Profile Type in the Actions tab of the rule. This allows you to choose from the predefined or custom Security Profiles that you have configured. Group-Profiles, Default-Profiles, and Tagged-Profiles are not valid options for attaching Security Profiles to Security policy rules.Reference:Set Up a Basic Security Policy,Security Profiles,Updated Certifications for PAN-OS 10.1

QUESTION 146
When a security rule is configured as Intrazone, which field cannot be changed?

A. Actions
B. Source Zone
C. Application
D. Destination Zone

Correct Answer: D
Section:
Explanation:
When a security rule is configured as Intrazone, the destination zone field cannot be changed. This is because an intrazone rule applies to traffic that originates and terminates in the same zone.The destination zone is automatically set to the same value as the source zone and cannot be modified1.An intrazone rule allows you to control and inspect traffic within a zone, such as applying security profiles or logging options2.Reference:What are Universal, Intrazone and Interzone Rules?,Security Policy,Updated Certifications for PAN-OS 10.1,Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0)or [Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0)].

QUESTION 147
In which two Security Profiles can an action equal to the block IP feature be configured? (Choose two.)

A. URL Filtering
B. Vulnerability Protection
C. Antivirus b
D. Anti-spyware

Correct Answer: B, D
Section:
Explanation:
The block IP feature can be configured in two Security Profiles: Vulnerability Protection and Anti-spyware. The block IP feature allows the firewall to block traffic from a source IP address for a specified period of time after detecting a threat.This feature can help prevent further attacks from the same source and reduce the load on the firewall1. The block IP feature can be enabled in the following Security Profiles:
Vulnerability Protection: A Vulnerability Protection profile defines the actions that the firewall takes to protect against exploits and vulnerabilities in applications and protocols.You can configure a rule in the Vulnerability Protection profile to block IP connections for a specific threat or a group of threats2.
Anti-spyware: An Anti-spyware profile defines the actions that the firewall takes to protect against spyware and command-and-control (C2) traffic. You can configure a rule in the Anti-spyware profile to block IP addresses for a specific spyware or C2 signature.

QUESTION 148
In which section of the PAN-OS GUI does an administrator configure URL Filtering profiles?

A. Network ab
B. Policies
C. Objects
D. Device

Correct Answer: C
Section:
Explanation:
URL Filtering profiles are configured in the Objects section of the PAN-OS GUI. A URL Filtering profile defines the actions that the firewall takes for different URL categories, such as allow, block, alert, continue, or override.You can also configure settings for credential phishing prevention, URL filtering inline machine learning, and safe search enforcement in a URL Filtering profile1.To create or modify a URL Filtering profile, you need to go to Objects > Security Profiles > URL Filtering2.Reference:URL Filtering Profile,Create a URL Filtering Profile,Updated Certifications for PAN-OS 10.1,Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0)or [Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0)].

QUESTION 149
What are three valid source or D=destination conditions available as Security policy qualifiers? (Choose three.)

A. Service
B. User
C. Application
D. Address
E. Zone ab

Correct Answer: B, C, E
Section:
Explanation:
Three valid source or destination conditions available as Security policy qualifiers are User, Application, and Zone. These qualifiers allow you to define the match criteria for a Security policy rule based on the identity of the user, the application used, and the zone where the traffic originates or terminates.You can use these qualifiers to enforce granular security policies that control access to network resources and prevent threats1. Some of the characteristics of these qualifiers are:
User: The User qualifier allows you to specify the source or destination user or user group for a Security policy rule. The firewall can identify users based on various methods, such as User-ID, Captive Portal, or GlobalProtect.You can use the User qualifier to apply different security policies for different users or user groups, such as allowing access to certain applications or resources based on user roles or privileges2.
Application: The Application qualifier allows you to specify the application or application group for a Security policy rule. The firewall can identify applications based on App-ID, which is a technology that classifies applications based on multiple attributes, such as signatures, protocol decoders, heuristics, and SSL decryption.You can use the Application qualifier to allow or deny access to specific applications or application groups, such as enabling web browsing but blocking social networking or file sharing3.
Zone: The Zone qualifier allows you to specify the source or destination zone for a Security policy rule. A zone is a logical grouping of one or more interfaces that have similar functions or security requirements. The firewall can apply security policies based on the zones where the traffic originates or terminates, such as intrazone, interzone, or universal.You can use the Zone qualifier to segment your network and isolate traffic based on different trust levels or network functions4.

QUESTION 150
Which feature enables an administrator to review the Security policy rule base for unused rules?

A. Test Policy Match
B. Policy Optimizer
C. View Rulebase as Groups
D. Security policy tags eb

Correct Answer: B
Section:
Explanation:
Policy Optimizer provides a simple workflow to migrate your legacy Security policy rulebase to an App-ID based rulebase, which improves your security by reducing the attack surface and gaining visibility into applications so you can safely enable them. Policy Optimizer can also identify unused rules, duplicate rules, and rules that can be merged or reordered to optimize your rulebase.You can use Policy Optimizer to review the usage statistics of your rules and take actions to clean up or modify your rulebase as needed1.Reference:Security Policy Rule Optimization,Updated Certifications for PAN-OS 10.1,Free PCNSE Questions for Palo Alto Networks PCNSE Exam

QUESTION 151
A systems administrator momentarily loses track of which is the test environment firewall and which is the production firewall. The administrator makes changes to the candidate configuration of the production firewall, but does not commit the changes. In addition, the configuration was not saved prior to
making the changes.
Which action will allow the administrator to undo the changes?

A. Load configuration version, and choose the first item on the list.
B. Load named configuration snapshot, and choose the first item on the list.
C. Revert to last saved configuration.

D. Revert to running configuration.

Correct Answer: D
Section:
Explanation:
Reverting to the running configuration will undo the changes made to the candidate configuration since the last commit. This operation will replace the settings in the current candidate configuration with the settings from the running configuration.The firewall provides the option to revert all the changes or only specific changes by administrator or location1.Reference:Revert Firewall Configuration Changes,How to Revert to a Previous Configuration,How to revert uncommitted changes on the firewall?.

QUESTION 152
What is used to monitor Security policy applications and usage?

A. Policy Optimizer
B. App-ID
C. Security profile
D. Policy-based forwarding

Correct Answer: A
Section:

QUESTION 153
What is a default setting for NAT Translated Packets when the destination NAT translation is selected as Dynamic IP (with session distribution)?

A. IP Hash
B. Source IP Hash
C. Round Robin
D. Least Sessions

Correct Answer: C
Section:
Explanation:
When the destination NAT translation is selected as Dynamic IP (with session distribution), the firewall uses a round-robin algorithm to distribute sessions among the available IP addresses that are resolved from the FQDN.This option allows you to load-balance traffic to multiple servers that have dynamic IP addresses1.Reference:Destination NAT,NAT,Getting Started: Network Address Translation (NAT).

QUESTION 154
Which table for NAT and NPTv6 (IPv6-to-IPv6 Network Prefix Translation) settings is available only on Panorama?

A. NAT Target Tab
B. NAT Active/Active HA Binding Tab
C. NAT Translated Packet Tab
D. NAT Policies General Tab

Correct Answer: A
Section:
Explanation:
The NAT Target tab is a table that allows you to specify the target firewalls or device groups for each NAT policy rule on Panorama. This tab is available only on Panorama and not on individual firewalls. The NAT Target tab enables you to create a single NAT policy rulebase on Panorama and then selectively push the rules to the firewalls or device groups that require them.This reduces the complexity and duplication of managing NAT policies across multiple firewalls1.Reference:NAT Target Tab,NAT Policy Overview,NPTv6 Overview,Updated Certifications for PAN-OS 10.1.

QUESTION 155
Which three Ethernet interface types are configurable on the Palo Alto Networks firewall? (Choose three.)

A. Virtual Wire
B. Tap
C. Dynamic
D. Layer 3
E. Static

Correct Answer: A, B, D
Section:
Explanation:
Palo Alto Networks firewalls support three types of Ethernet interfaces that can be configured on the firewall: virtual wire, tap, and layer 31. These interface types determine how the firewall processes traffic and applies security policies. Some of the characteristics of these interface types are:
Virtual Wire: A virtual wire interface allows the firewall to transparently pass traffic between two network segments without modifying the packets or affecting the routing.The firewall can still apply security policies and inspect the traffic based on the source and destination zones of the virtual wire2.
Tap: A tap interface allows the firewall to passively monitor traffic from a network switch or router without affecting the traffic flow. The firewall can only receive traffic from a tap interface and cannot send traffic out of it.The firewall can apply security policies and inspect the traffic based on the source and destination zones of the tap interface3.
Layer 3: A layer 3 interface allows the firewall to act as a router and participate in the network routing.The firewall can send and receive traffic from a layer 3 interface and apply security policies and inspect the traffic based on the source and destination IP addresses and zones of the interface4.

QUESTION 156
Within a WildFire Analysis Profile, what match criteria can be defined to forward samples for analysis?

A. Application Category
B. Source
C. File Size
D. Direction

Correct Answer: D
Section:
Explanation:
A WildFire Analysis Profile allows you to specify which files or email links to forward for WildFire analysis based on the application, file type, and transmission direction (upload or download) of the traffic. The direction match criteria determines whether the file or email link was sent from the source zone to the destination zone (upload) or from the destination zone to the source zone (download). You can also select both directions to forward files or email links regardless of the direction of the traffic.Reference:Security Profile: Wildfire Analysis,Objects > Security Profiles > WildFire Analysis

QUESTION 157
What must first be created on the firewall for SAML authentication to be configured?

A. Server Policy
B. Server Profile
C. Server Location
D. Server Group

Correct Answer: B
Section:
Explanation:
A server profile identifies the external authentication service and instructs the firewall on how to connect to that authentication service and access the authentication credentials for your users. To configure SAML

authentication, you must create a server profile and register the firewall and the identity provider (IdP) with each other. You can import a SAML metadata file from the IdP to automatically create a server profile and populate the connection, registration, and IdP certificate information.Reference:Configure SAML Authentication,Set Up SAML Authentication,Introduction to SAML

QUESTION 158
Which two options does the firewall use to dynamically populate address group members? (Choose two.)

A. IP Addresses
B. Tags
C. MAC Addresses
D. Tag-based filters

Correct Answer: B, D
Section:
Explanation:
A dynamic address group populates its members dynamically using look ups for tags and tag-based filters. Tags are metadata elements or attribute-value pairs that are registered for each IP address. Tag-based filters use logical and and or operators to match the tags and determine the membership of the dynamic address group. For example, you can create a dynamic address group that includes all IP addresses that have the tags ''web-server'' and ''linux''. You can also use static tags as part of the filter criteria.Reference:Policy Object: Address Groups,Use Dynamic Address Groups in Policy,Statics vs. Dynamic Address Objects Groups

QUESTION 159
What two actions can be taken when implementing an exception to an External Dynamic List? (Choose two.)

A. Exclude an IP address by making use of wildcards.
B. Exclude a URL entry by making use of regular expressions.
C. Exclude an IP address by making use of regular expressions.
D. Exclude a URL entry by making use of wildcards.

Correct Answer: A, B
Section:

QUESTION 160
Which feature enables an administrator to review the Security policy rule base for unused rules?

A. Security policy tags
B. Test Policy Match
C. View Rulebase as Groups
D. Policy Optimizer

Correct Answer: D
Section:
Explanation:
The Policy Optimizer feature enables an administrator to review the Security policy rule base for unused rules, unused applications, and shadowed rules. The Policy Optimizer provides information and recommendations to help optimize the Security policy rules and reduce the attack surface.The Policy Optimizer can also identify rules that can be converted to use App-ID instead of port-based criteria12.Reference:Policy Optimizer,Tips & Tricks: How to Identify Unused Policies on a Palo Alto Networks Device

QUESTION 161
An administrator should filter NGFW traffic logs by which attribute column to determine if the entry is for the start or end of the session?

A. Receive Time

B. Type
C. Destination
D. Source

Correct Answer: B
Section:
Explanation:
The Type attribute column in the NGFW traffic logs indicates whether the log entry is for the start or end of the session. The possible values are START, END, DROP, DENY, and INVALID. The START value means that the log entry is for the start of the session, and the END value means that the log entry is for the end of the session.The other values indicate that the session was terminated by the firewall for various reasons12.Reference:Traffic Log Fields,Session Log Best Practices

QUESTION 162
What is the default action for the SYN Flood option within the DoS Protection profile?

A. Alert
B. Random Early Drop
C. Reset-client
D. Sinkhole

Correct Answer: B
Section:
Explanation:
Random Early Drop ---The firewall uses an algorithm to progressively start dropping that type of packet. If the attack continues, the higher the incoming cps rate (above the Activate Rate) gets, the more packets the firewall drops. .. (https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/zone-protection-and-dos-protection/dos-protection-against-flooding-of-new-sessions/configure-dos-protection-against-flooding-of-new-sessions)

QUESTION 163
Which Security policy set should be used to ensure that a policy is applied first?

A. Child device-group pre-rulebase
B. Shared pre-rulebase
C. Parent device-group pre-rulebase
D. Local firewall policy

Correct Answer: B
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/panorama-web-interface/defining-policies-on-panorama

QUESTION 164
Which type of DNS signatures are used by the firewall to identify malicious and command-and-control domains?

A. DNS Malicious signatures
B. DNS Malware signatures
C. DNS Block signatures
D. DNS Security signatures

Correct Answer: D
Section:
Explanation:
https://docs.paloaltonetworks.com/dns-security/administration/configure-dns-security/enable-dns-security#tabs-id066476b2-c4dd-4fc0-b7e4-f4ba32e19f60

QUESTION 165
Which three types of entries can be excluded from an external dynamic list (EDL)? (Choose three.)

A. IP addresses
B. Domains
C. User-ID
D. URLs
E. Applications

Correct Answer: A, B, D
Section:
Explanation:
Three types of entries that can be excluded from an external dynamic list (EDL) are IP addresses, domains, and URLs. An EDL is a text file that is hosted on an external web server and contains a list of objects, such as IP addresses, URLs, domains, International Mobile Equipment Identities (IMEIs), or International Mobile Subscriber Identities (IMSIs) that the firewall can import and use in policy rules. You can exclude entries from an EDL to prevent the firewall from enforcing policy on those entries.For example, you can exclude benign domains that applications use for background traffic from Authentication policy1. To exclude entries from an EDL, you need to:
Select the EDL on the firewall and clickManual Exceptions.
Add the entries that you want to exclude in theManual Exceptionslist. The entries must match the type and format of the EDL. For example, if the EDL contains IP addresses, you can only exclude IP addresses.
ClickOKto save the changes. The firewall will not enforce policy on the excluded entries.

QUESTION 166
The administrator profile 'SYS01 Admin' is configured with authentication profile 'Authentication Sequence SYS01,' and the authentication sequence SYS01 has a profile list with four authentication profiles:
* Auth Profile LDAP
* Auth Profile Radius
* Auth Profile Local
* Auth Profile TACACS
After a network outage, the LDAP server is no longer reachable. The RADIUS server is still reachable but has lost the 'SYS01 Admin' username and password.
What is the 'SYS01 Admin' login capability after the outage?

A. Auth KO because RADIUS server lost user and password for SYS01 Admin
B. Auth KO because LDAP server is not reachable
C. Auth OK because of the Auth Profile Local
D. Auth OK because of the Auth Profile TACACS -

Correct Answer: C
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/authentication/configure-an-authentication-profile-and-sequence

QUESTION 167
In which two Security Profiles can an action equal to the block IP feature be configured? (Choose two.)

A. Antivirus
B. URL Filtering

C. Vulnerability Protection
D. Anti-spyware

Correct Answer: C, D
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/objects/objects-security-profiles/actions-in-security-profiles

QUESTION 168
What are two valid selections within an Anti-Spyware profile? (Choose two.)

A. Default
B. Deny
C. Random early drop
D. Drop

Correct Answer: A, D
Section:
Explanation:
Deny is a policy action, random early drop is part of the inner workings of DoS protection

QUESTION 169
When is an event displayed under threat logs?

A. When traffic matches a corresponding Security Profile
B. When traffic matches any Security policy
C. Every time a session is blocked
D. Every time the firewall drops a connection

Correct Answer: A
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/monitoring/view-and-manage-logs/log-types-and-severity-levels/threat-logs#:~:text=Threat%20logs%20display%20entries%20when,security%20rule%20on%20the%20firewall.

QUESTION 170
Which Security profile should be applied in order to protect against illegal code execution?

A. Vulnerability Protection profile on allowed traffic
B. Antivirus profile on allowed traffic
C. Antivirus profile on denied traffic
D. Vulnerability Protection profile on denied traffic

Correct Answer: A
Section:
Explanation:
The Security profile that should be applied in order to protect against illegal code execution is the Vulnerability Protection profile on allowed traffic. The Vulnerability Protection profile defines the actions that the firewall takes to protect against exploits and vulnerabilities in applications and protocols. The firewall can block or alert on traffic that matches a specific threat signature or a group of threats.The Vulnerability Protection profile can

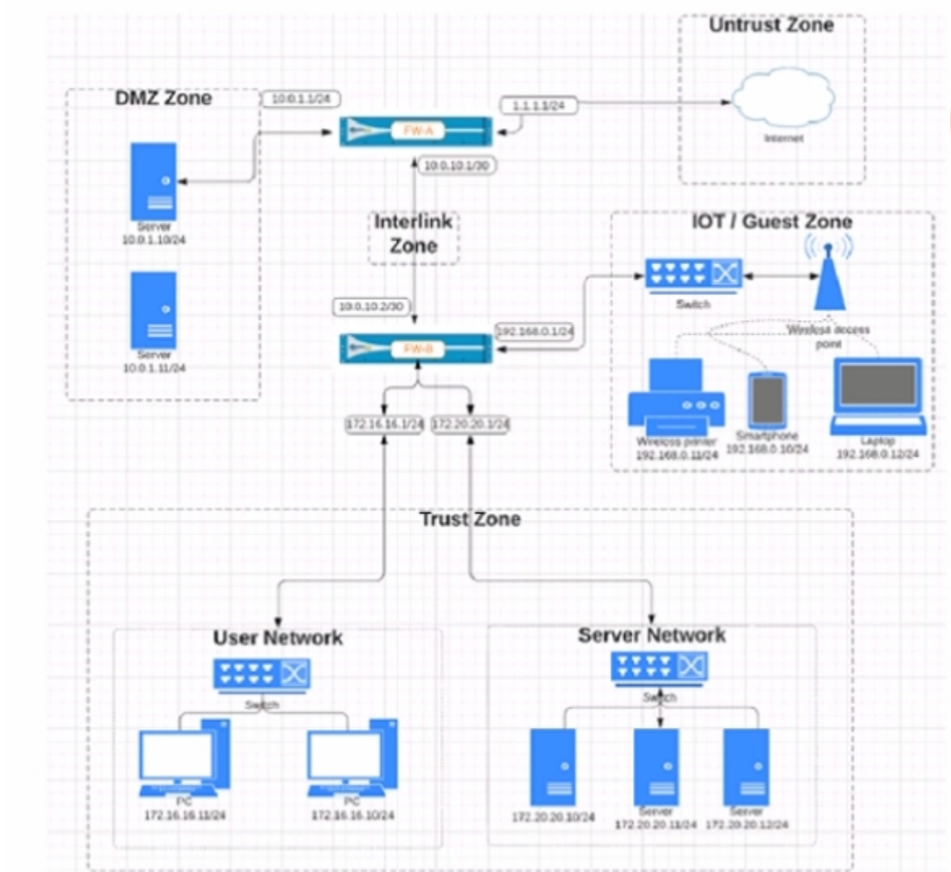
prevent illegal code execution by detecting and blocking attempts to exploit buffer overflows, format string vulnerabilities, or other code injection techniques1. To apply the Vulnerability Protection profile on allowed traffic, you need to:
Create or modify a Vulnerability Protection profile on the firewall or Panorama and configure the rules and exceptions for the threats that you want to protect against2.
Attach the Vulnerability Protection profile to a Security policy rule that allows traffic that you want to scan for vulnerabilities3.
Commit the changes to the firewall or Panorama and the managed firewalls.

QUESTION 171
Which three types of Source NAT are available to users inside a NGFW? (Choose three.)

A. Dynamic IP and Port (DIPP)
B. Static IP
C. Static Port
D. Dynamic IP
E. Static IP and Port (SIPP)

Correct Answer: A, B, E
Section:

QUESTION 172
Refer to the exhibit.



Based on the network diagram provided, which two statements apply to traffic between the User and Server networks? (Choose two.)

A. Traffic is permitted through the default intrazone 'allow' rule.
B. Traffic restrictions are possible by modifying intrazone rules.
C. Traffic restrictions are not possible, because the networks are in the same zone.
D. Traffic is permitted through the default interzone 'allow' rule.

Correct Answer: A, B
Section:
Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail? id=kA10g000000ClTHCA0&lang=es

QUESTION 173
Which two types of profiles are needed to create an authentication sequence? (Choose two.)

A. Server profile
B. Authentication profile
C. Security profile
D. Interface Management profile

Correct Answer: A, B
Section:
Explanation:
In the FW you define an Auth sequence which specifies the Auth Profile. If you click add on an Auth Profile and define one named TACACS for example, the Auth Profile calls in the TACACS+ Server Profile.

QUESTION 174
Which setting is available to edit when a tag is created on the local firewall?

A. Location
B. Color
C. Order
D. Priority

Correct Answer: B
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/objects/objects-tags/create-tags

QUESTION 175
What is the best-practice approach to logging traffic that traverses the firewall?

A. Enable both log at session start and log at session end.
B. Enable log at session start only.
C. Enable log at session end only.
D. Disable all logging options.

Correct Answer: C
Section:

Explanation:
The best-practice approach to logging traffic that traverses the firewall is to enable log at session end only. This option allows the firewall to generate a log entry only when a session ends, which reduces the load on the firewall and the log storage. The log entry contains information such as the source and destination IP addresses, ports, zones, application, user, bytes, packets, and duration of the session.The log at session end option also provides more accurate information about the session, such as the final application and user, the total bytes and packets, and the session end reason1. To enable log at session end only, you need to:
Create or modify a Security policy rule that matches the traffic that you want to log.
Select the Actions tab in the policy rule and check the Log at Session End option.
Commit the changes to the firewall or Panorama and the managed firewalls.

QUESTION 176
Where in Panorama Would Zone Protection profiles be configured?

A. Shared
B. Templates
C. Device Groups
D. Panorama tab

Correct Answer: B
Section:
Explanation:
https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/manage-firewalls/use-case-configure-firewalls-using-panorama/set-up-your-centralized-configuration-and-policies/use-templates-to-administer-a-base-configuration

QUESTION 177
Based on the image provided, which two statements apply to the Security policy rules? (Choose two.)

				Source			Destination						
	NAME	TAGS	TYPE	ZONE	ADDRESS	DEVICE	ZONE	ADDRESS	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
19	Allow-Office-Programs	none	universal	Internal	any	any	External	any	office-programs	application-defa...	Allow		
20	Allow-FTP	none	universal	Internal	any	any	External	FTP Server	any	FTP	Allow		
21	Allow-Social-Media	none	universal	Internal	any	any	External	any	facebook	application-defa...	Allow		
22	intrazone-default	none	intrazone	any	any	any	(intrazone)	any	any	any	Allow	none	
23	interzone-default	none	interzone	any	any	any	any	any	any	any	Deny	none	

A. The Allow-Office-Programs rule is using an application filter.
B. The Allow-Office-Programs rule is using an application group.
C. The Allow-Social-Media rule allows all Facebook functions.
D. In the Allow-FTP policy, FTP is allowed using App-ID.

Correct Answer: A, C
Section:

QUESTION 178
How would a Security policy need to be written to allow outbound traffic using Secure Shell (SSH) to destination ports tcp/22 and tcp/4422?

A. The admin creates a custom service object named 'tcp-4422' with port tcp/4422. The admin then creates a Security policy allowing application 'ssh' and service 'tcp-4422'.
B. The admin creates a custom service object named 'tcp-4422' with port tcp/4422. The admin then creates a Security policy allowing application 'ssh', service 'tcp-4422'. and service 'application-default'.
C. The admin creates a Security policy allowing application 'ssh' and service 'application-default'.
D. The admin creates a custom service object named 'tcp-4422' with port tcp/4422. The admin also creates a custom service object named 'tcp-22' with port tcp/22. The admin then creates a Security policy allowing application 'ssh', service 'tcp-4422'. and service 'tcp-22'.

Correct Answer: D
Section:

QUESTION 179
Which feature must be configured to enable a data plane interface to submit DNS queries originated from the firewall on behalf of the control plane?

A. Service route
B. Admin role profile
C. DNS proxy
D. Virtual router

Correct Answer: A
Section:
Explanation:
By default, the firewall uses the management (MGT) interface to access external services, such as DNS servers, external authentication servers, Palo Alto Netw orks services such as soft ware, URL updates, licenses, and AutoFocus. An alternative to using the MGT interface is configuring a data port (a standard interface) to access these services. The path from the interface to th e service on a server is aservice route. [Palo Alto Networks] PAN-OS 10 -> Device -> Setup -> Services -> Service Features -> Service Route Configuration

QUESTION 180
An administrator creates a new Security policy rule to allow DNS traffic from the LAN to the DMZ zones. The administrator does not change the rule type from its default value.
What type of Security policy rule is created?

A. Tagged
B. Intrazone
C. Universal
D. Interzone

Correct Answer: C
Section:

QUESTION 181
When HTTPS for management and GlobalProtect are enabled on the same data plane interface, which TCP port is used for management access?

A. 80
B. 443
C. 4443
D. 8443

Correct Answer: C
Section:

Explanation:
The GlobalProtect Portal can be accessed by going to the IP address of the designated interface using https on port 443. The WebUI on the same interface can be accessed by going to the interface's IP address using https on port 4443. The port for WebUI management is changed because the tcp/443 socket used by GlobalProtect takes precedence

QUESTION 182
An administrator manages a network with 300 addresses that require translation. The administrator configured NAT with an address pool of 240 addresses and found that connections from addresses that needed new translations were being dropped.
Which type of NAT was configured?

A. Static IP
B. Dynamic IP
C. Destination NAT
D. Dynamic IP and Port

Correct Answer: B
Section:
Explanation:
The size of the NAT pool should be equal to the number of internal hosts that require address translations. By default, if the source address pool is larger than the NAT address pool and eventually all of the NAT addresses are allocated, new connections that need address translation are dropped. To override this default behavior, use Advanced (Dynamic IP/Port Fallback) to enable the use of DIPP addresses when necessary

QUESTION 183
What are the two main reasons a custom application is created? (Choose two.)

A. To correctly identify an internal application in the traffic log
B. To change the default categorization of an application
C. To visually group similar applications
D. To reduce unidentified traffic on a network

Correct Answer: A, D
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/app-id/use-application-objects-in-policy/create-a-custom-application

QUESTION 184
What Policy Optimizer policy view differ from the Security policy do?

A. It shows rules that are missing Security profile configurations.
B. It indicates rules with App-ID that are not configured as port-based.
C. It shows rules with the same Source Zones and Destination Zones.
D. It indicates that a broader rule matching the criteria is configured above a more specific rule.

Correct Answer: B
Section:
Explanation:
Policy Optimizer policy view differs from the Security policy view in several ways. One of them is that it indicates rules with App-ID that are not configured as port-based. These are rules that have the application set to ''any'' instead of a specific application or group of applications. These rules are overly permissive and can introduce security gaps, as they allow any application traffic on the specified ports.Policy Optimizer helps you convert these rules to application-based rules that follow the principle of least privilege access12.You can use Policy Optimizer to discover and convert port-based rules to application-based rules, and also to remove unused applications, eliminate unused rules, and discover new applications that match your policy criteria3.Reference:

Policy Optimizer Best Practices - Palo Alto Networks
Manage: Policy Optimizer - Palo Alto Networks | TechDocs
Why use Security Policy Optimizer and what are the benefits?

QUESTION 185
How does the Policy Optimizer policy view differ from the Security policy view?

A. It provides sorting options that do not affect rule order.
B. It displays rule utilization.
C. It details associated zones.
D. It specifies applications seen by rules.

Correct Answer: A
Section:
Explanation:
You can't filter or sort rules in PoliciesSecurity because that would change the order of the policy rules in the rulebase. Filtering and sorting PoliciesSecurityPolicy OptimizerNo App Specified, PoliciesSecurityPolicy OptimizerUnused Apps, and PoliciesSecurityPolicy OptimizerNew App Viewer (if you have a SaaS Inline Security subscription) does not change the order of the rules in the rulebase. https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/app-id/security-policy-rule-optimization/policy-optimizer-concepts/sorting-and-filtering-security-policy-rules

QUESTION 186
Which System log severity level would be displayed as a result of a user password change?

A. High
B. Critical
C. Medium
D. Low

Correct Answer: D
Section:
Explanation:
System logs display entries for each system event on the firewall.
1. Critical - Hardware failures, including high availability (HA) failover and link failures.
2. High - Serious issues, including dropped connections with external devices, such as LDAP and RADIUS servers.
3. Medium - Mid-level notifications, such as antivirus package upgrades.
4. Low - Minor severity notifications, such as user password changes.
5. Informational - Log in/log off, administrator name or password change, any configuration change, and all other events not covered by the other severity levels.
https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/monitoring/view-and-manage-logs/log-types-and-severity-levels/system-logs#id8edbfdae-ed92-4d8e-ab76-6a38f96e8cb1

QUESTION 187
Which situation is recorded as a system log?

A. An attempt to access a spoofed website has been blocked.
B. A connection with an authentication server has been dropped.
C. A file that has been analyzed is potentially dangerous for the system.
D. A new asset has been discovered on the network.

Correct Answer: B
Section:

QUESTION 188
Where within the URL Filtering security profile must a user configure the action to prevent credential submissions?

A. URL Filtering > Inline Categorization
B. URL Filtering > Categories
C. URL Filtering > URL Filtering Settings
D. URL Filtering > HTTP Header Insertion

Correct Answer: B
Section:
Explanation:
URL filtering technology protects users from web-based threats by providing granular control over user access and interaction with content on the Internet. You can develop a URL filtering policy that limits access to sites based on URL categories, users, and groups. For example, you can block access to sites known to host malware and prevent end users from entering corporate credentials to sites in certain categories.

QUESTION 189
Which two features implement one-to-one translation of a source IP address while allowing the source port to change? (Choose two.)

A. Static IP
B. Dynamic IP / Port Fallback
C. Dynamic IP
D. Dynamic IP and Port (DIPP)

Correct Answer: A, D
Section:
Explanation:
Static IP and Dynamic IP and Port (DIPP) are two features that implement one-to-one translation of a source IP address while allowing the source port to change.Static IP translates a single source address to a specific public address, and allows the source port to change dynamically1.Dynamic IP and Port (DIPP) translates the source IP address or range to a single IP address, and uses the source port to differentiate between multiple source IPs that share the same translated address2. Both of these features provide a one-to-one translation of IP addresses, but do not restrict the source port.Reference:
Static IP - Palo Alto Networks
Dynamic IP and Port - Palo Alto Networks

QUESTION 190
A network administrator creates an intrazone security policy rule on a NGFW. The source zones are set to IT. Finance, and HR.
To which two types of traffic will the rule apply? (Choose two.)

A. Within zone HR
B. Within zone IT
C. Between zone IT and zone HR
D. Between zone IT and zone Finance

Correct Answer: A, B
Section:
Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClTHCA0

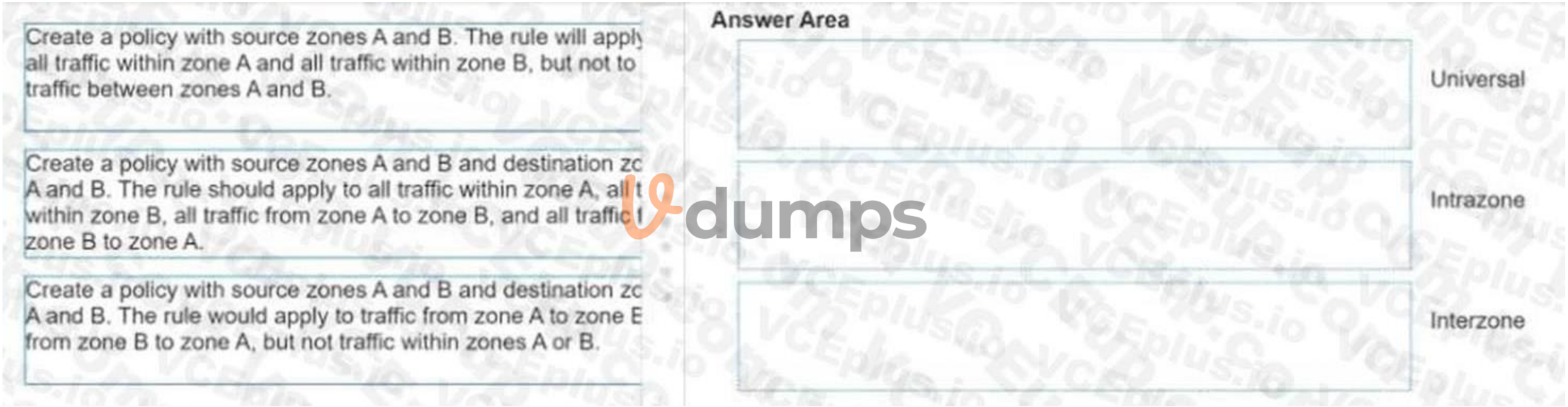
QUESTION 191
An organization has some applications that are restricted for access by the Human Resources Department only, and other applications that are available for any known user in the organization.
What object is best suited for this configuration?

A. Application Group
B. Tag
C. External Dynamic List
D. Application Filter

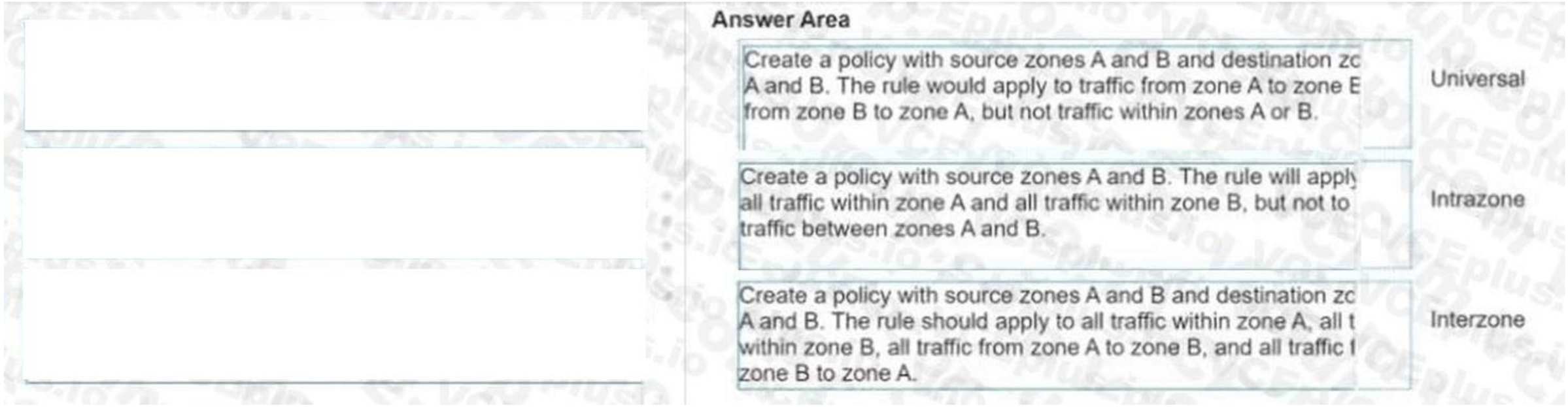
Correct Answer: A
Section:

QUESTION 192
DRAG DROP
Match each rule type with its example

Select and Place:



Correct Answer:



Section:
Explanation:

QUESTION 193
An administrator configured a Security policy rule where the matching condition includes a single application and the action is set to deny. What deny action will the firewall perform?

A. Drop the traffic silently
B. Perform the default deny action as defined in the App-ID database for the application
C. Send a TCP reset packet to the client- and server-side devices
D. Discard the session's packets and send a TCP reset packet to let the client know the session has been terminated

Correct Answer: D
Section:

QUESTION 194
Which object would an administrator create to enable access to all applications in the officeprograms subcategory?

A. HIP profile
B. Application group
C. URL category
D. Application filter

Correct Answer: C
Section:

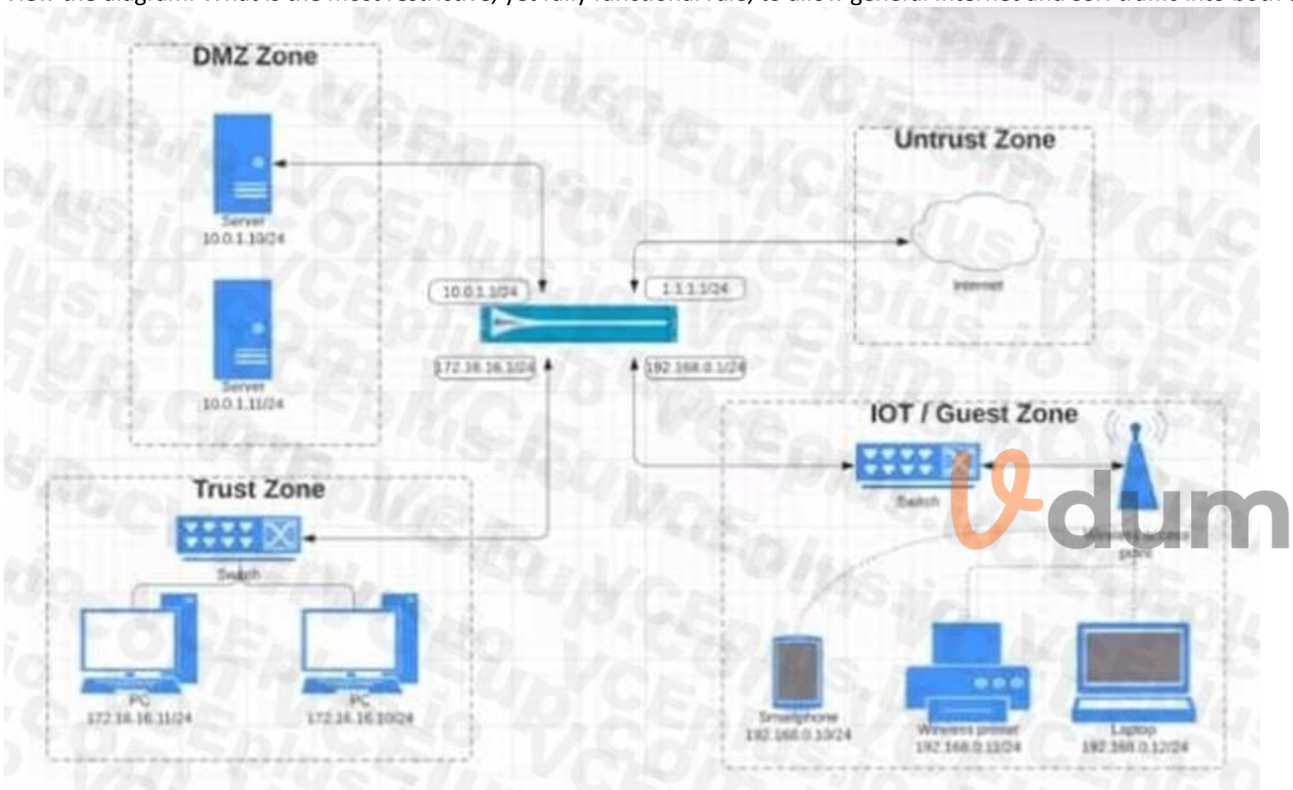
QUESTION 195
What do you configure if you want to set up a group of objects based on their ports alone?

A. Application groups

B. Service groups
C. Address groups
D. Custom objects

Correct Answer: B
Section:

QUESTION 196
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 lOT/Guest and Trust Zones?



A
.

NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE
02-A	none	universal	IOT-Guest Trust	172.16.18.0/24 192.168.0.0/24	any	any	DMZ Untrust	any	any	ssh ssl web-browsing	application-default

B

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE		
03-A	none	universal	IOT-Guest Trust	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

C.

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE		
01-A	none	universal	IOT-Guest Trust	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-defau

D.

NAME	TAGS	TYPE	Source				Destination		
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	

Correct Answer: C
Section:

QUESTION 197
By default, which action is assigned to the interzone-default rule?

A. Reset-client
B. Reset-server
C. Deny
D. Allow

Correct Answer: C
Section:

QUESTION 198
Where does a user assign a tag group to a policy rule in the policy creation window?

A. Application tab
B. General tab
C. Actions tab
D. Usage tab

Correct Answer: B
Section:
Explanation:
A user can assign a tag group to a policy rule in the policy creation window by selecting the General tab. A tag group is a collection of tags that can be used to identify and filter policy rules based on different criteria, such as function, location, or priority.A user can create a tag group on Panorama and assign it to a policy rule to apply the same set of tags to multiple firewalls or device groups1. To assign a tag group to a policy rule, the user needs to:
Select the General tab in the policy creation window.
Click the Tag Group drop-down menu and select the tag group that the user wants to assign to the policy rule.
Click OK to save the changes. The policy rule will inherit the tags from the tag group and display them in the Tag column.

QUESTION 199
Which policy set should be used to ensure that a policy is applied just before the default security rules?

A. Parent device-group post-rulebase
B. Child device-group post-rulebase
C. Local Firewall policy
D. Shared post-rulebase

Correct Answer: D
Section:
Explanation:
The policy set that should be used to ensure that a policy is applied just before the default security rules is the shared post-rulebase. The shared post-rulebase is a set of Security policy rules that are defined on Panorama and apply to all firewalls or device groups. The shared post-rulebase is evaluated after the local firewall policy and the child device-group post-rulebase, but before the default security rules.The shared post-rulebase can be used to enforce common security policies across multiple firewalls or device groups, such as blocking high-risk applications or traffic1.Reference:Security Policy Rule Hierarchy,Security Policy Rulebase,Certifications - Palo Alto Networks,Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0)or [Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0)].

QUESTION 200
A website is unexpectedly allowed due to miscategorization.
What are two ways to resolve this issue for a proper response? (Choose two.)

A. Identify the URL category being assigned to the website.
Edit the active URL Filtering profile and update that category's site access settings to block.
B. Create a URL category and assign the affected URL.
Update the active URL Filtering profile site access setting for the custom URL category to block.
C. Review the categorization of the website on https://urlfiltering.paloaltonetworks.com.
Submit for "request change*, identifying the appropriate categorization, and wait for confirmation before testing again.
D. Create a URL category and assign the affected URL.
Add a Security policy with a URL category qualifier of the custom URL category below the original policy. Set the policy action to Deny.

Correct Answer: C, D
Section:

QUESTION 201
Why should a company have a File Blocking profile that is attached to a Security policy?

A. To block uploading and downloading of specific types of files
B. To detonate files in a sandbox environment
C. To analyze file types

D. To block uploading and downloading of any type of files

Correct Answer: A
Section:

QUESTION 202
An administrator is troubleshooting traffic that should match the interzone-default rule. However, the administrator doesn't see this traffic in the traffic logs on the firewall. The interzone-default was never changed from its default configuration.
Why doesn't the administrator see the traffic?

A. Logging on the interzone-default policy is disabled.
B. Traffic is being denied on the interzone-default policy.
C. The Log Forwarding profile is not configured on the policy.
D. The interzone-default policy is disabled by default.

Correct Answer: A
Section:

QUESTION 203
Given the detailed log information above, what was the result of the firewall traffic inspection?

A. It was blocked by the Anti-Virus Security profile action.
B. It was blocked by the Anti-Spyware Profile action.
C. It was blocked by the Vulnerability Protection profile action.
D. It was blocked by the Security policy action.

Correct Answer: B
Section: