Number: PCNSA
Passing Score: 800
Time Limit: 120
File Version: 16.0

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

Exam A

QUESTION 1
Which statement is true regarding a Prevention Posture Assessment?

A. The Security Policy Adoption Heatmap component filters the information by device groups, serial numbers, zones, areas of architecture, and other categories
B. It provides a set of questionnaires that help uncover security risk prevention gaps across all areas of network and security architecture
C. It provides a percentage of adoption for each assessment area
D. It performs over 200 security checks on Panorama/firewall for the assessment

Correct Answer: B
Section:

QUESTION 2
Which five Zero Trust concepts does a Palo Alto Networks firewall apply to achieve an integrated approach to prevent threats? (Choose five.)

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

Correct Answer: A, C, D, E, F
Section:

QUESTION 3
The PowerBall Lottery has reached a high payout amount and a company has decided to help employee morale by allowing employees to check the number, but doesn't want to unblock the gambling URL category.
Which two methods will allow the employees to get to the PowerBall Lottery site without the company unlocking the gambling URL category? (Choose two.)

A. Add all the URLs from the gambling category except powerball.com to the block list and then set the action for the gambling category to allow.
B. Manually remove powerball.com from the gambling URL category.
C. Add *.powerball.com to the allow list
D. Create a custom URL category called PowerBall and add *.powerball.com to the category and set the action to allow.

Correct Answer: C, D
Section:

QUESTION 4
Which service protects cloud-based applications such as Dropbox and Salesforce by administering permissions and scanning files for sensitive information?

A. Aperture
B. AutoFocus
C. Parisma SaaS

D. GlobalProtect

Correct Answer: C
Section:

QUESTION 5
Which administrator receives a global notification for a new malware that infects hosts. The infection will result in the infected host attempting to contact and command-and-control (C2) server.
Which security profile components will detect and prevent this threat after the firewall`s signature database has been updated?

A. antivirus profile applied to outbound security policies
B. data filtering profile applied to inbound security policies
C. data filtering profile applied to outbound security policies
D. vulnerability profile applied to inbound security policies

Correct Answer: C
Section:

QUESTION 6
Which update option is not available to administrators?

A. New Spyware Notifications
B. New URLs
C. New Application Signatures
D. New Malicious Domains
E. New Antivirus Signatures

Correct Answer: B
Section:

QUESTION 7
A server-admin in the USERS-zone requires SSH-access to all possible servers in all current and future Public Cloud environments. All other required connections have already been enabled between the USERS- and the OUTSIDE-zone.
What configuration-changes should the Firewall-admin make?

A. Create a custom-service-object called SERVICE-SSH for destination-port-TCP-22. Create a securityrule between zone USERS and OUTSIDE to allow traffic from any source IP-address to any destination IP-address for SERVICE-SSH
B. Create a security-rule that allows traffic from zone USERS to OUTSIDE to allow traffic from any source IP-address to any destination IP-address for application SSH
C. In addition to option a, a custom-service-object called SERVICE-SSH-RETURN that contains sourceport- TCP-22 should be created. A second security-rule is required that allows traffic from zone OUTSIDE to USERS for SERVICE-SSH-RETURN for any source-IP-address to any destination-Ip-address
D. In addition to option c, an additional rule from zone OUTSIDE to USERS for application SSH from any source-IP-address to any destination-IP-address is required to allow the return-traffic from the SSH-servers to reach the server-admin

Correct Answer: B
Section:

QUESTION 8
How often does WildFire release dynamic updates?

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

Correct Answer: A
Section:
Explanation:
References:

QUESTION 9
What is the minimum timeframe that can be set on the firewall to check for new WildFire signatures?

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

Correct Answer: D
Section:
Explanation:
Because new WildFire signatures are now available every five minutes, it is a best practice to use this setting to ensure the firewall retrieves these signatures within a minute of availability.

QUESTION 10
A network has 10 domain controllers, multiple WAN links, and a network infrastructure with bandwidth needed to support mission-critical applications. Given the scenario, which type of User-ID agent is considered a best practice by Palo Alto Networks?

A. Windows-based agent on a domain controller
B. Captive Portal
C. Citrix terminal server with adequate data-plane resources
D. PAN-OS integrated agent

Correct Answer: A
Section:

QUESTION 11
What must be configured for the firewall to access multiple authentication profiles for external services to authenticate a non-local account?

A. authentication sequence
B. LDAP server profile
C. authentication server list
D. authentication list profile

Correct Answer: A
Section:
Explanation:
References:

QUESTION 12
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 13
Which interface type can use virtual routers and routing protocols?

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

Correct Answer: B
Section:

QUESTION 14
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 15
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 16
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 17
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 18
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 19
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 20

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

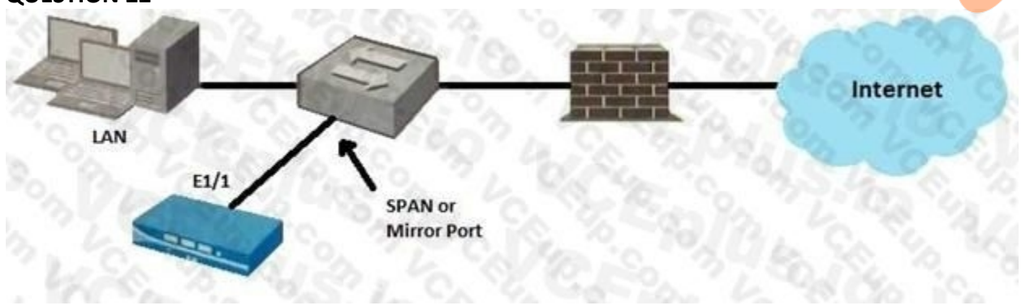
A. Review Policies
B. Review Apps
C. Pre-analyze
D. Review App Matches

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 21
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 22


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 23
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 24
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 25
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 26
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 27
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 28
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 29
In a security policy what is the quickest way to rest all policy rule hit counters to zero?

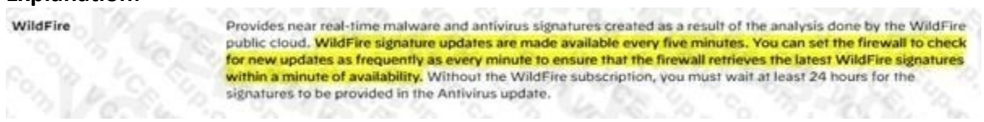
A. Use the CLI enter the command reset rules all
B. Highlight each rule and use the Reset Rule Hit Counter > Selected Rules.
C. use the Reset Rule Hit Counter > All Rules option.
D. Reboot the firewall.

Correct Answer: C
Section:

QUESTION 30
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 31
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

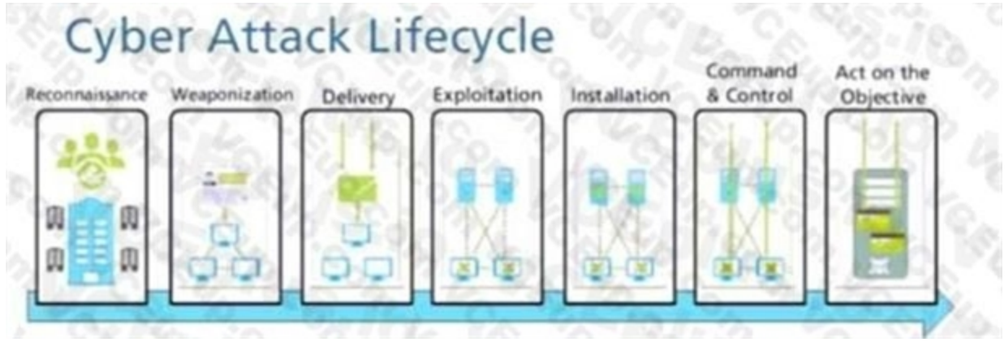
Correct Answer: C
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/user-id-features/dynamicusergroups#:~:text=Dynamic%20user%20groups%20help%20you,activity%20while%20maintaining%20user%20visibility.

QUESTION 32
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 33
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 34
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 35
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+

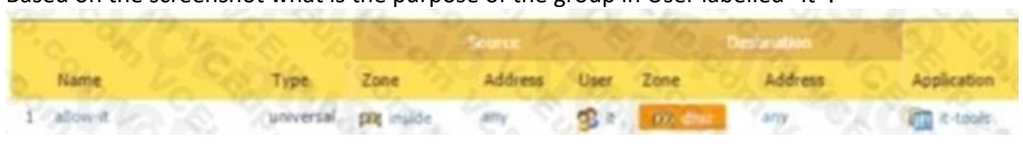
Correct Answer: A, B, D
Section:

QUESTION 36
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 37
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 38
Which dynamic update type includes updated anti-spyware signatures?

A. Applications and Threats
B. GlobalProtect Data File

C. Antivirus
D. PAN-DB

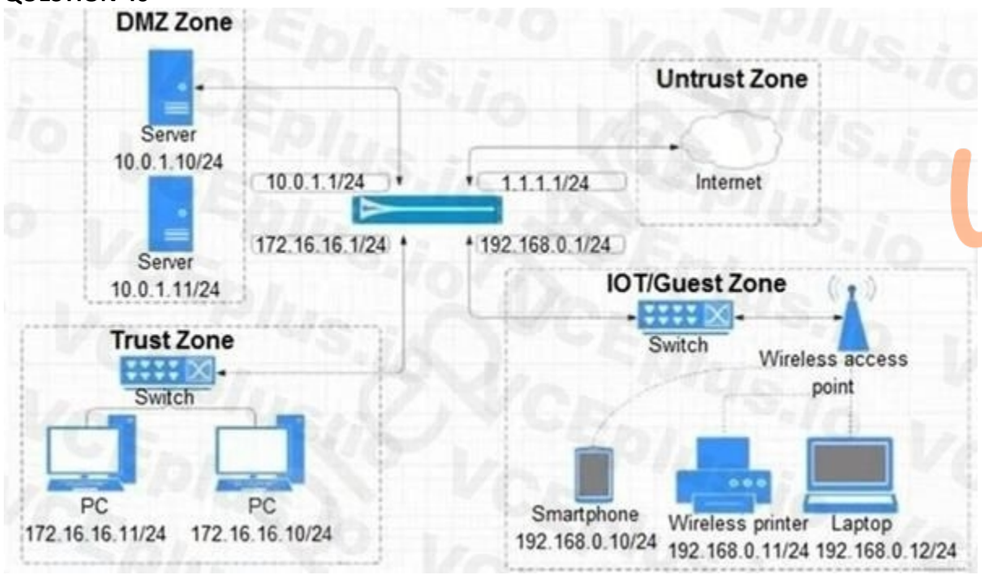
Correct Answer: A
Section:

QUESTION 39
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 40



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.

			Source				Destination				
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE
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	app

B.

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

C.

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

D.

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 41
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 42
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 43
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 44
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 45
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 46
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 47
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 48
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 49
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 50
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 51
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 52
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 53
Which rule type is appropriate for matching traffic both within and between the source and destination zones?

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

Correct Answer: A
Section:

QUESTION 54
What must be considered with regards to content updates deployed from Panorama?

A. Content update schedulers need to be configured separately per device group.
B. Panorama can only install up to five content versions of the same type for potential rollback scenarios.
C. A PAN-OS upgrade resets all scheduler configurations for content updates.
D. Panorama can only download one content update at a time for content updates of the same type.

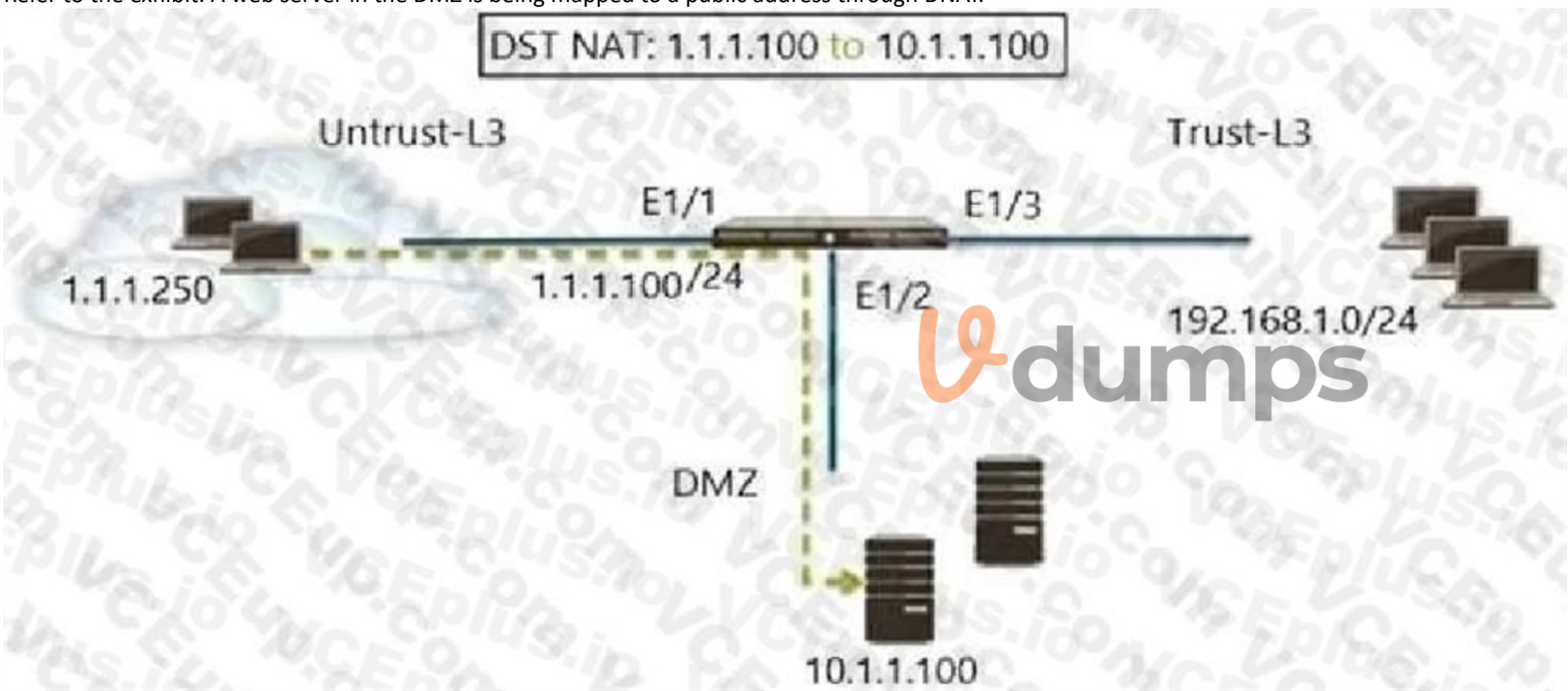
Correct Answer: D
Section:
Explanation:
Reference: https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/manage-licensesand-updates/deploy-updates-to-firewalls-log-collectors-and-wildfire-appliances-usingpanorama/schedule-a-content-update-using-panorama.html

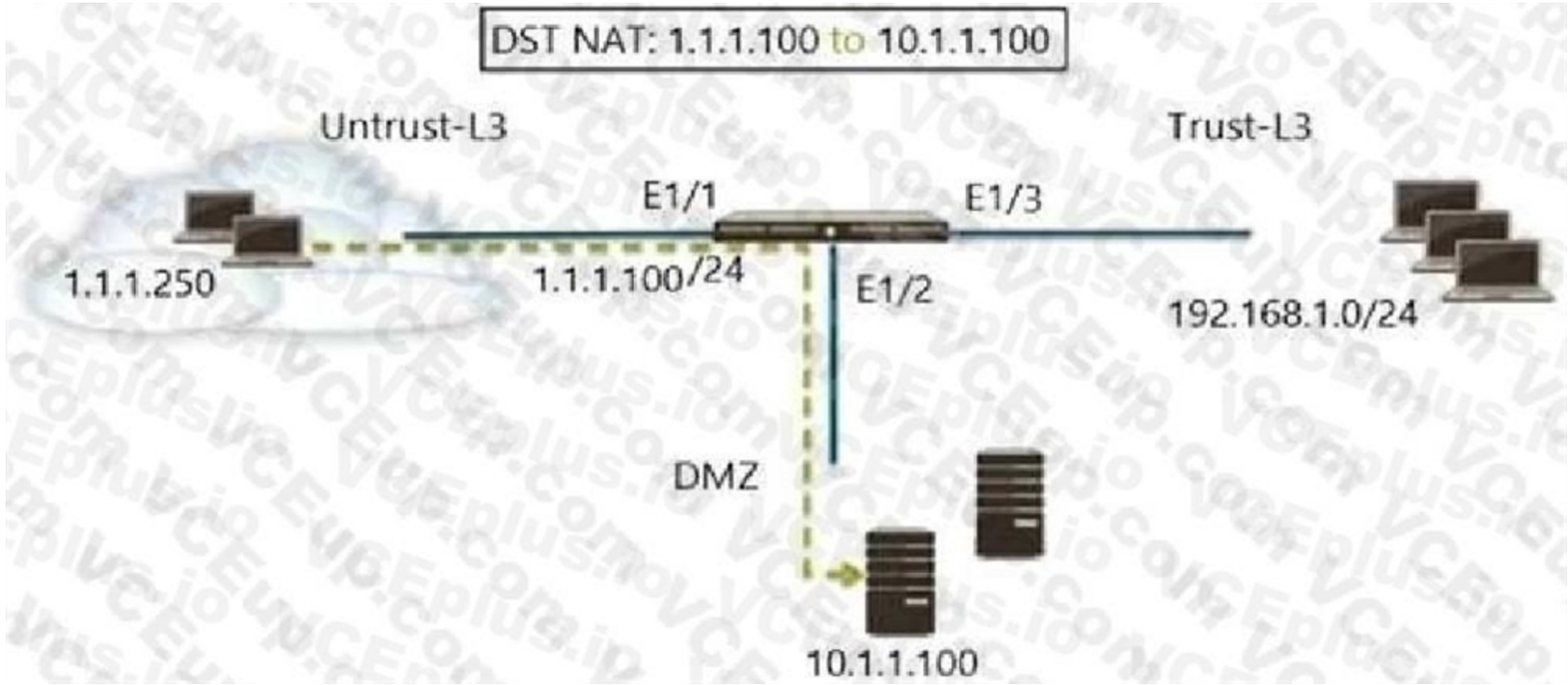
QUESTION 55
During the packet flow process, which two processes are performed in application identification?
(Choose two.)

A. pattern based application identification
B. application override policy match
C. session application identified
D. application changed from content inspection

Correct Answer: A, B
Section:
Explanation:
Reference: http://live.paloaltonetworks.com//t5/image/serverpage/imageid/12862i950F549C7D4E6309

QUESTION 56
Refer to the exhibit. A web server in the DMZ is being mapped to a public address through DNAT.





Which Security policy rule will allow traffic to flow to the web server?

A. Untrust (any) to DMZ (10.1.1.100), web browsing -Allow
B. Untrust (any) to Untrust (1.1.1.100), web browsing - Allow
C. Untrust (any) to Untrust (10.1.1.100), web browsing -Allow
D. Untrust (any) to DMZ (1.1.1.100), web browsing - Allow

Correct Answer: D
Section:
Explanation:
Reference: https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/networking/nat/natconfiguration-examples/destination-nat-exampleone-to-one-mapping

QUESTION 57
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 58
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 59
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 60
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 61
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

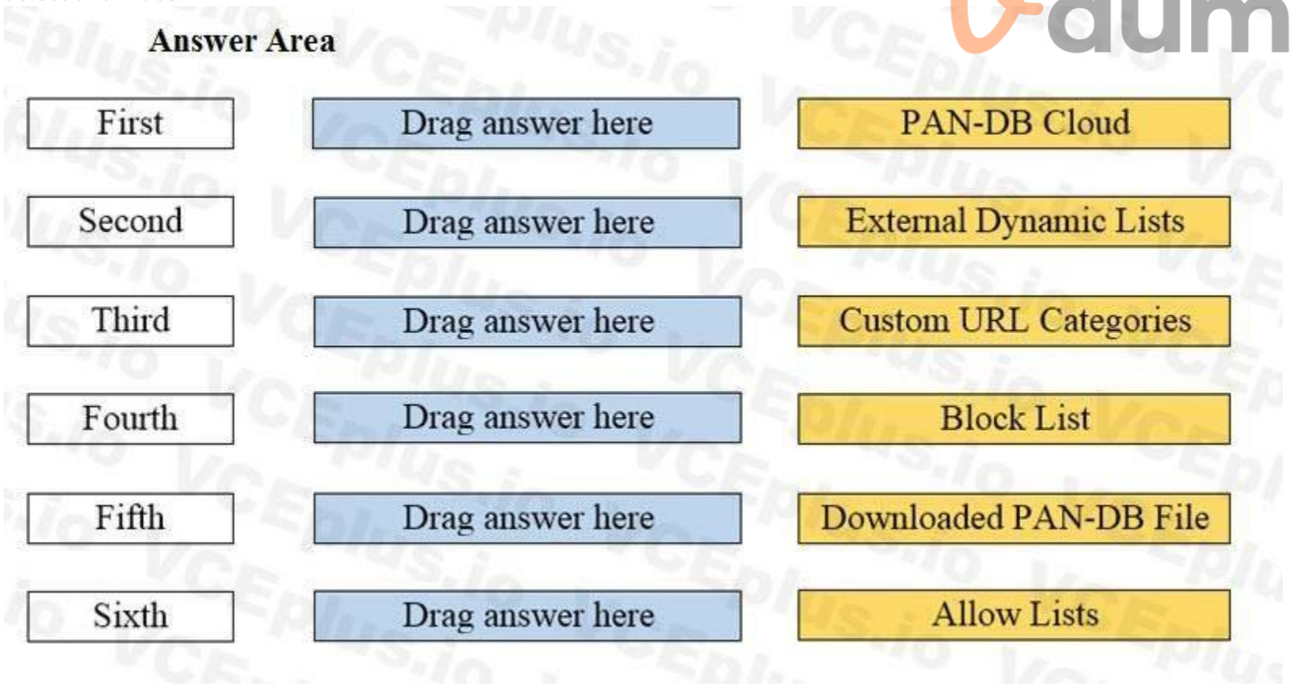
QUESTION 62
Given the screenshot, what are two correct statements about the logged traffic? (Choose two.)

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.

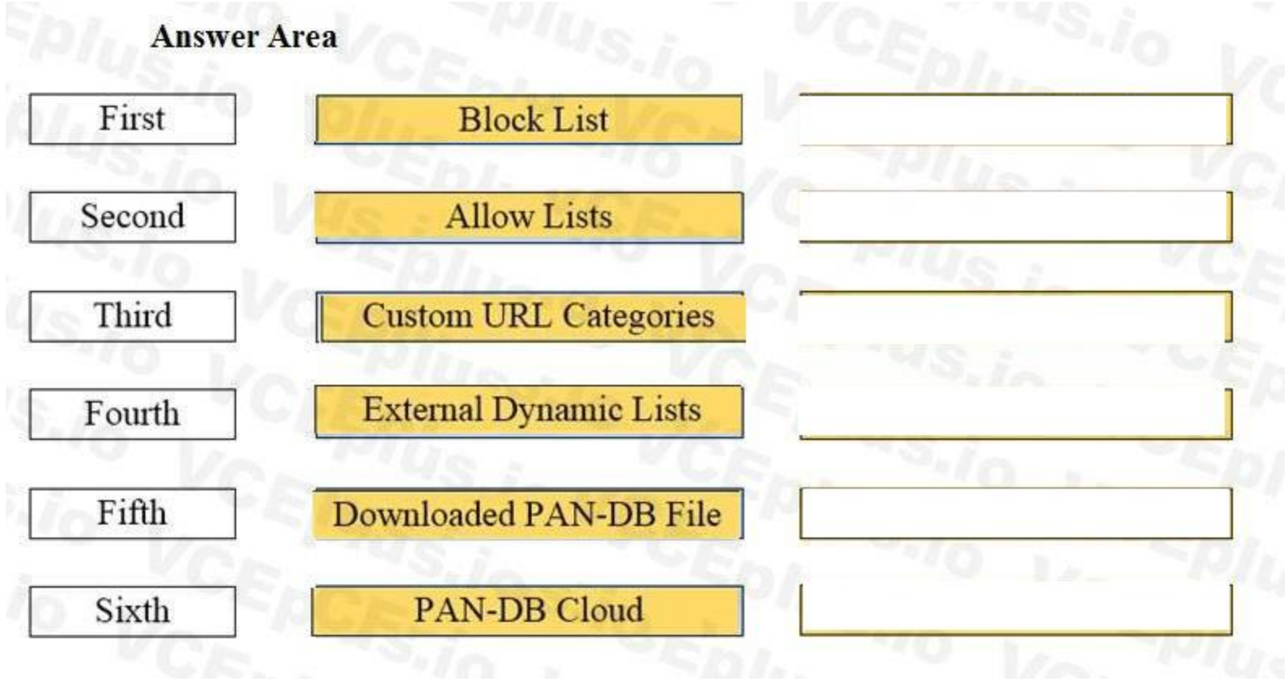
Correct Answer: C, D
Section:

QUESTION 63
DRAG DROP
Arrange the correct order that the URL classifications are processed within the system.

Select and Place:



Correct Answer:

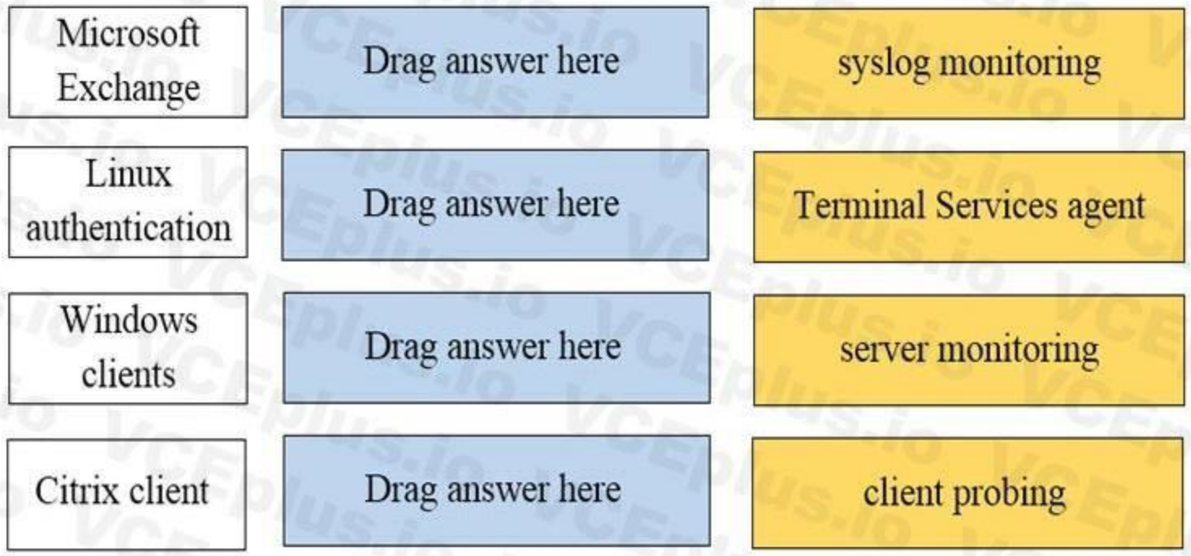


Section:
Explanation:

QUESTION 64
DRAG DROP
Match the network device with the correct User-ID technology.

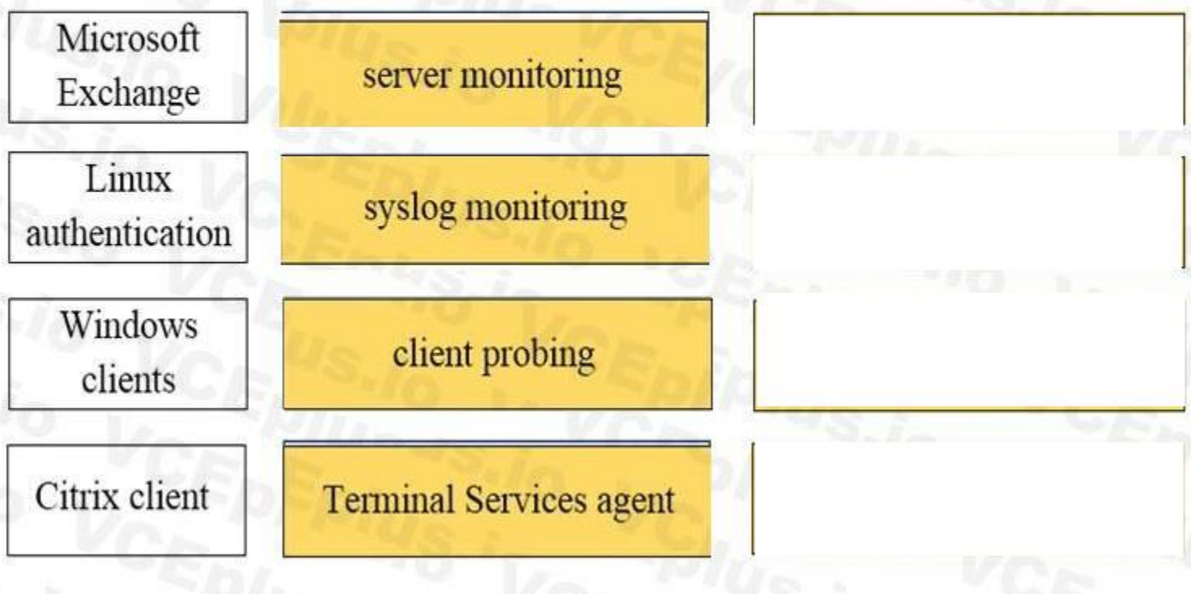
Select and Place:

Answer Area



Correct Answer:

Answer Area

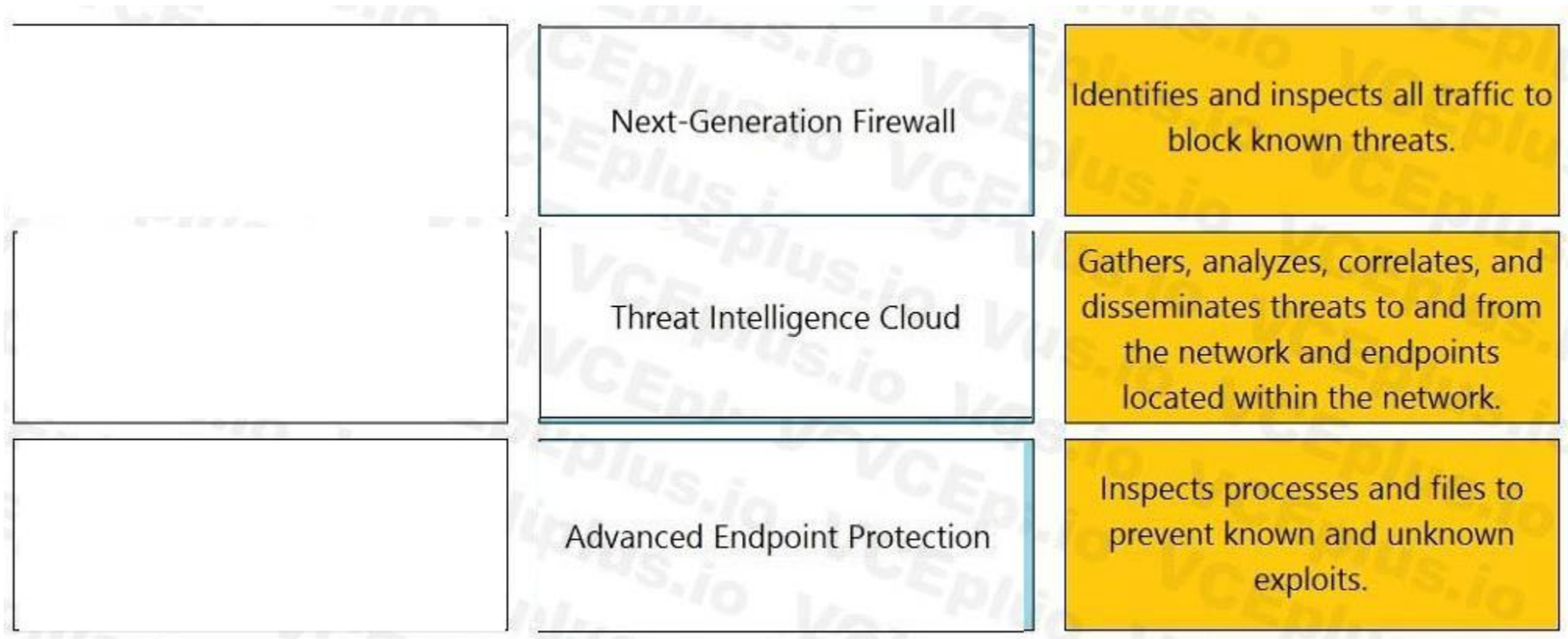


Section:
Explanation:

QUESTION 65
DRAG DROP
Match each feature to the DoS Protection Policy or the DoS Protection Profile.

Select and Place:

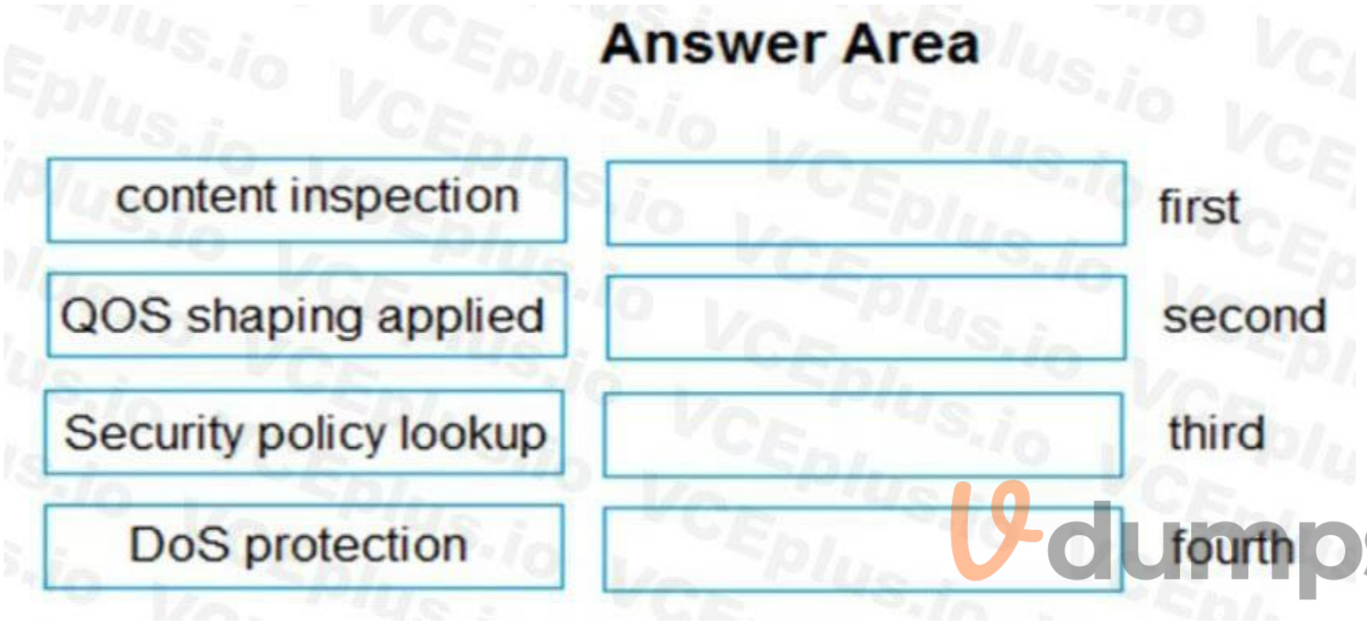
Correct Answer:



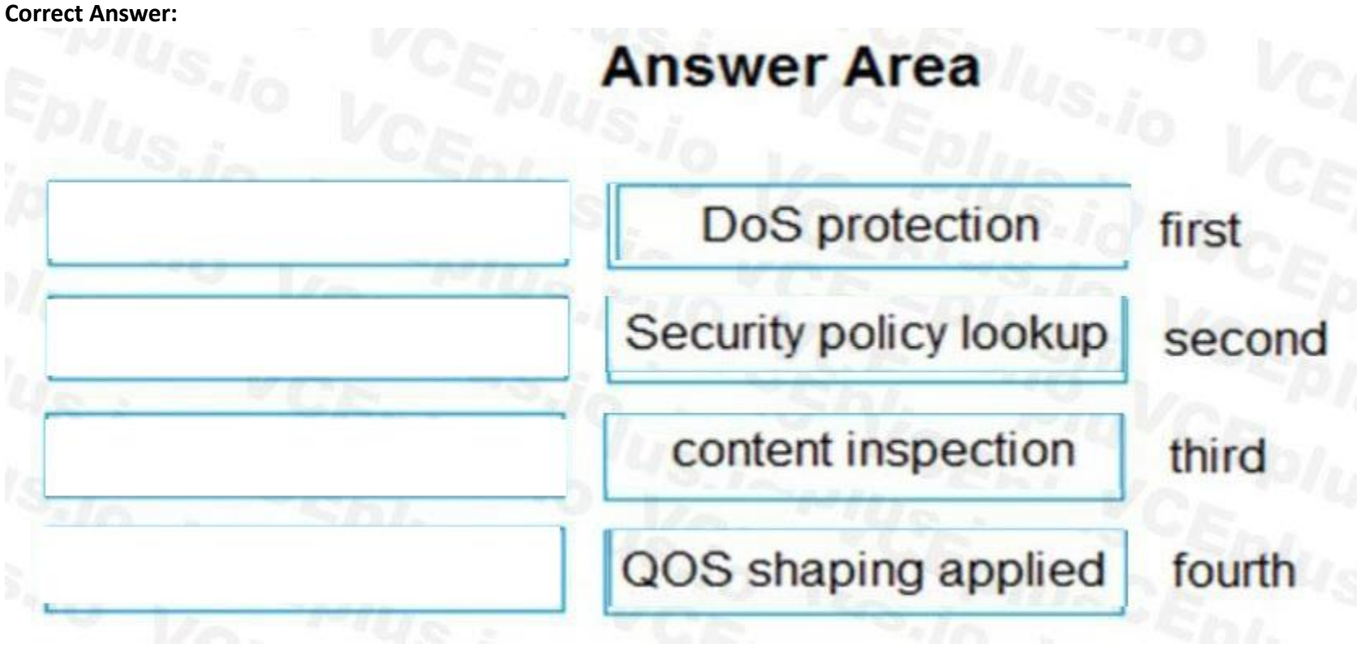
Section:
Explanation:

QUESTION 66
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 67
DRAG DROP
Place the steps in the correct packet-processing order of operations.

Select and Place:

Correct Answer:

Section:
Explanation:

QUESTION 68
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 69
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 70
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 71
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 72
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 73
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 74
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 75
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 76
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 77

What can be used as match criteria for creating a dynamic address group?

A. Usernames
B. IP addresses
C. Tags
D. MAC addresses

Correct Answer: C
Section:

QUESTION 78
An administrator needs to allow users to use only certain email applications.
How should the administrator configure the firewall to restrict users to specific email applications?

A. Create an application filter and filter it on the collaboration category, email subcategory.
B. Create an application group and add the email applications to it.
C. Create an application filter and filter it on the collaboration category.
D. Create an application group and add the email category to it.

Correct Answer: B
Section:

QUESTION 79
An administrator has an IP address range in the external dynamic list and wants to create an exception for one specific IP address in this address range.
Which steps should the administrator take?

A. Add the address range to the Manual Exceptions list and exclude the IP address by selecting the entry.
B. Add each IP address in the range as a list entry and then exclude the IP address by adding it to the Manual Exceptions list.
C. Select the address range in the List Entries list. A column will open with the IP addresses. Select the entry to exclude.
D. Add the specific IP address from the address range to the Manual Exceptions list by using regular expressions to define the entry.

Correct Answer: D
Section:

QUESTION 80
An administrator is implementing an exception to an external dynamic list by adding an entry to the list manually. The administrator wants to save the changes, but the OK button is grayed out.
What are two possible reasons the OK button is grayed out? (Choose two.)

A. The entry contains wildcards.
B. The entry is duplicated.
C. The entry doesn't match a list entry.
D. The entry matches a list entry.

Correct Answer: B, C
Section:

QUESTION 81

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	CorObj6006	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 82
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 83
Which two matching criteria are used when creating a Security policy involving NAT? (Choose two.)

A. Post-NAT address

B. Post-NAT zone
C. Pre-NAT zone
D. Pre-NAT address

Correct Answer: B, D
Section:

QUESTION 84
What are three valid information sources that can be used when tagging users to dynamic user groups? (Choose three.)

A. Blometric scanning results from iOS devices
B. Firewall logs
C. Custom API scripts
D. Security Information and Event Management Systems (SIEMS), such as Splun
E. DNS Security service

Correct Answer: B, C, E
Section:

QUESTION 85
What is the maximum volume of concurrent administrative account sessions?

A. Unlimited
B. 2
C. 10
D. 1

Correct Answer: C
Section:

QUESTION 86
In a File Blocking profile, which two actions should be taken to allow file types that support critical apps? (Choose two.)

A. Clone and edit the Strict profile.
B. Use URL filtering to limit categories in which users can transfer files.
C. Set the action to Continue.
D. Edit the Strict profile.

Correct Answer: A, D
Section:

QUESTION 87
Where within the firewall GUI can all existing tags be viewed?

A. Network > Tags
B. Monitor > Tags
C. Objects > Tags

D. Policies > Tags

Correct Answer: C
Section:

QUESTION 88
Which Security profile must be added to Security policies to enable DNS Signatures to be checked?

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

Correct Answer: D
Section:

QUESTION 89
Which Security profile would you apply to identify infected hosts on the protected network uwall user database?

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

Correct Answer: A
Section:

QUESTION 90
What can be achieved by disabling the Share Unused Address and Service Objects with Devices setting on Panorama?

A. Increase the backup capacity for configuration backups per firewall
B. Increase the per-firewall capacity for address and service objects
C. Reduce the configuration and session synchronization time between HA pairs
D. Reduce the number of objects pushed to a firewall

Correct Answer: D
Section:

QUESTION 91
The NetSec Manager asked to create a new firewall Local Administrator profile with customized privileges named NewAdmin. This new administrator has to authenticate without inserting any username or password to access the WebUI.
What steps should the administrator follow to create the New_Admin Administrator profile?

A. 1. Select the "Use only client certificate authentication" check box.
B. Set Role to Role Based.
C. Issue to the Client a Certificate with Common Name = NewAdmin
D. 1. Select the "Use only client certificate authentication" check box.

E. Set Role to Dynamic.
F. Issue to the Client a Certificate with Certificate Name = NewAdmin
G. 1. Set the Authentication profile to Local.
H. Select the "Use only client certificate authentication" check box.
I. Set Role to Role Based.
J. 1. Select the "Use only client certificate authentication" check box.
K. Set Role to Dynamic.
L. Issue to the Client a Certificate with Common Name = New Admin

Correct Answer: B
Section:

QUESTION 92
Why does a company need an Antivirus profile?

A. To prevent command-and-control traffic
B. To protect against viruses, worms, and trojans
C. To prevent known exploits
D. To prevent access to malicious web content

Correct Answer: B
Section:

QUESTION 93
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.

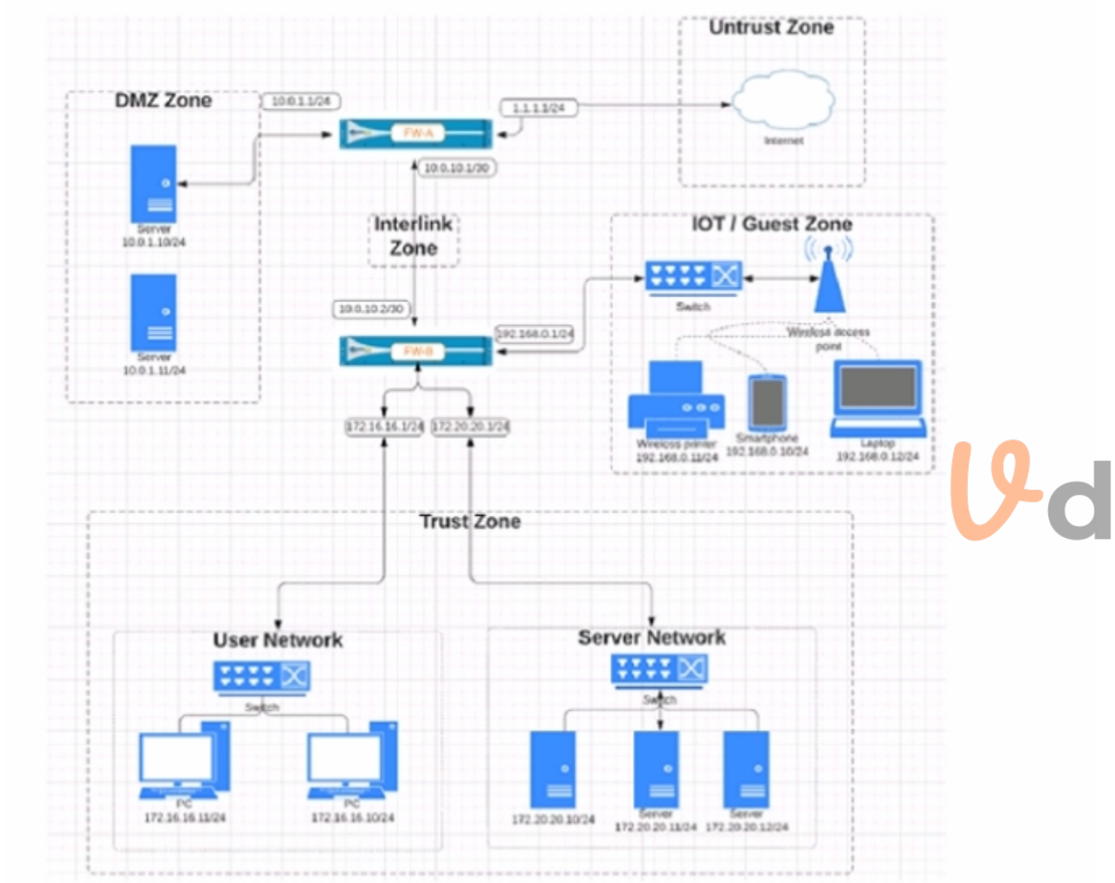
QUESTION 94
Which three types of Source NAT are available to users inside a NGFW? (Choose three.)

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 95
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 96
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 97
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 98
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 99
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 100
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 101
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 102
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 103
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 104
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 105
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 106
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 107
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 108
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