Exam Questions PCNSA

Palo Alto Networks Certified Network Security Administrator

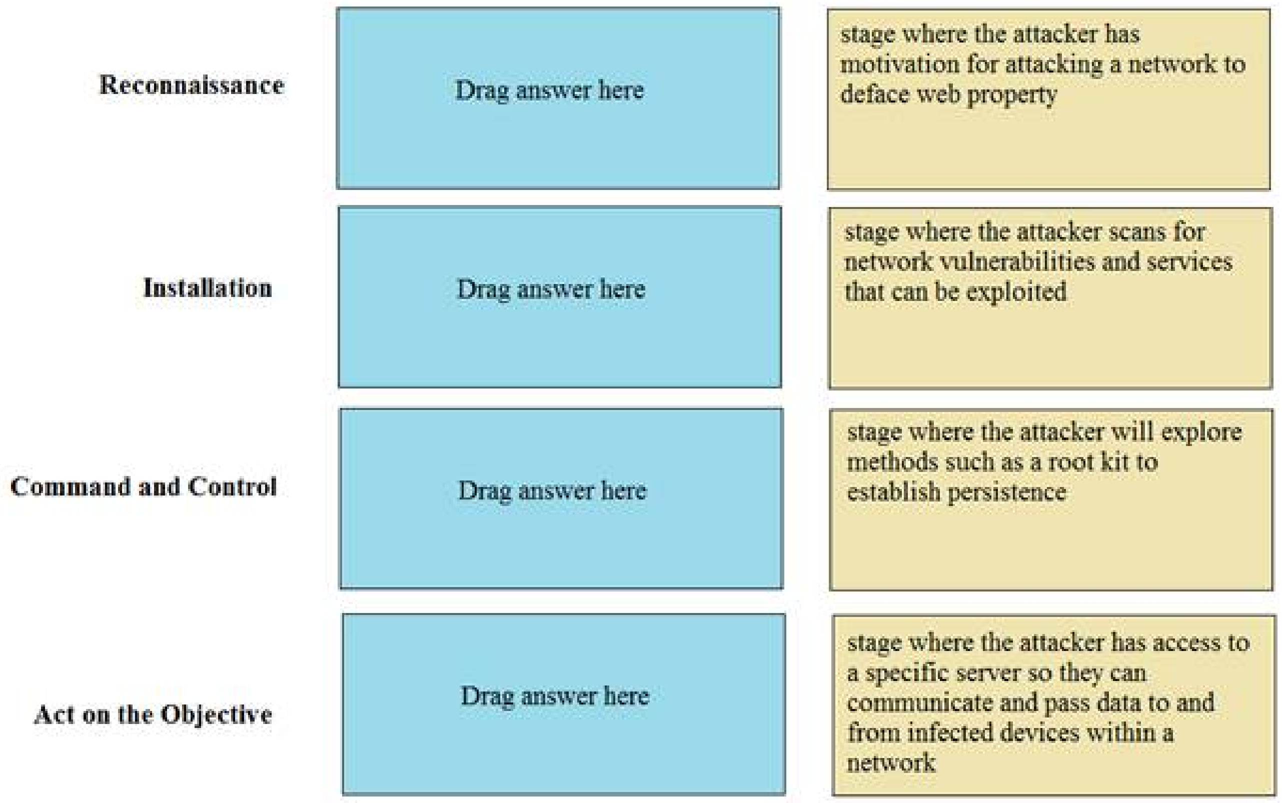
https://www.2passeasy.com/dumps/PCNSA/

NEW QUESTION 1
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

Answer: B

NEW QUESTION 2
DRAG DROP
Match the Cyber-Attack Lifecycle stage to its correct description.



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

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 3
Actions can be set for which two items in a URL filtering security profile? (Choose two.)

A. Block List
B. Custom URL Categories
C. PAN-DB URL Categories
D. Allow List

Answer: AD

Explanation:
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/url-filtering/url-filtering-concepts/url-filtering-profile-actions

NEW QUESTION 4
Which information is included in device state other than the local configuration?

A.

uncommitted changes
B. audit logs to provide information of administrative account changes
C. system logs to provide information of PAN-OS changes
D. device group and template settings pushed from Panorama

Answer: D

Explanation:
Reference:https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/device/device-setup-operations.html

NEW QUESTION 5
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

Answer: CD

NEW QUESTION 6
Which User-ID mapping method should be used for an environment with clients that do not authenticate to Windows Active Directory?

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

Answer: C

Explanation:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/user-id/map-ip-addresses-to-users/map-ip-addresses-to-usernames-using-captive-portal.html

NEW QUESTION 7
Which statement best describes the use of Policy Optimizer?

A. Policy Optimizer can display which Security policies have not been used in the last 90 days
B. Policy Optimizer on a VM-50 firewall can display which Layer 7 App-ID Security policies have unused applications
C. Policy Optimizer can add or change a Log Forwarding profile for each Secunty policy selected
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

Answer: B

NEW QUESTION 8
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

Answer: B

NEW QUESTION 9
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.

Answer: ABC

Explanation:
DNS Security subscription enables users to access real-time protections using advanced predictive analytics. When techniques such as DGA/DNS tunneling detection and machine learning are used, threats hidden within DNS traffic can be proactively identified and shared through an infinitely scalable cloud service. Because the DNS signatures and protections are stored in a cloud-based architecture, you can access the full database of ever-expanding signatures that have been generated using a multitude of data sources. This list of signatures allows you to defend against an array of threats using DNS in real- time against newly generated malicious domains. To combat future threats, updates to the analysis, detection, and prevention capabilities of the DNS Security service will be available through content releases. To access the DNS Security service, you must have a Threat Prevention license and DNS Security license.

NEW QUESTION 10
You need to allow users to access the office–suite 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.

Answer: C

NEW QUESTION 10
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>.

Answer: C

NEW QUESTION 14
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.

Answer: C

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

NEW QUESTION 15
Which two settings allow you to restrict access to the management interface? (Choose two)

A. Mastered
B. Not Mastered

Answer: A

NEW QUESTION 20
The PowerBall Lottery has reached an unusually high value this week. Your company has decided to raise morale by allowing employees to access the PowerBall Lottery website (www.powerball.com) for just this week. However, the company does not want employees to access any other websites also listed in the URL filtering “gambling” category.
Which method allows the employees to access the PowerBall Lottery website but without unblocking access to the “gambling” URL category?

A. Add just the URL www.powerball.com to a Security policy allow rule.
B.

Manually remove powerball.com from the gambling URL category.
C. Add *.powerball.com to the URL Filtering allow list.
D. Create a custom URL category, add *.powerball.com to it and allow it in the Security Profile.

Answer: CD

NEW QUESTION 24
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.

Answer: BC

NEW 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

Answer: B

NEW QUESTION 31
Which file is used to save the running configuration with a Palo Alto Networks firewall?

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

Answer: A

NEW QUESTION 33
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>

Answer: A

NEW QUESTION 34
Which interface type is used to monitor traffic and cannot be used to perform traffic shaping?

A. Mastered
B. Not Mastered

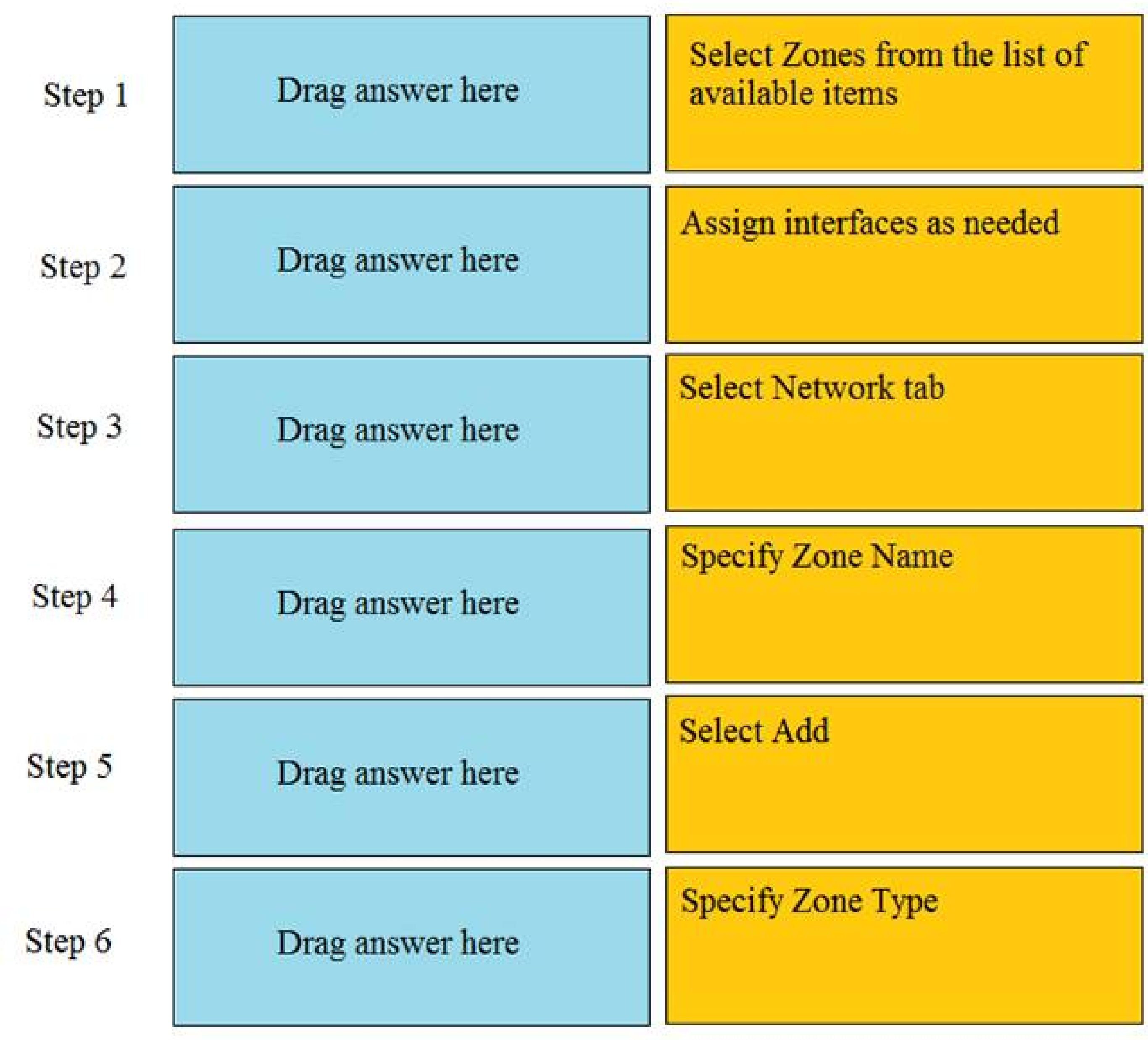
Answer: A

NEW QUESTION 38
Which license must an administrator acquire prior to downloading Antivirus updates for use with the firewall?

A. URL filtering
B. Antivirus
C. WildFire
D. Threat Prevention

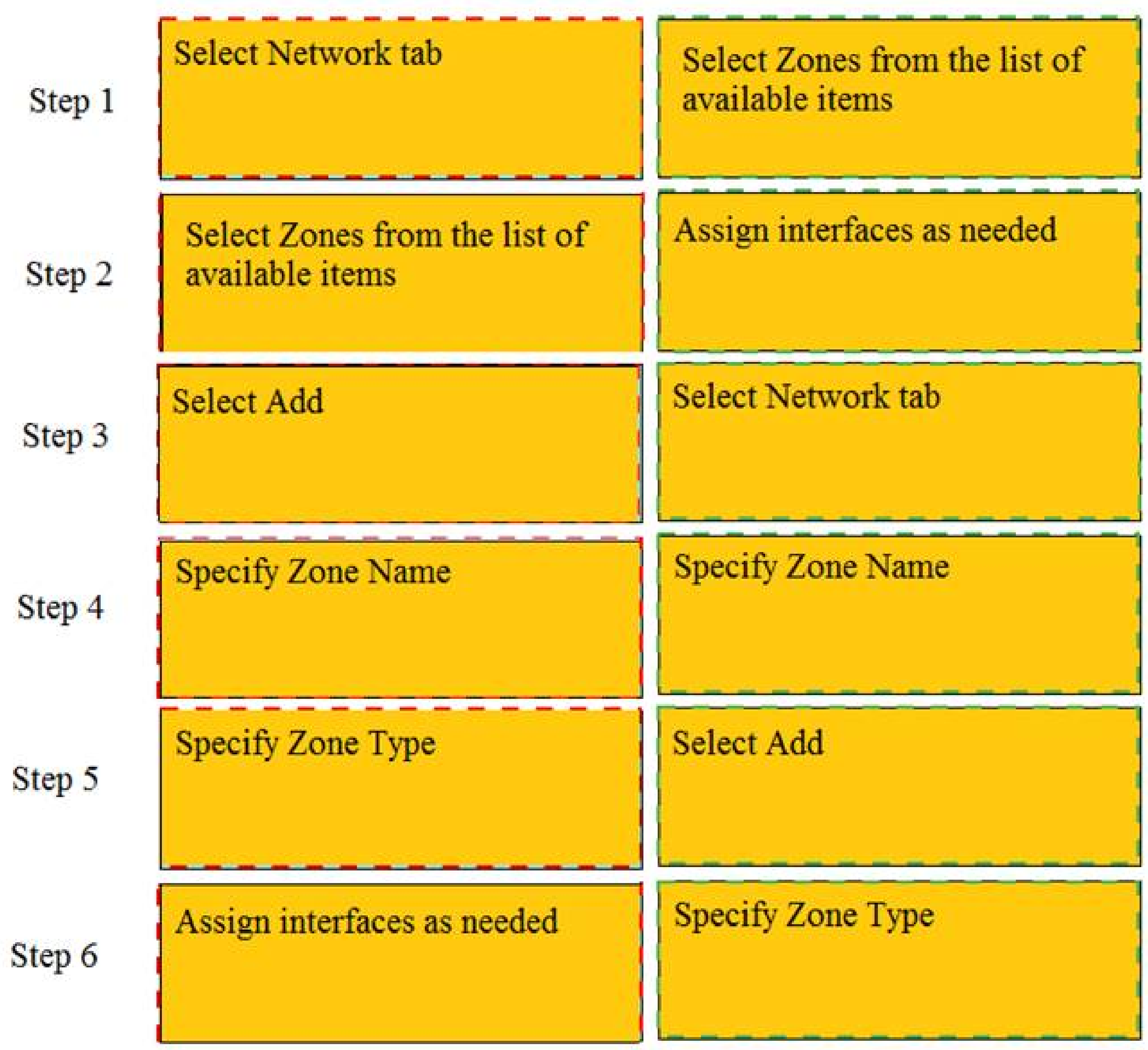
Answer: D

NEW QUESTION 43
DRAG DROP
Order the steps needed to create a new security zone with a Palo Alto Networks firewall.



Step 1	Drag answer here	Select Zones from the list of available items
Step 2	Drag answer here	Assign interfaces as needed
Step 3	Drag answer here	Select Network tab
Step 4	Drag answer here	Specify Zone Name
Step 5	Drag answer here	Select Add
Step 6	Drag answer here	Specify Zone Type

Answer:



Step 1	Select Network tab	Select Zones from the list of available items
Step 2	Select Zones from the list of available items	Assign interfaces as needed
Step 3	Select Add	Select Network tab
Step 4	Specify Zone Name	Specify Zone Name
Step 5	Specify Zone Type	Select Add
Step 6	Assign interfaces as needed	Specify Zone Type

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Step 1 – Select network tab
Step 2 – Select zones from the list of available items Step 3 – Select Add
Step 4 – Specify Zone Name Step 5 – Specify Zone Type
Step 6 – Assign interfaces as needed

NEW QUESTION 46
All users from the internal zone must be allowed only HTTP access to a server in the DMZ zone.
Complete the empty field in the Security policy using an application object to permit only this type of access.
Source Zone: Internal - Destination Zone: DMZ Zone -
Application:
Service: application-default -
Action: allow

A. Application = "any"
B. Application = "web-browsing"
C. Application = "ssl"
D. Application = "http"

Answer: B

NEW QUESTION 48
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.

Answer: B

NEW QUESTION 52
Identify the correct order to configure the PAN-OS integrated USER-ID agent.
* 3. add the service account to monitor the server(s)

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

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

Answer: D

NEW QUESTION 56
What does an application filter help you to do?

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

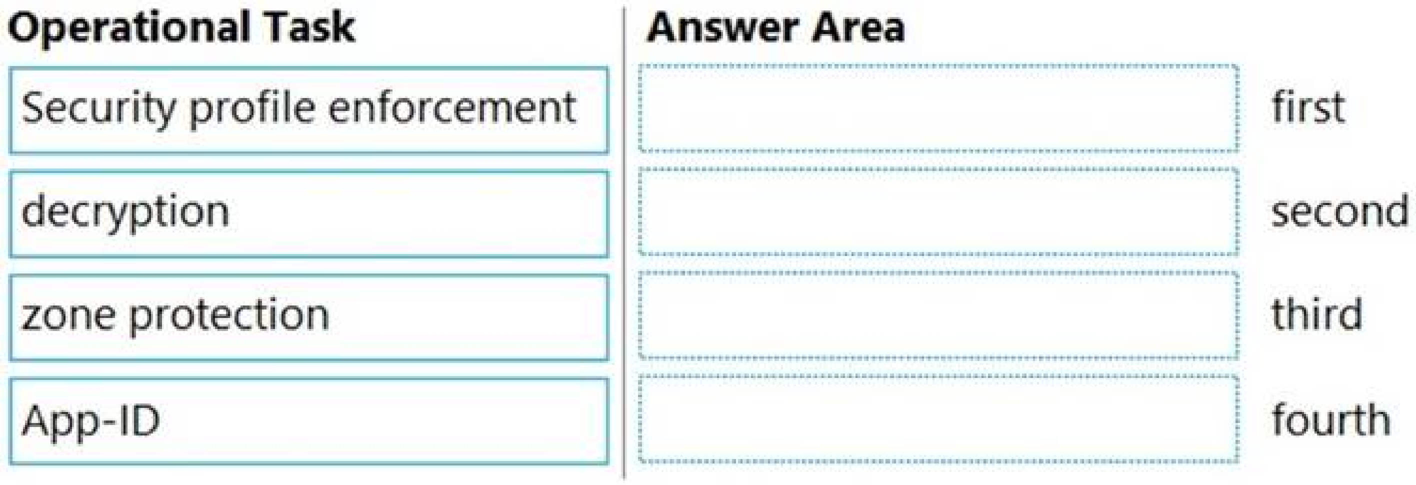
Answer: C

NEW QUESTION 60
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

Answer: A

NEW QUESTION 62
DRAG DROP
Place the steps in the correct packet-processing order of operations.



Operational Task
Security profile enforcement
decryption
zone protection
App-ID

Answer Area
first
second
third
fourth

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW 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. Mastered
B. Not Mastered

Answer: A

NEW QUESTION 68
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

Answer: AB

Explanation:
Reference:http://live.paloaltonetworks.com//t5/image/serverpage/image- id/12862i950F549C7D4E6309

NEW QUESTION 72
Which administrator type provides more granular options to determine what the administrator can view and modify when creating an administrator account?

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

Answer: C

NEW QUESTION 77
The Palo Alto Networks NGFW was configured with a single virtual router named VR-1 What changes are required on VR-1 to route traffic between two interfaces on the NGFW?

A. Add zones attached to interfaces to the virtual router
B. Add interfaces to the virtual router
C. Enable the redistribution profile to redistribute connected routes
D. Add a static routes to route between the two interfaces

Answer: D

Explanation:

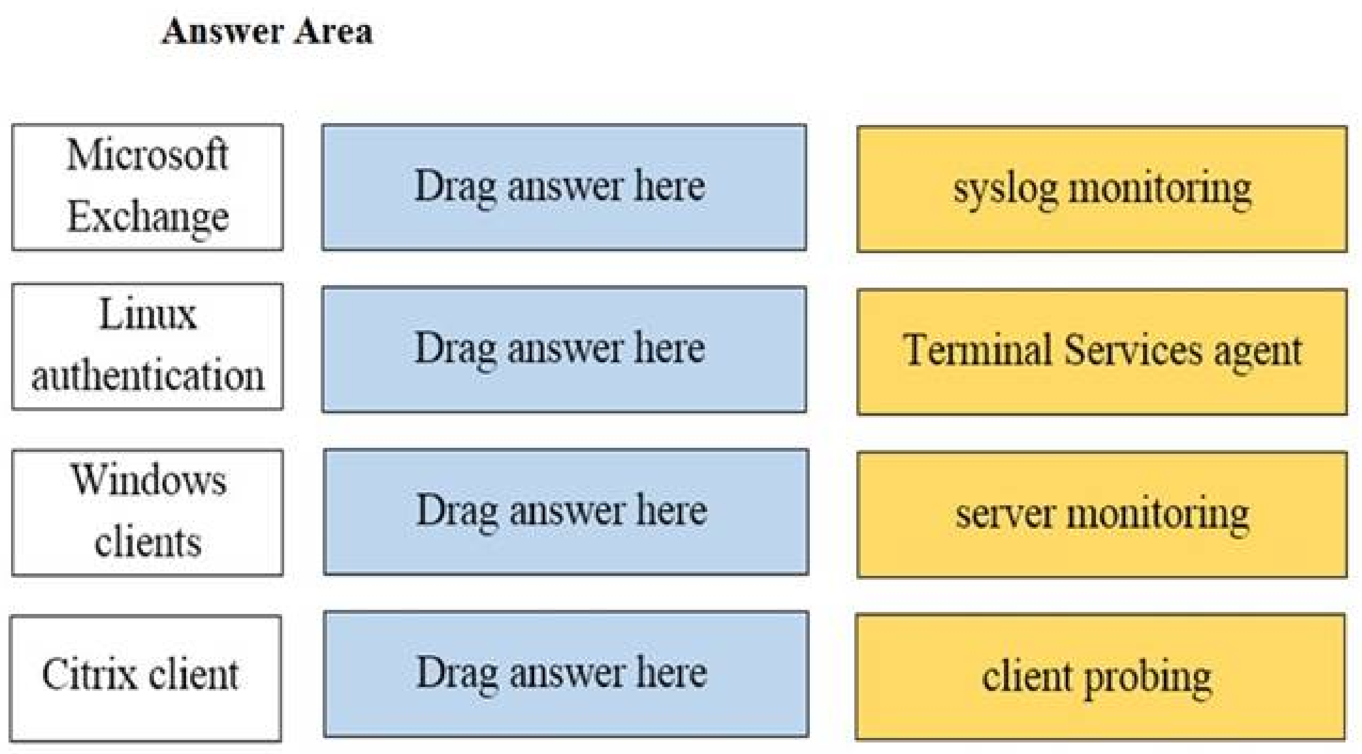
NEW QUESTION 81
What action will inform end users when their access to Internet content is being restricted?

A. Create a custom 'URL Category' object with notifications enabled.
B: Publish monitoring data for Security policy deny logs.
C. Ensure that the 'site access" setting for all URL sites is set to 'alert'.
D. Enable 'Response Pages' on the interface providing Internet access.

Answer: D

Explanation:
Reference:https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface-help/device/device-response-pages.html

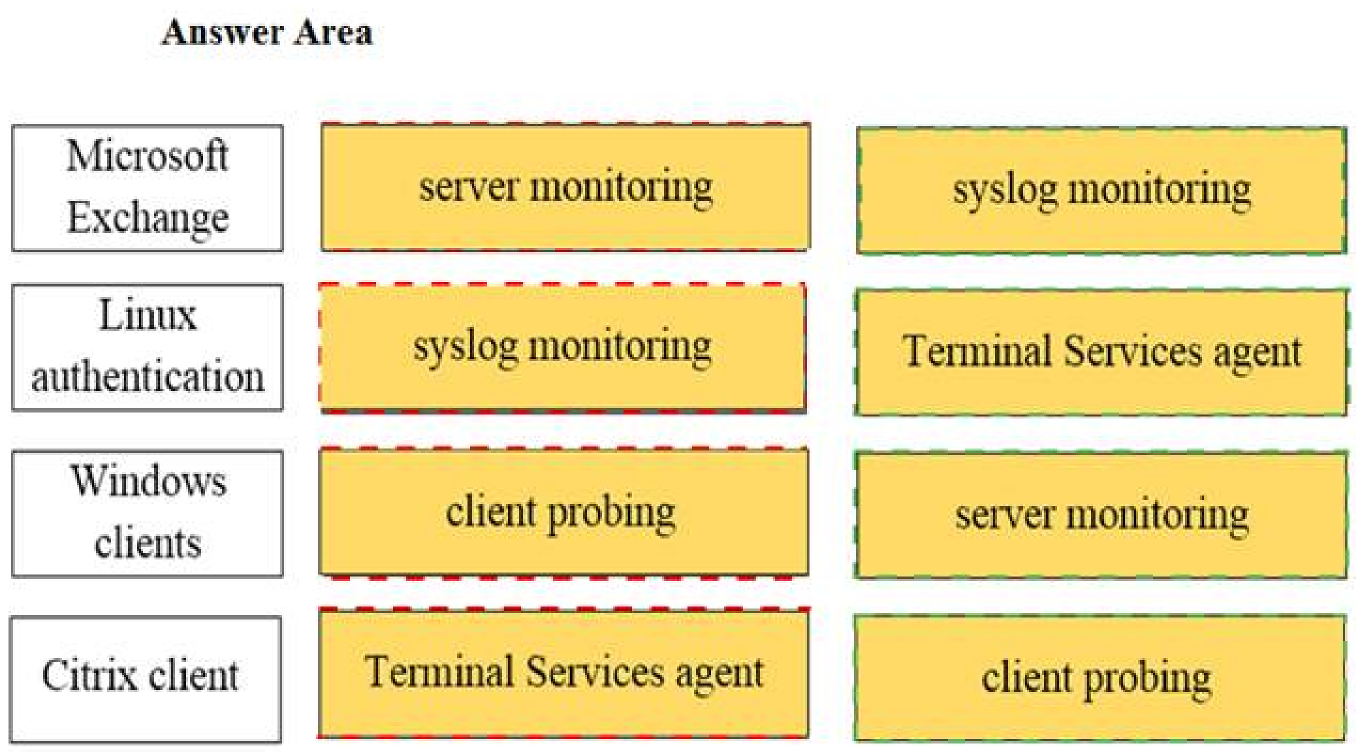
NEW QUESTION 83
DRAG DROP
Match the network device with the correct User-ID technology.



Answer Area

Microsoft Exchange	Drag answer here	syslog monitoring
Linux authentication	Drag answer here	Terminal Services agent
Windows clients	Drag answer here	server monitoring
Citrix client	Drag answer here	client probing

Answer:



Answer Area

Microsoft Exchange	server monitoring	syslog monitoring
Linux authentication	syslog monitoring	Terminal Services agent
Windows clients	client probing	server monitoring
Citrix client	Terminal Services agent	client probing

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Microsoft Exchange – Server monitoring
Linux authentication – syslog monitoring
Windows Client – client probing
Citrix client – Terminal Services agent

NEW QUESTION 88
When creating a custom URL category object, which is a valid type?

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

Answer: D

Explanation:
Reference:https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/objects/objects-custom-objects-url-category.html

NEW QUESTION 91
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

Answer: A

NEW QUESTION 94
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?

Security policy = drop, Gambling category in URL profile = allow
A.
B: Security policy = den
C. Gambling category in URL profile = block
D. Security policy = allow, Gambling category in URL profile = alert
E. Security policy = allo
F. Gambling category in URL profile = allow

Answer: C

NEW QUESTION 99
Which Palo Alto Networks firewall security platform provides network security for mobile endpoints by inspecting traffic deployed as internet gateways?

A. GlobalProtect

B. AutoFocus
C. Aperture
D. Panorama

Answer: A

Explanation:
GlobalProtect: GlobalProtect safeguards your mobile workforce by inspecting all traffic using your next-generation firewalls deployed as internet gateways, whether at the perimeter, in the Demilitarized Zone (DMZ), or in the cloud.

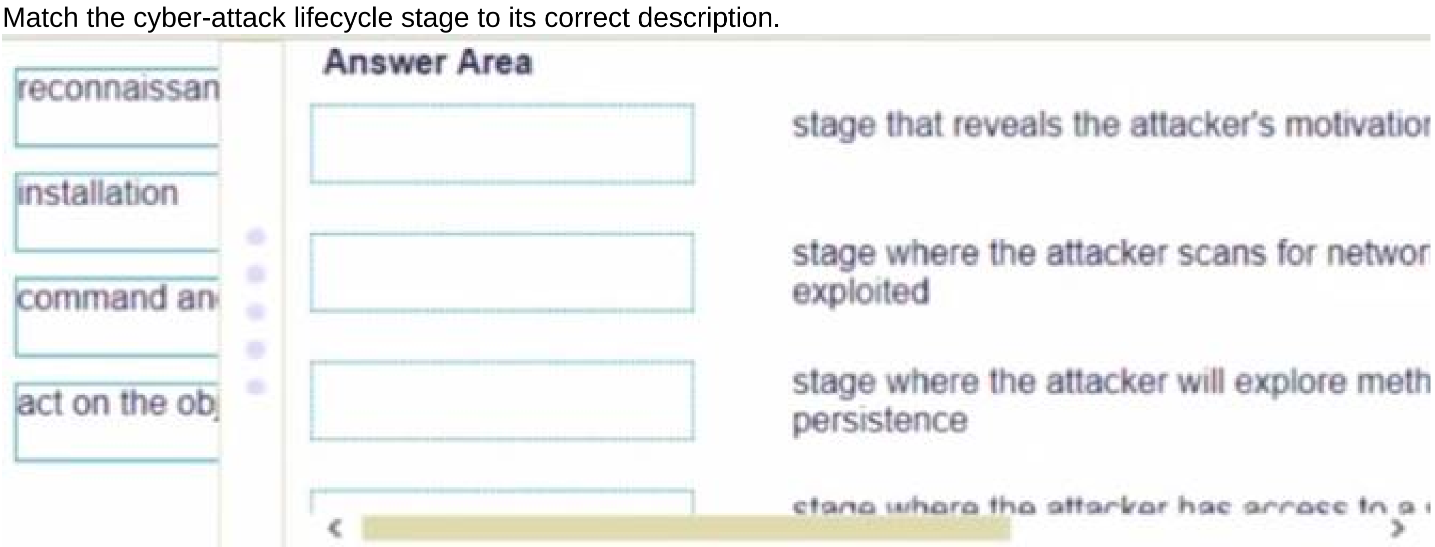
NEW QUESTION 103
Which link in the web interface enables a security administrator to view the security policy rules that match new application signatures?

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

Answer: D

Explanation:

NEW QUESTION 106
DRAG DROP
Match the cyber-attack lifecycle stage to its correct description.



reconnaissan
installation
command an
act on the ob

Answer Area

stage that reveals the attacker's motivatior

stage where the attacker scans for networ exploited

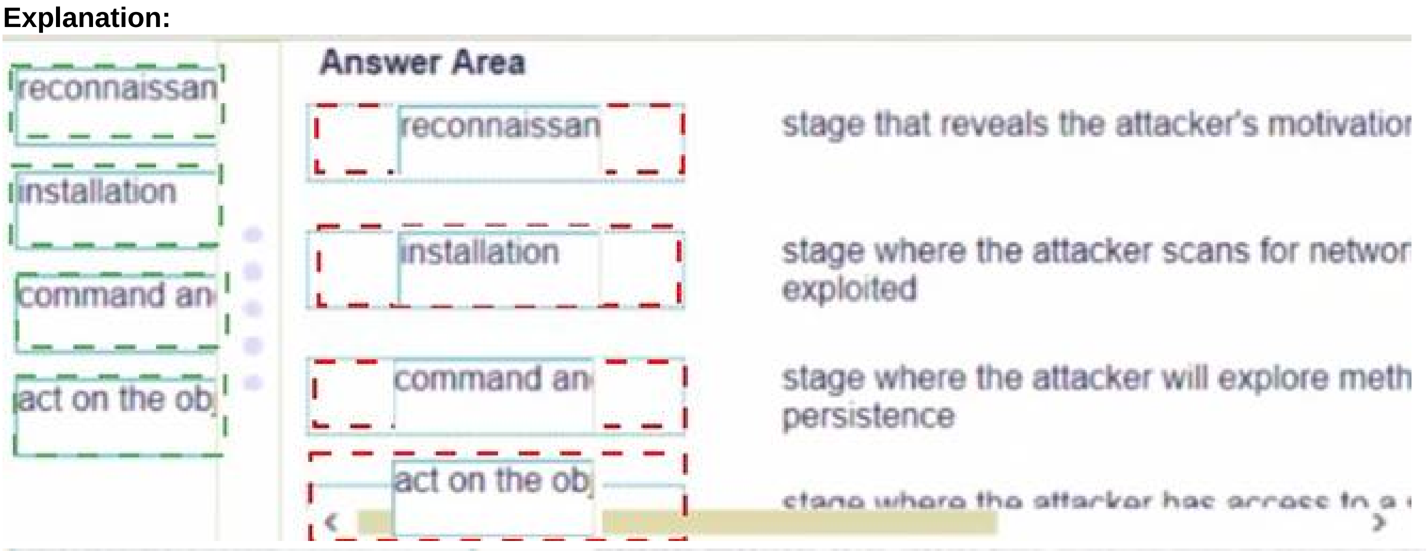
stage where the attacker will explore meth persistence

stage where the attacker has access to a

A. Mastered
B. Not Mastered

Answer: A

Explanation:



reconnaissan
installation
command an
act on the ob

Answer Area

reconnaissan — stage that reveals the attacker's motivatior

installation — stage where the attacker scans for networ exploited

command an — stage where the attacker will explore meth persistence

act on the ob — stage where the attacker has access to a

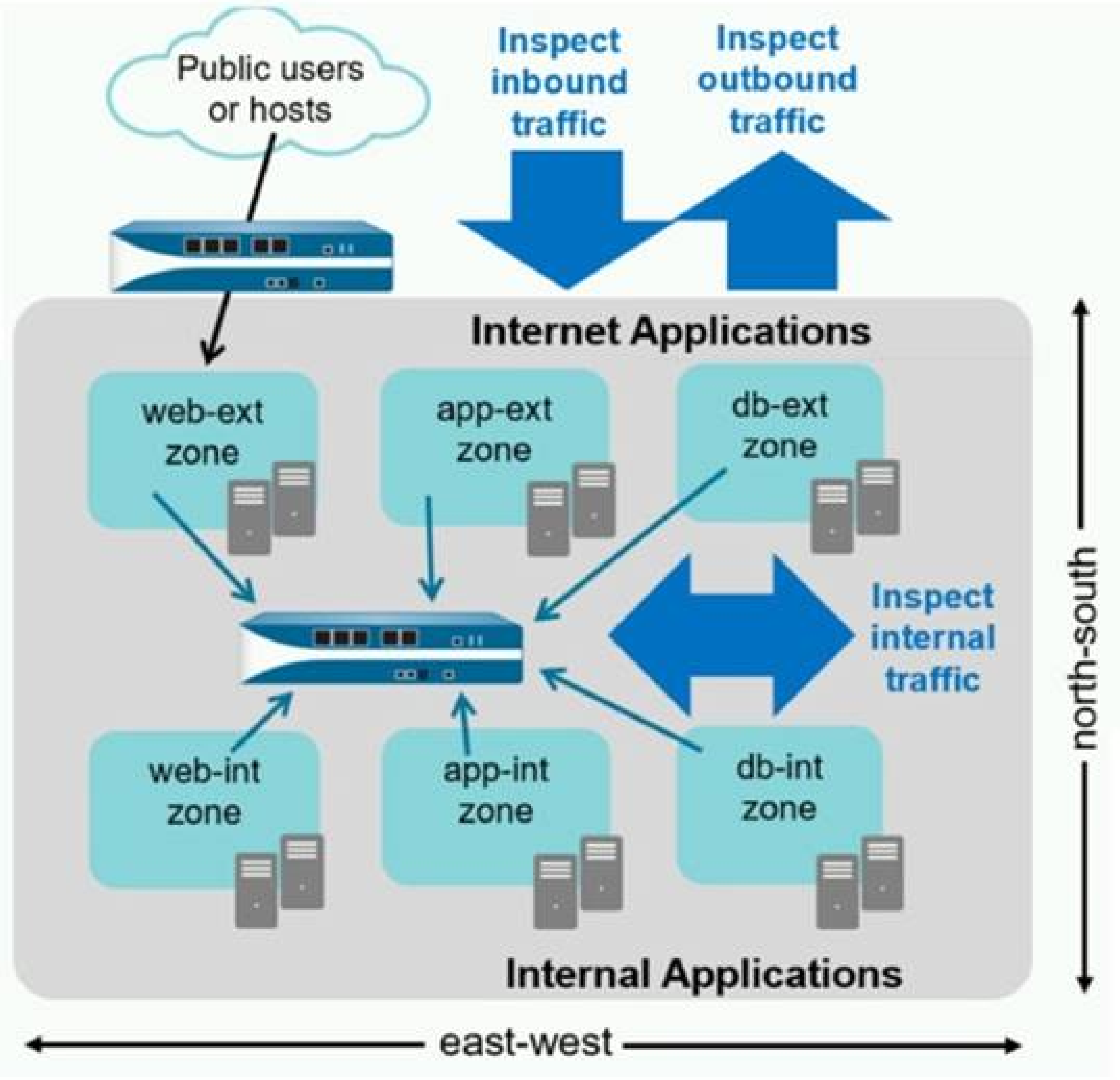
NEW QUESTION 109
An administrator is troubleshooting traffic that should match the interzone-default rule. However, the administrator doesn't see this traffic in the traffic logs on the firewall. The interzone-default was never changed from its default configuration.
Why doesn't the administrator see 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

Answer: D

NEW QUESTION 113

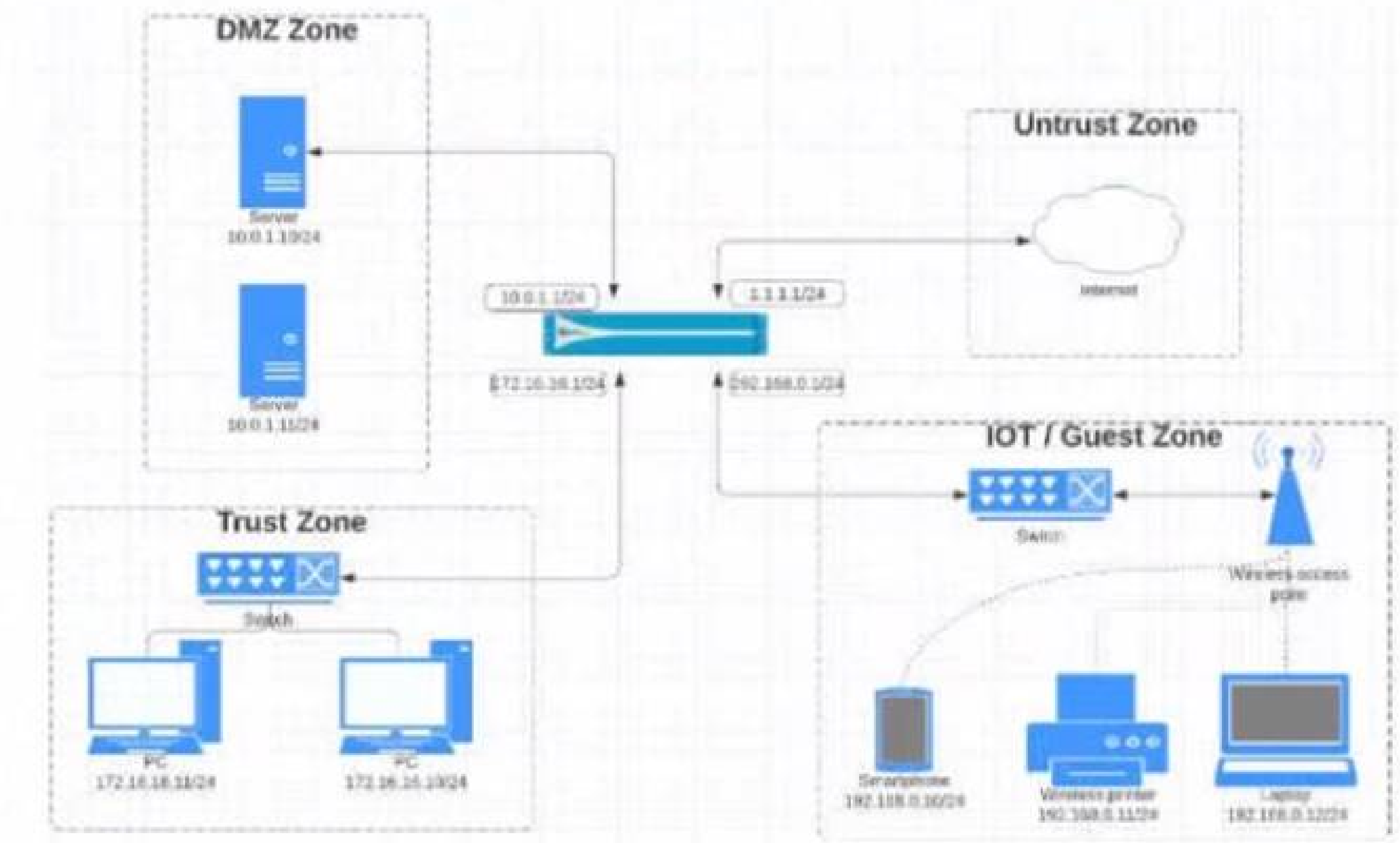
An administrator notices that protection is needed for traffic within the network due to malicious lateral movement activity. Based on the image shown, which traffic would the administrator need to monitor and block to mitigate the malicious activity?



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

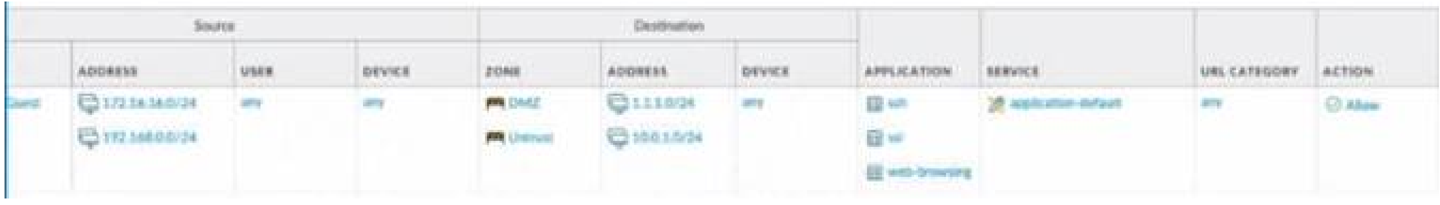
Answer: D

NEW QUESTION 114
View the diagram.



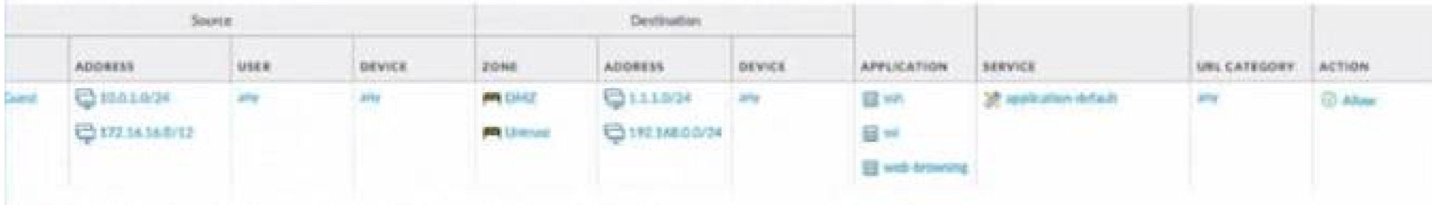
What is the most restrictive yet fully functional rule to allow general Internet and SSH traffic into both the DMZ and Untrust/Internet zones from each of the IOT/Guest and Trust Zones?

A)



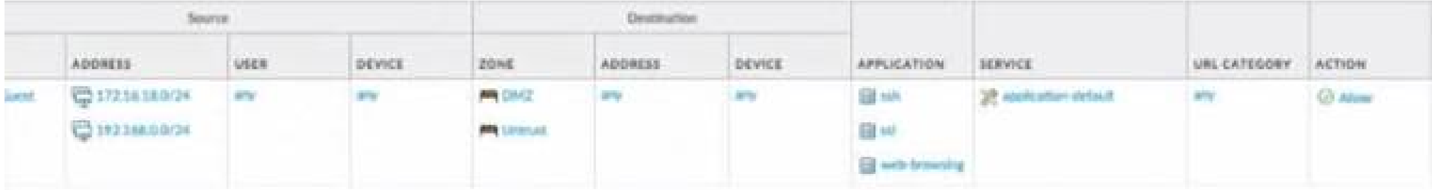
Source				Destination						
	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	URL CATEGORY	ACTION
Guest	172.16.16.0/24 192.168.0.0/24	any	any	DMZ Untrust	1.1.1.0/24 10.0.1.0/24	any	ssh ssl web-browsing	application-default	any	Allow

B)



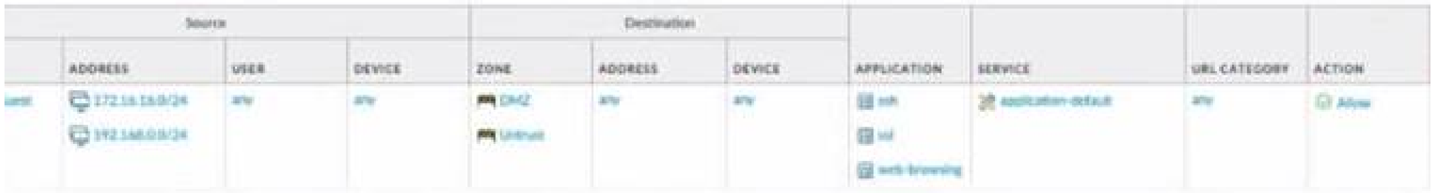
	Source			Destination						
	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	URL CATEGORY	ACTION
Guest	10.0.1.0/24 172.16.16.0/12	any	any	DMZ Untrust	1.1.1.0/24 192.168.0.0/24	any	ssh ssl web-browsing	application-default	any	Allow

C)



	Source			Destination						
	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	URL CATEGORY	ACTION
uest	172.16.18.0/24 192.168.0.0/24	any	any	DMZ Untrust	any	any	ssh ssl web-browsing	application-default	any	Allow

D)



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

A. Option A
B. Option B
C. Option C
D. Option D

Answer: C

NEW QUESTION 115
Which Palo Alto network security operating platform component provides consolidated policy creation and centralized management?

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

Answer: B

Explanation:

NEW QUESTION 116
An administrator needs to allow users to use their own office applications. How should the administrator configure the firewall to allow multiple applications in a dynamic environment?

A. Mastered
B. Not Mastered

Answer: A

Explanation:
An application filter is an object that dynamically groups applications based on application attributes that you define, including category, subcategory, technology, risk factor, and characteristic. This is useful when you want to safely enable access to applications that you do not explicitly sanction, but that you want users to be able to access. For example, you may want to enable employees to choose their own office programs (such as Evernote, Google Docs, or Microsoft Office 365) for business use. To safely enable these types of applications, you could create an application filter that matches on the Category business-systems and the Subcategory office-programs. As new applications office programs emerge and new App-IDs get created, these new applications will automatically match the filter you defined; you will not have to make any additional changes to your policy rulebase to safely enable any application that matches the attributes you defined for the filter. https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/app-id/use-application-objects- in -policy/create-an-application-filter.html

NEW QUESTION 121
In which section of the PAN-OS GUI does an administrator configure URL Filtering profiles?

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

Answer: C

Explanation:
An administrator can configure URL Filtering profiles in the Objects section of the PAN-OS GUI. A URL Filtering profile is a collection of URL filtering controls that you can apply to individual Security policy rules that allow access to the internet1. You can set site access for URL categories, allow or disallow user credential submissions, enable safe search enforcement, and various other settings1.
To create a URL Filtering profile, go to Objects > Security Profiles > URL Filtering and click Add. You can then specify the profile name, description, and settings for each URL category and action2. Youcan also configure other options such as User Credential Detection, HTTP Header Insertion, and URL Filtering Inline ML2. After creating the profile, you can attach it to a Security policy rule that allows web traffic2.

NEW QUESTION 122
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

Answer: A

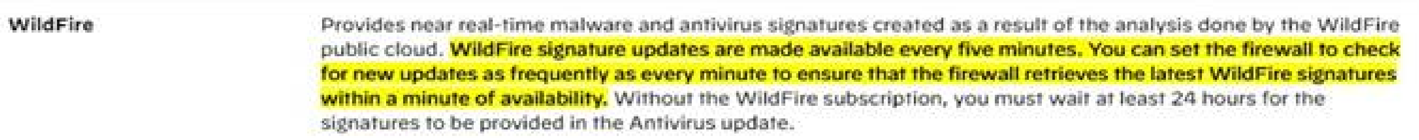
Explanation:
Another reason to choose the Windows agent over the integrated PAN-OS agent is to save processing cycles on the firewall’s management plane.

NEW QUESTION 123
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

Answer: B

Explanation:



WildFire	Provides near real-time malware and antivirus signatures created as a result of the analysis done by the WildFire public cloud. **WildFire signature updates are made available every five minutes. You can set the firewall to check for new updates as frequently as every minute to ensure that the firewall retrieves the latest WildFire signatures within a minute of availability.** Without the WildFire subscription, you must wait at least 24 hours for the signatures to be provided in the Antivirus update.

NEW QUESTION 124
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.

Answer: AD

NEW QUESTION 129
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

Answer: C

NEW QUESTION 133
Which user mapping method could be used to discover user IDs in an environment with multiple Windows domain controllers?

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

Answer: A

NEW QUESTION 134
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

Answer: C

Explanation:

NEW QUESTION 137
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

Answer: C

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

NEW QUESTION 142
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

Answer: C

NEW QUESTION 143
Which statement is true regarding a Best Practice Assessment?

A. The BPA tool can be run only on firewalls
B. It provides a percentage of adoption for each assessment data
C. The assessment, guided by an experienced sales engineer, helps determine the areas of greatest risk where you should focus prevention activities
D. It provides a set of questionnaires that help uncover security risk prevention gaps across all areas of network and security architecture

Answer: C

NEW QUESTION 145
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.

Answer: C

NEW QUESTION 146
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

Answer: A

NEW QUESTION 151
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

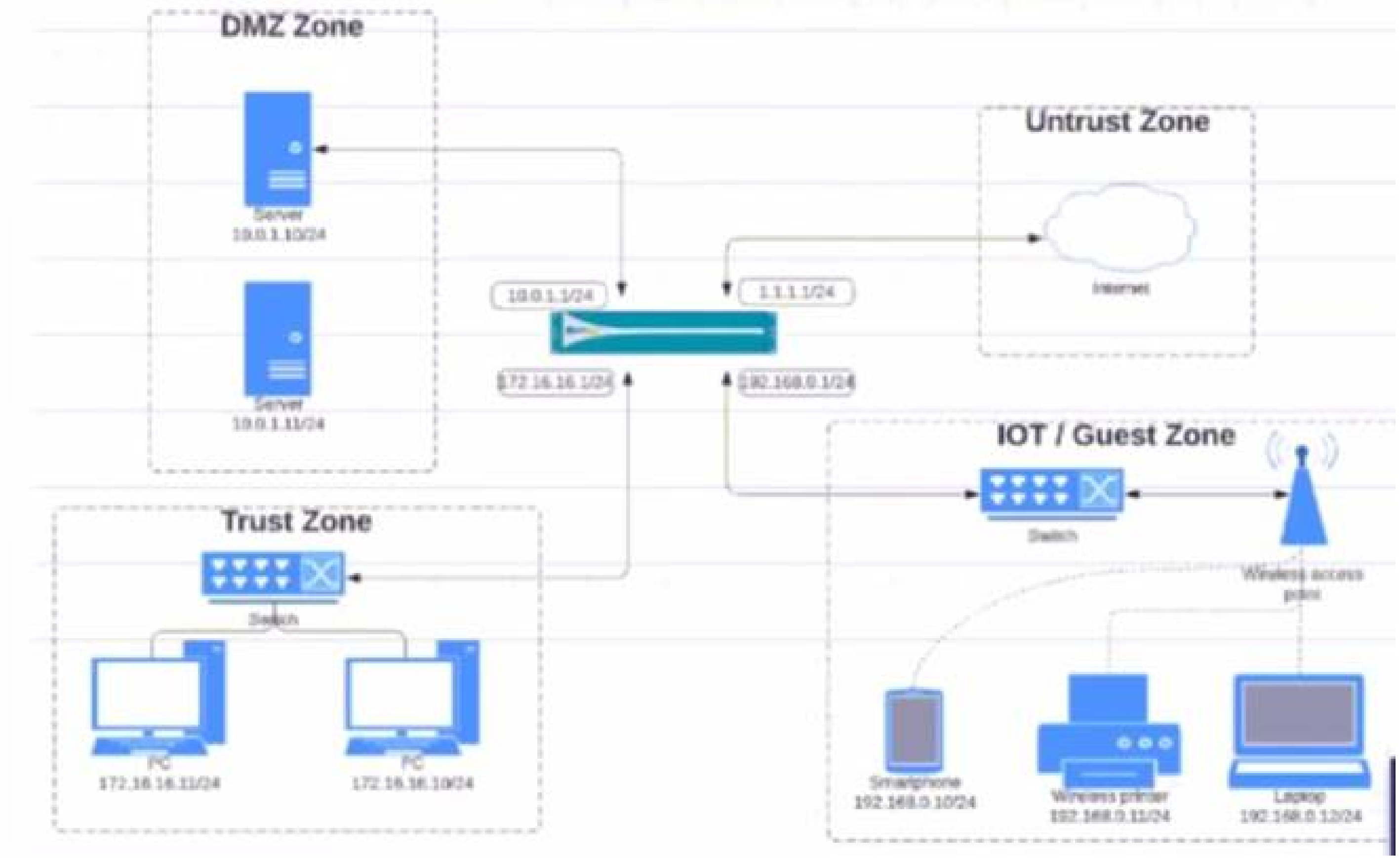
Answer: BD

NEW QUESTION 154
Palo Alto Networks firewall architecture accelerates content map minimizing latency using which two components'? (Choose two)

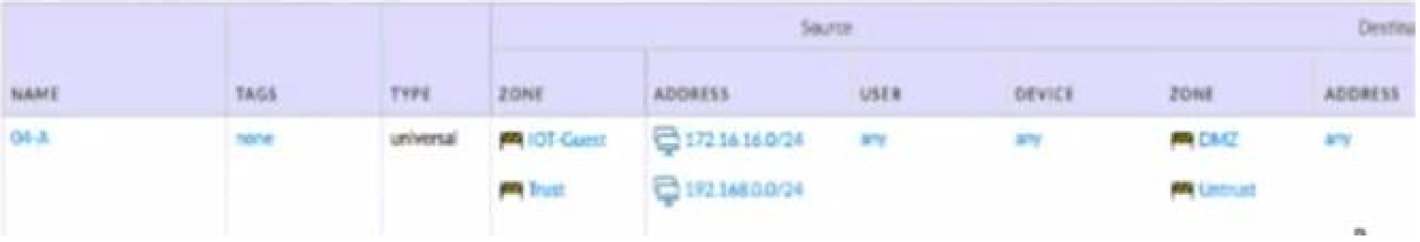
A. Network Processing Engine
B. Single Stream-based Engine
C. Policy Engine
D. Parallel Processing Hardware

Answer: B

NEW QUESTION 159
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

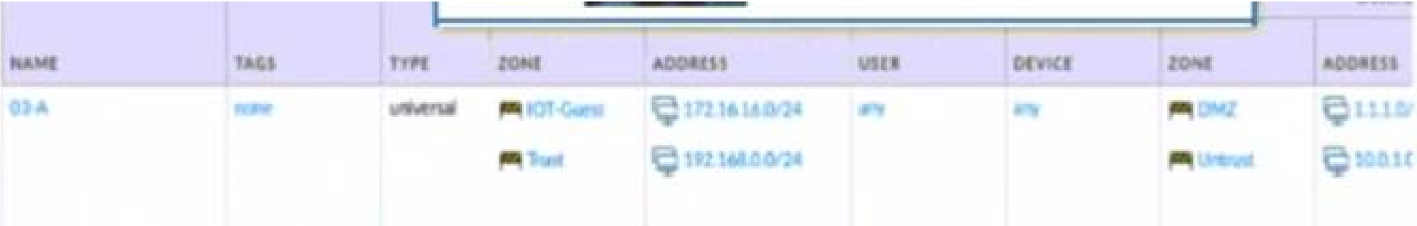


Which policy achieves the desired results?
A)



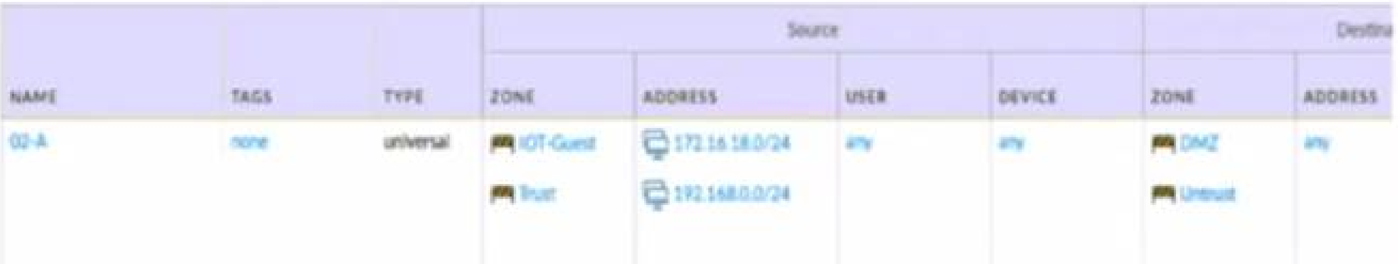
			Source				Destina	
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS
04-A	none	universal	IOT-Guest Trust	172.16.16.0/24 192.168.0.0/24	any	any	DMZ Untrust	any

B)



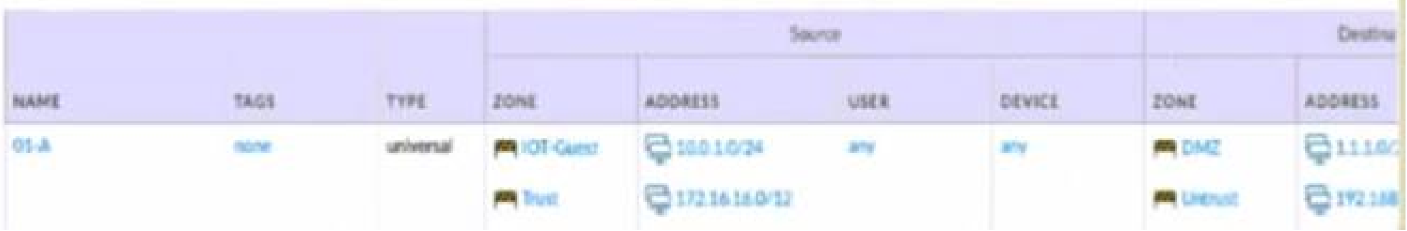
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS
03-A	none	universal	IOT-Guest Trust	172.16.16.0/24 192.168.0.0/24	any	any	DMZ Untrust	1.1.1.0/ 10.0.1.0

C)



			Source				Destina	
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS
02-A	none	universal	IOT-Guest Trust	172.16.18.0/24 192.168.0.0/24	any	any	DMZ Untrust	any

D)



			Source				Destina	
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS
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/ 192.168

A. Option
B. Option
C. Option
D. Option

Answer: C

NEW QUESTION 161
Which two features can be used to tag a user name so that it is included in a dynamic user group? (Choose two)

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

Answer: AD

Explanation:
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/url-filtering/url-filtering-concepts/url-filtering-profile-actions

NEW QUESTION 166
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

Answer: A

NEW QUESTION 171
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

Answer: C

Explanation:

Reference:https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface-help/objects/objects-security-profiles-vulnerability-protection.html

Vulnerability Protection Security Profiles protect against threats entering the network. For example, Vulnerability Protection Security Profiles protect against buffer overflows, illegal code execution, and other attempts to exploit system vulnerabilities. The default Vulnerability Protection Security Profile protects clients and servers from all known critical-, high-, and medium-severity threats. You also can create exceptions that enable you to change the response to a specific signature.

NEW QUESTION 176
An administrator needs to add capability to perform real-time signature lookups to block or sinkhole all known malware domains.
Which type of single unified engine will get this result?

A. User-ID
B. App-ID
C. Security Processing Engine
D. Content-ID

Answer: A

NEW QUESTION 178
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

Answer: A

Explanation:

Reference:https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g00000 0ClVHCA0

NEW QUESTION 182
You receive notification about new malware that is being used to attack hosts The malware exploits a software bug in a common application
Which Security Profile detects and blocks access to this threat after you update the firewall's threat signature database?

A. Data Filtering Profile applied to outbound Security policy rules
B. Antivirus Profile applied to outbound Security policy rules
C. Data Filtering Profile applied to inbound Security policy rules
D. Vulnerability Profile applied to inbound Security policy rules

Answer: B

NEW QUESTION 187
How many zones can an interface be assigned with a Palo Alto Networks firewall?

A. two
B. three

C. four
D. one

Answer: D

NEW QUESTION 188
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

Answer: BC

Explanation:

Reference:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/security-profiles

NEW QUESTION 191
Which firewall feature do you need to configure to query Palo Alto Networks service updates over a data-plane interface instead of the management interface?

A. Data redistribution
B. Dynamic updates
C. SNMP setup
D. Service route

Answer: D

NEW QUESTION 193
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.

Answer: D

Explanation:

Reference:https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/manage-licenses-and-updates/deploy-updates-to-firewalls-log-collectors-and-wildfire-appliances-using-panorama/schedule-a-content-update-using-panorama.html

NEW QUESTION 198
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

Answer: B

NEW QUESTION 200
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

Answer: AB

NEW QUESTION 203
Access to which feature requires PAN-OS Filtering licens?

A. PAN-DB database
B. URL external dynamic lists
C. Custom URL categories
D. DNS Security

Answer: A

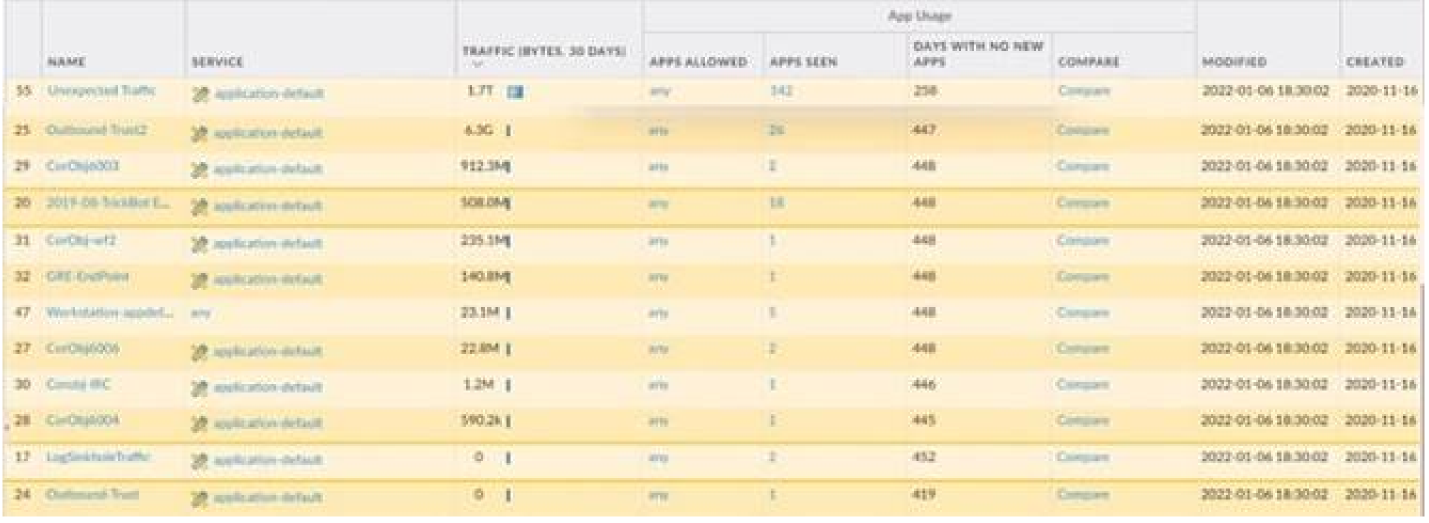
Explanation:
Reference:https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/getting-started/activate-licenses-and-subscriptions.html

NEW QUESTION 204
Which prevention technique will prevent attacks based on packet count?

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

Answer: A

NEW QUESTION 207
An administrator is updating Security policy to align with best practices. Which Policy Optimizer feature is shown in the screenshot below?



				App Usage					
	NAME	SERVICE	TRAFFIC (BYTES, 30 DAYS)	APPS ALLOWED	APPS SEEN	DAYS WITH NO NEW APPS	COMPARE	MODIFIED	CREATED
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	1	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

Answer: C

NEW QUESTION 208
......