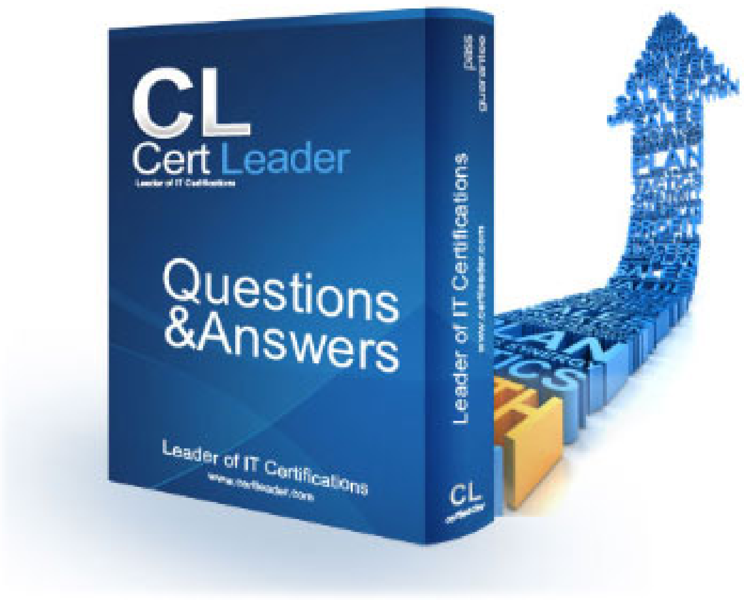
PCNSA Dumps

Palo Alto Networks Certified Network Security Administrator

https://www.certleader.com/PCNSA-dumps.html



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
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

Answer: C

Explanation:

NEW QUESTION 3
Which object would an administrator create to enable access to all applications in the office-programs subcategory?

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

Answer: A

NEW QUESTION 4
Which Security policy action will message a user's browser thai their web session has been terminated?

A. Mastered
B. Not Mastered

Answer: A

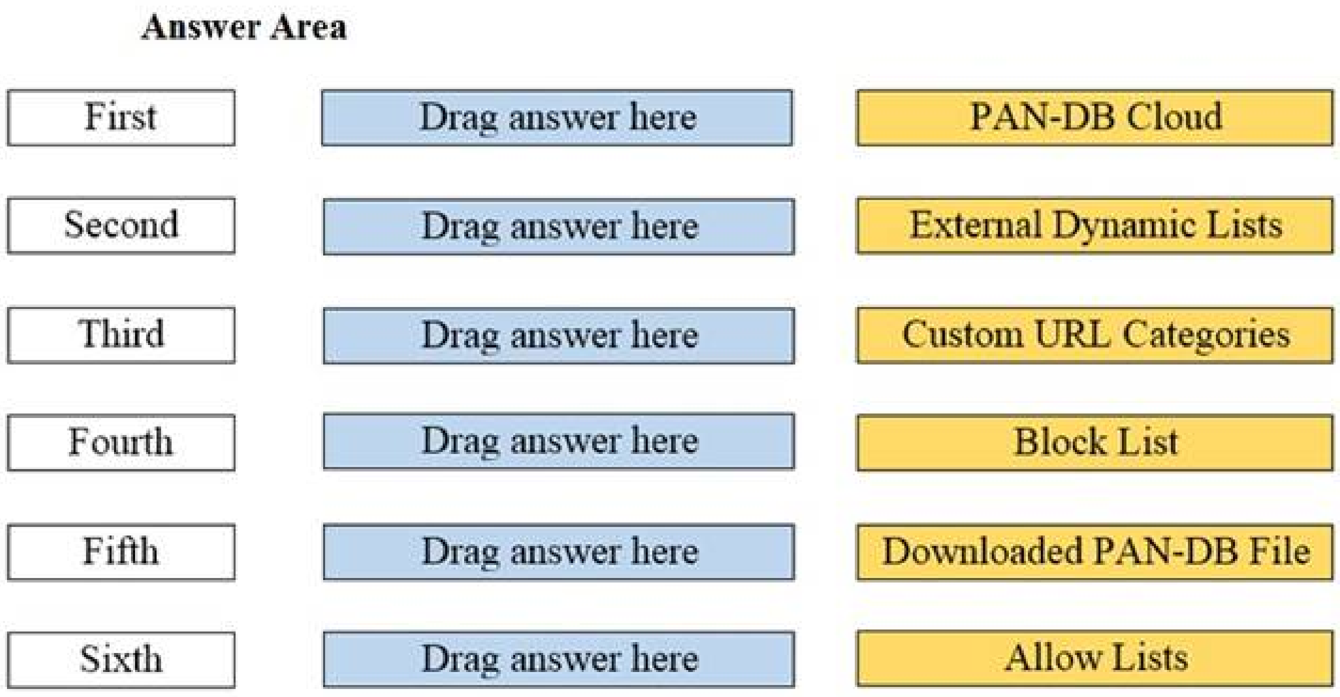
NEW QUESTION 5
Actions can be set for which two items in a URL filtering security profile? (Choose two.)

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

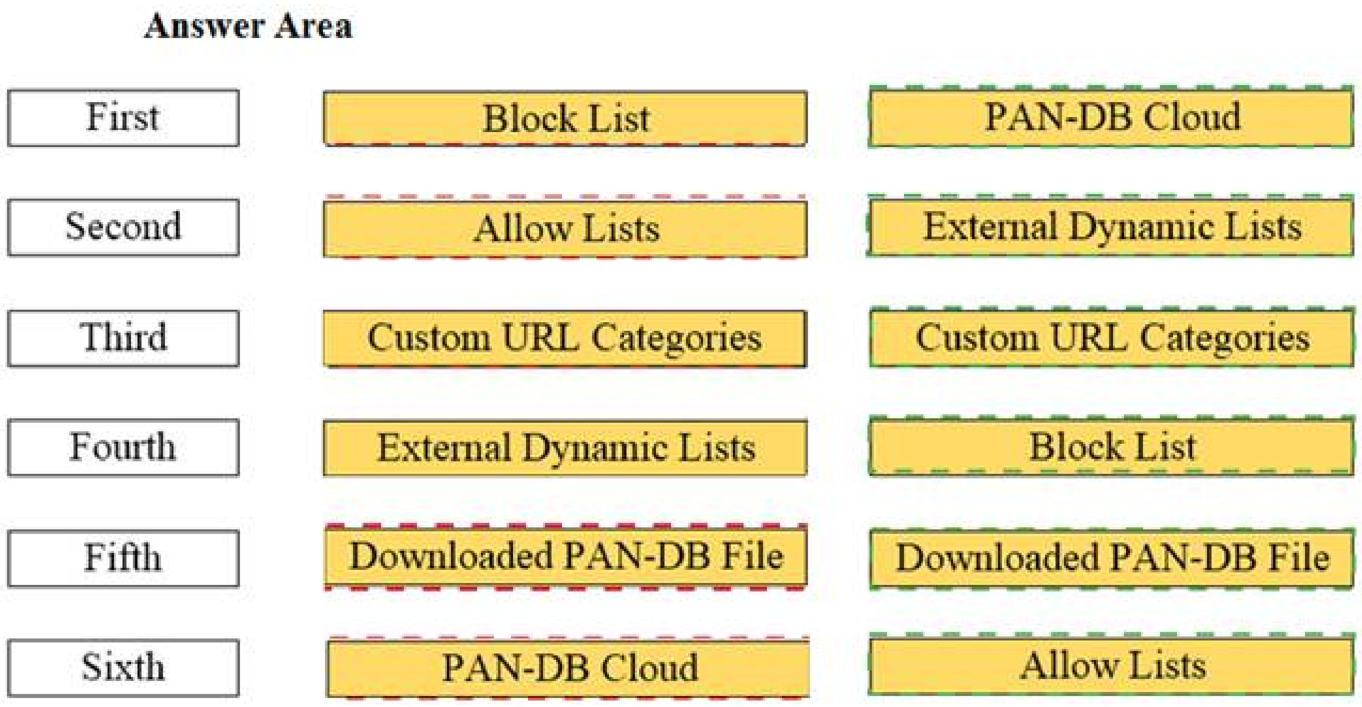
NEW QUESTION 6
DRAG DROP
Arrange the correct order that the URL classifications are processed within the system.



Answer Area

First	Drag answer here	PAN-DB Cloud
Second	Drag answer here	External Dynamic Lists
Third	Drag answer here	Custom URL Categories
Fourth	Drag answer here	Block List
Fifth	Drag answer here	Downloaded PAN-DB File
Sixth	Drag answer here	Allow Lists

Answer:



Answer Area

First	Block List	PAN-DB Cloud
Second	Allow Lists	External Dynamic Lists
Third	Custom URL Categories	Custom URL Categories
Fourth	External Dynamic Lists	Block List
Fifth	Downloaded PAN-DB File	Downloaded PAN-DB File
Sixth	PAN-DB Cloud	Allow Lists

A. Mastered
B. Not Mastered

Answer: A

Explanation:

First – Block List Second – Allow List
Third – Custom URL Categories Fourth – External Dynamic Lists
Fifth – Downloaded PAN-DB Files Sixth - PAN-DB Cloud

NEW QUESTION 7
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 8
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 9
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 10
Which object would an administrator create to enable access to all applications in the office-programs subcategory?

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

Answer: C

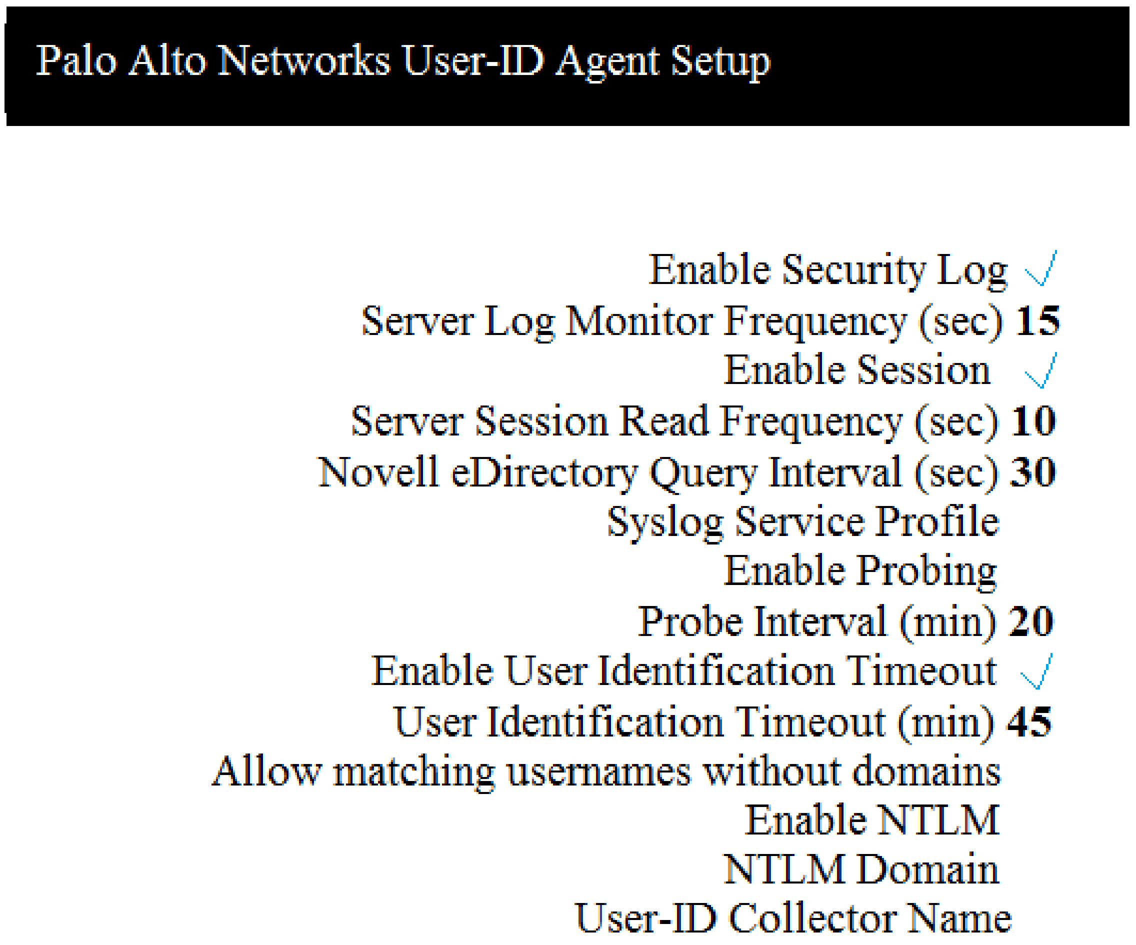
NEW QUESTION 10
What is considered best practice with regards to committing configuration changes?

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

Answer: A

NEW QUESTION 12

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



Palo Alto Networks User-ID Agent Setup

Enable Security Log ✓
Server Log Monitor Frequency (sec) **15**
Enable Session ✓
Server Session Read Frequency (sec) **10**
Novell eDirectory Query Interval (sec) **30**
Syslog Service Profile
Enable Probing
Probe Interval (min) **20**
Enable User Identification Timeout ✓
User Identification Timeout (min) **45**
Allow matching usernames without domains
Enable NTLM
NTLM Domain
User-ID Collector Name

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

Answer: BC

NEW QUESTION 15
What are two differences between an implicit dependency and an explicit dependency in App-ID? (Choose two.)

A. An implicit dependency does not require the dependent application to be added in the security policy
B. An implicit dependency requires the dependent application to be added in the security policy
C. An explicit dependency does not require the dependent application to be added in the security policy
D. An explicit dependency requires the dependent application to be added in the security policy

Answer: AD

NEW QUESTION 18
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 21
An administrator would like to block access to a web server, while also preserving

resources and minimizing half-open sockets. What are two security policy actions the administrator can select? (Choose two.)

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

Answer: AC

NEW QUESTION 24
You receive notification about a new malware that infects hosts An infection results in the infected host attempting to contact a command-and-control server Which Security Profile when applied to outbound Security policy rules detects and prevents this threat from establishing a command-and-control connection?

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

Answer: D

Explanation:
Anti-Spyware Security Profiles block spyware on compromised hosts from trying to communicate with external command-and-control (C2) servers, thus enabling you to detect malicious traffic leaving the network from infected clients.

NEW QUESTION 26
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 31
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 34
What are three factors that can be used in domain generation algorithms? (Choose three.)

A. cryptographic keys
B.

time of day
C. other unique values
D. URL custom categories
E. IP address

Answer: ABC

Explanation:
Domain generation algorithms (DGAs) are used to auto-generate domains, typically in large numbers within the context of establishing a malicious command-and-control (C2) communications channel. DGA-based malware (such as Pushdo, BankPatch, and CryptoLocker) limit the number of domains from being blocked by hiding the location of their active C2 servers within a large number of possible suspects, and can be algorithmically generated based on factors such as time of day, cryptographic keys, or other unique values.
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/threat-prevention/dns-security/domain-generation-algorithm-detection

NEW QUESTION 38
What is an advantage for using application tags?

A. They are helpful during the creation of new zones
B. They help with the design of IP address allocations in DHCP.
C. They help content updates automate policy updates
D. They help with the creation of interfaces

Answer: C

NEW QUESTION 40
Four configuration choices are listed, and each could be used to block access to a specific URL. If you configured each choices to block the sameURL then which choice would be the last to block access to the URL?

A. Mastered
B. Not Mastered

Answer: A

Explanation:
The precedence is from the top down; First Match Wins: 1) Block list: Manually entered blocked URLs Objects - 2) Allow list: Manually entered allowed URLs Objects - 3) Custom URL Categories - 4) Cached Cached: URLs learned from External Dynamic Lists (EDLs) -
5) Pre-Defined Categories: PAN-DB or Brightcloud categories.

NEW QUESTION 42
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 45
Which two App-ID applications will need to be allowed to use Facebook-chat? (Choose two.)

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

Answer: BC

NEW QUESTION 46
How are Application Fillers or Application Groups used in firewall policy?

A. An Application Filter is a static way of grouping applications and can be configured as a nested member of an Application Group
B. An Application Filter is a dynamic way to group applications and can be configured as a nested member of an Application Group
C. An Application Group is a dynamic way of grouping applications and can be configured as a nested member of an Application Group
D. An Application Group is a static way of grouping applications and cannot be configured as a nested member of Application Group

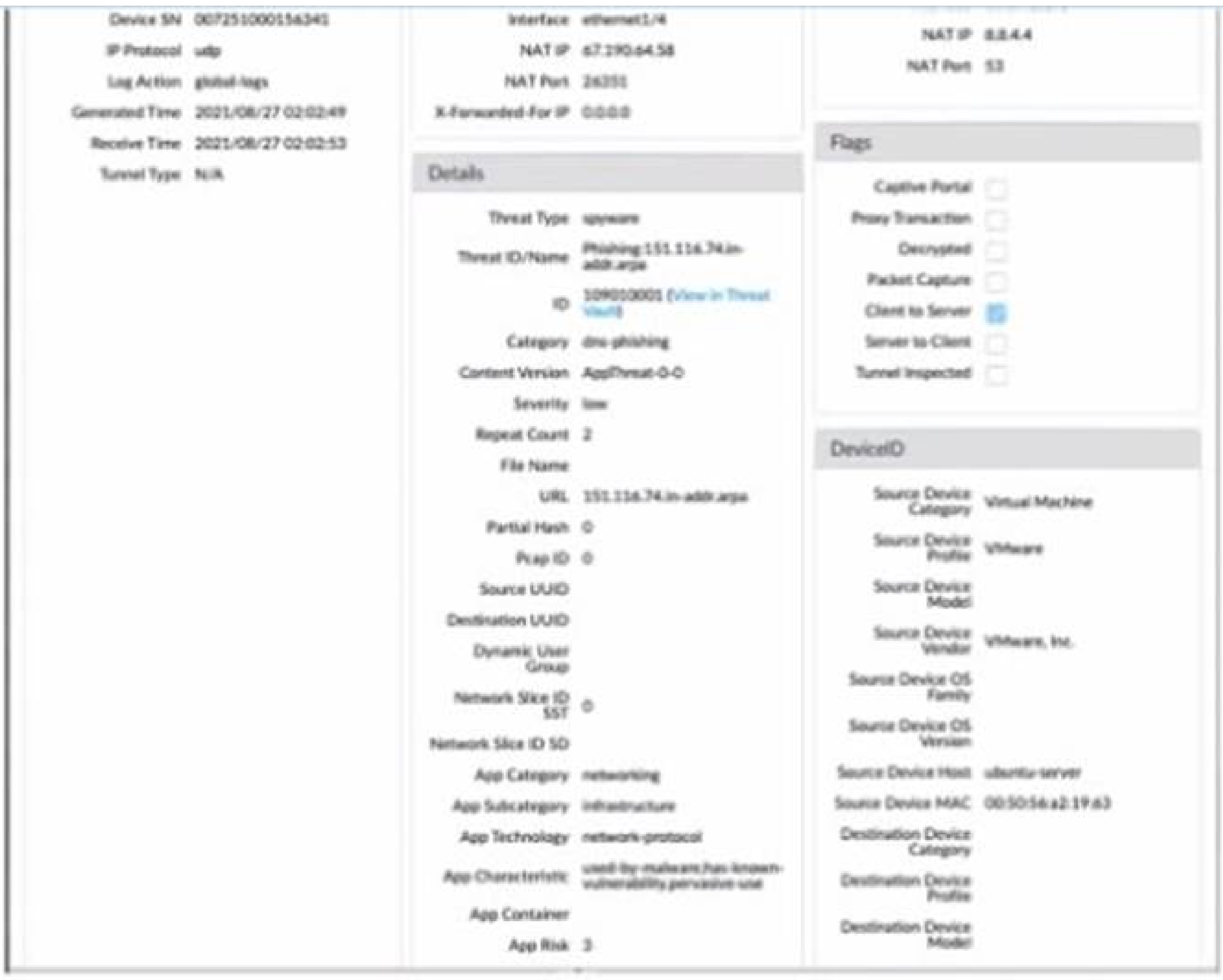
Answer: B

NEW QUESTION 51
Which data flow direction is protected in a zero trust firewall deployment that is not protected in a perimeter-only firewall deployment?

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

Answer: D

NEW QUESTION 52
Given the detailed log information above, what was the result of the firewall traffic inspection?



Device SN 007251000156341
IP Protocol udp
Log Action global-logs
Generated Time 2021/08/27 02:02:49
Receive Time 2021/08/27 02:02:53
Tunnel Type N/A

Interface ethernet1/4
NAT IP 67.190.64.58
NAT Port 26351
X-Forwarded-For IP 0.0.0.0

Details

Threat Type spyware
Threat ID/Name Phishing:151.116.74.in-addr.arpa
ID 109010001 (View in Threat Vault)
Category dns-phishing
Content Version AppThreat-0-0
Severity low
Repeat Count 2
File Name
URL 151.116.74.in-addr.arpa
Partial Hash 0
Pcap ID 0
Source UUID
Destination UUID
Dynamic User Group
Network Slice ID SST 0
Network Slice ID SD
App Category networking
App Subcategory infrastructure
App Technology network-protocol
App Characteristic used-by-malware,has-known-vulnerability,pervasive-use
App Container
App Risk 3

NAT IP 8.8.4.4
NAT Port 53

Flags

Captive Portal □
Proxy Transaction □
Decrypted □
Packet Capture □
Client to Server ☑
Server to Client □
Tunnel Inspected □

DeviceID

Source Device Category Virtual Machine
Source Device Profile VMware
Source Device Model
Source Device Vendor VMware, Inc.
Source Device OS Family
Source Device OS Version
Source Device Host ubuntu-server
Source Device MAC 00:50:56:a2:19:63
Destination Device Category
Destination Device Profile
Destination Device Model

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

Answer: C

NEW QUESTION 53
Which action would an administrator take to ensure that a service object will be available only to the selected device group?

A. create the service object in the specific template
B. uncheck the shared option
C. ensure that disable override is selected
D. ensure that disable override is cleared

Answer: D

Explanation:
https://docs.paloaltonetworks.com/panorama/9-0/panorama-admin/manage- firewalls/manage-device-groups/create-objects-for-use-in-shared-or-device-group-policy

NEW QUESTION 56
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 57
Which feature would be useful for preventing traffic from hosting providers that place few restrictions on content, whose services are frequently used by attackers to distribute illegal or unethical material?

A. Palo Alto Networks Bulletproof IP Addresses
B. Palo Alto Networks C&C IP Addresses
C. Palo Alto Networks Known Malicious IP Addresses
D. Palo Alto Networks High-Risk IP Addresses

Answer: A

Explanation:

To block hosts that use bulletproof hosts to provide malicious, illegal, and/or unethical content, use the bulletproof IP address list in policy.
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-new-features/content-inspection-features/edl-for-bulletproof-isps#:~:text=A%20new%20built%2Din%20external,%2C%20illegal%2C%20and%20unethi cal%20content.

NEW QUESTION 62
Which option is part of the content inspection process?

A. IPsec tunnel encryption
B.

Packet egress process
C. SSL Proxy re-encrypt
D. Packet forwarding process

Answer: C

NEW QUESTION 64
Which two features can be used to tag a username so that it is included in a dynamic user group? (Choose two.)

A. GlobalProtect agent
B. XML API
C.

User-ID Windows-based agent
D. log forwarding auto-tagging

Answer: BC

NEW QUESTION 65
By default, which action is assigned to the interzone-default rule?

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

Answer: C

NEW QUESTION 70
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 72
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

Answer: BD

Explanation:

NEW QUESTION 74
Which stage of the cyber-attack lifecycle makes it important to provide ongoing education to users on spear phishing links, unknown emails, and risky websites?

A. reconnaissance
B. delivery
C. exploitation
D. installation

Answer: B

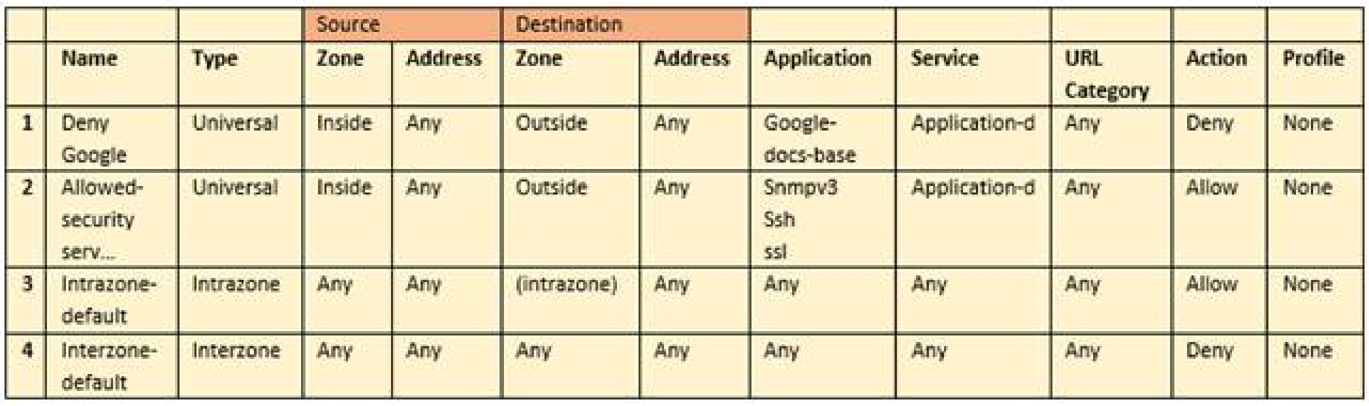
Explanation:
Weaponization and Delivery: Attackers will then determine which methods to use in order to deliver malicious payloads. Some of the methods they might utilize are automated tools, such as exploit kits, spear phishing attacks with malicious links, or attachments and malvertizing.
? Gain full visibility into all traffic, including SSL, and block high-risk applications.
Extend those protections to remote and mobile devices.
? Protect against perimeter breaches by blocking malicious or risky websites through URL filtering.
? Block known exploits, malware and inbound command-and-control communications using multiple threat prevention disciplines, including IPS, anti- malware, anti-CnC, DNS monitoring and sinkholing, and file and content blocking.
? Detect unknown malware and automatically deliver protections globally to thwart new attacks.
? Provide ongoing education to users on spear phishing links, unknown emails, risky websites, etc.
https://www.paloaltonetworks.com/cyberpedia/how-to-break-the-cyber-attack-lifecycle

NEW QUESTION 79
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 81
Based on the security policy rules shown, ssh will be allowed on which port?

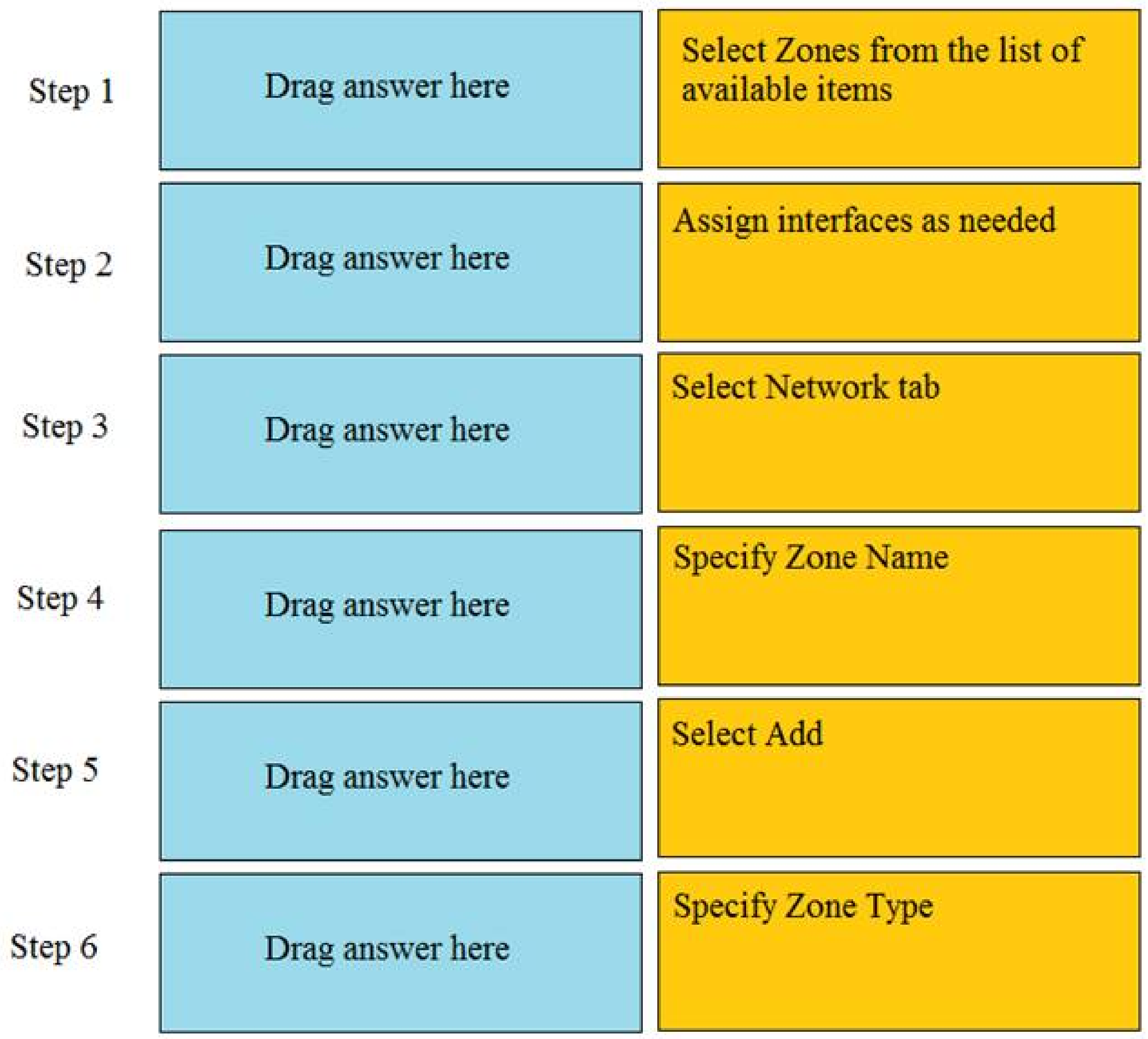


			Source		Destination						
	Name	Type	Zone	Address	Zone	Address	Application	Service	URL Category	Action	Profile
1	Deny Google	Universal	Inside	Any	Outside	Any	Google-docs-base	Application-d	Any	Deny	None
2	Allowed-security serv...	Universal	Inside	Any	Outside	Any	Snmpv3 Ssh ssl	Application-d	Any	Allow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

A. any port
B. same port as ssl and snmpv3
C. the default port
D. only ephemeral ports

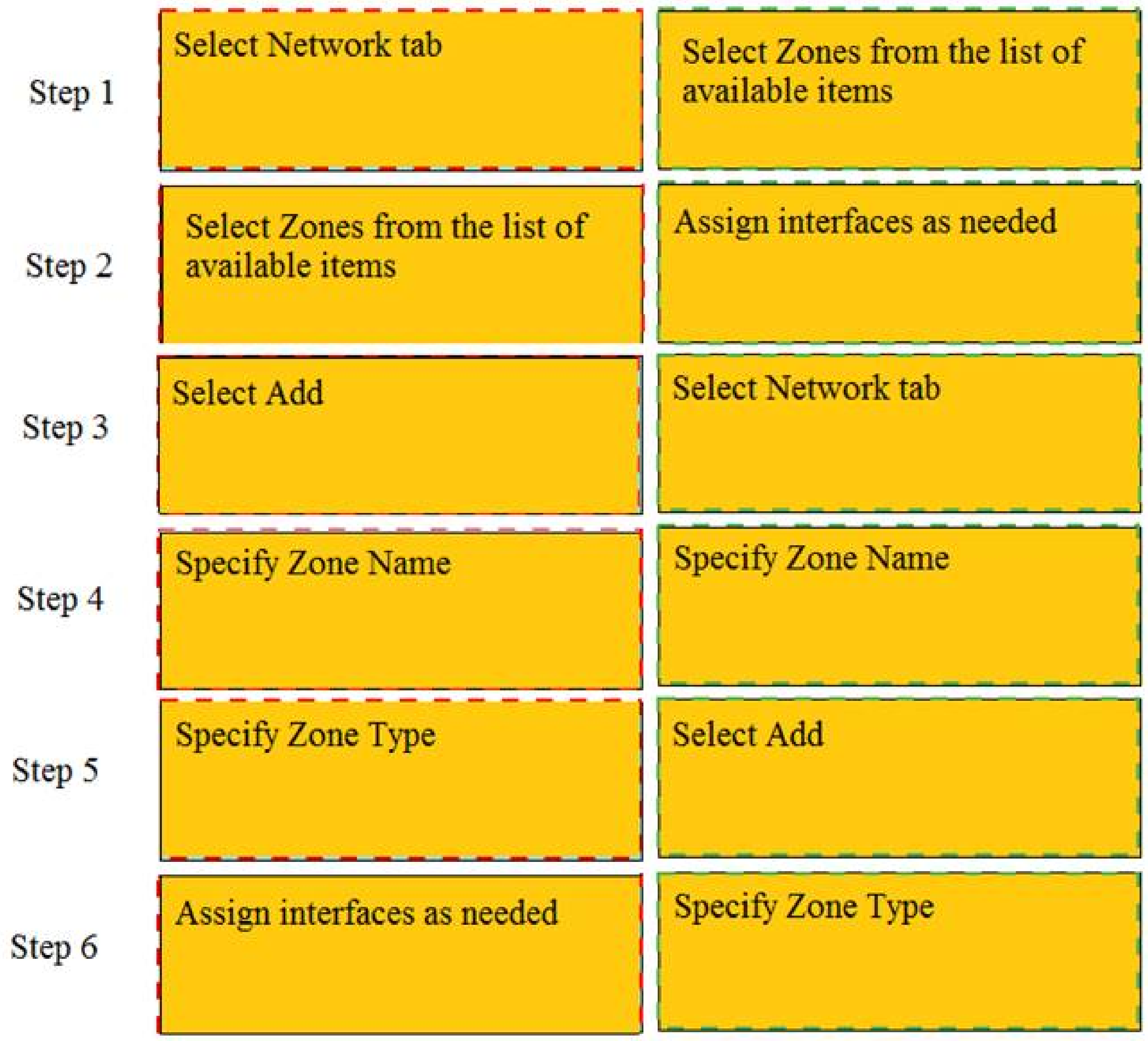
Answer: C

NEW QUESTION 86
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:



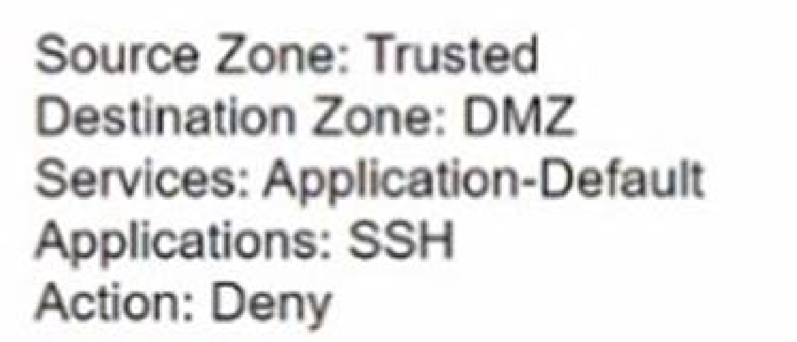
Step 1	Select Network tab	Select Zones from the list of available items
Step 2	Select Zones from the list of available items	Assign interfaces as needed
Step 3	Select Add	Select Network tab
Step 4	Specify Zone Name	Specify Zone Name
Step 5	Specify Zone Type	Select Add
Step 6	Assign interfaces as needed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

A. Mastered
B. Not Mastered

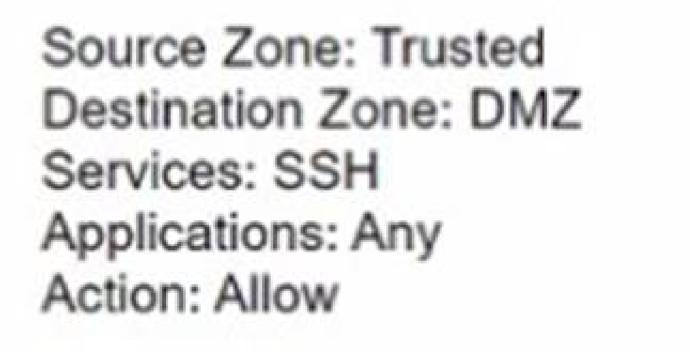
Answer: A

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

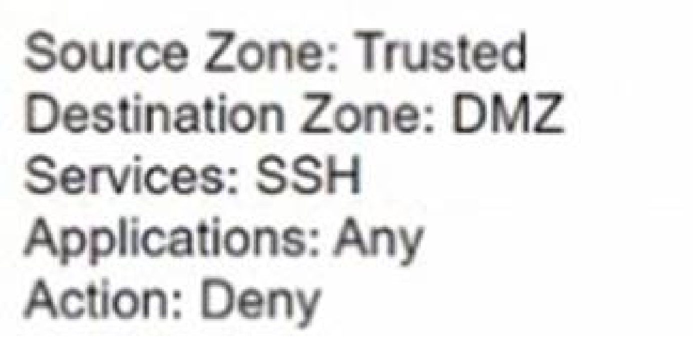
NEW QUESTION 89
If users from the Trusted zone need to allow traffic to an SFTP server in the DMZ zone, how should a Security policy with App-ID be configured?
A)


Source Zone: Trusted
Destination Zone: DMZ
Services: Application-Default
Applications: SSH
Action: Deny

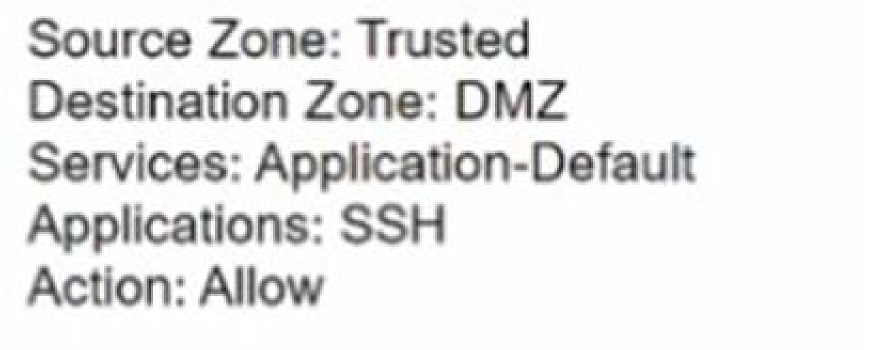
B)


Source Zone: Trusted
Destination Zone: DMZ
Services: SSH
Applications: Any
Action: Allow

C)


Source Zone: Trusted
Destination Zone: DMZ
Services: SSH
Applications: Any
Action: Deny

D)


Source Zone: Trusted
Destination Zone: DMZ
Services: Application-Default
Applications: SSH
Action: Allow

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

Answer: D

NEW QUESTION 91
Which option lists the attributes that are selectable when setting up an Application filters?

A. Category, Subcategory, Technology, and Characteristic
B. Category, Subcategory, Technology, Risk, and Characteristic
C. Name, Category, Technology, Risk, and Characteristic
D. Category, Subcategory, Risk, Standard Ports, and Technology

Answer: B

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

NEW QUESTION 94

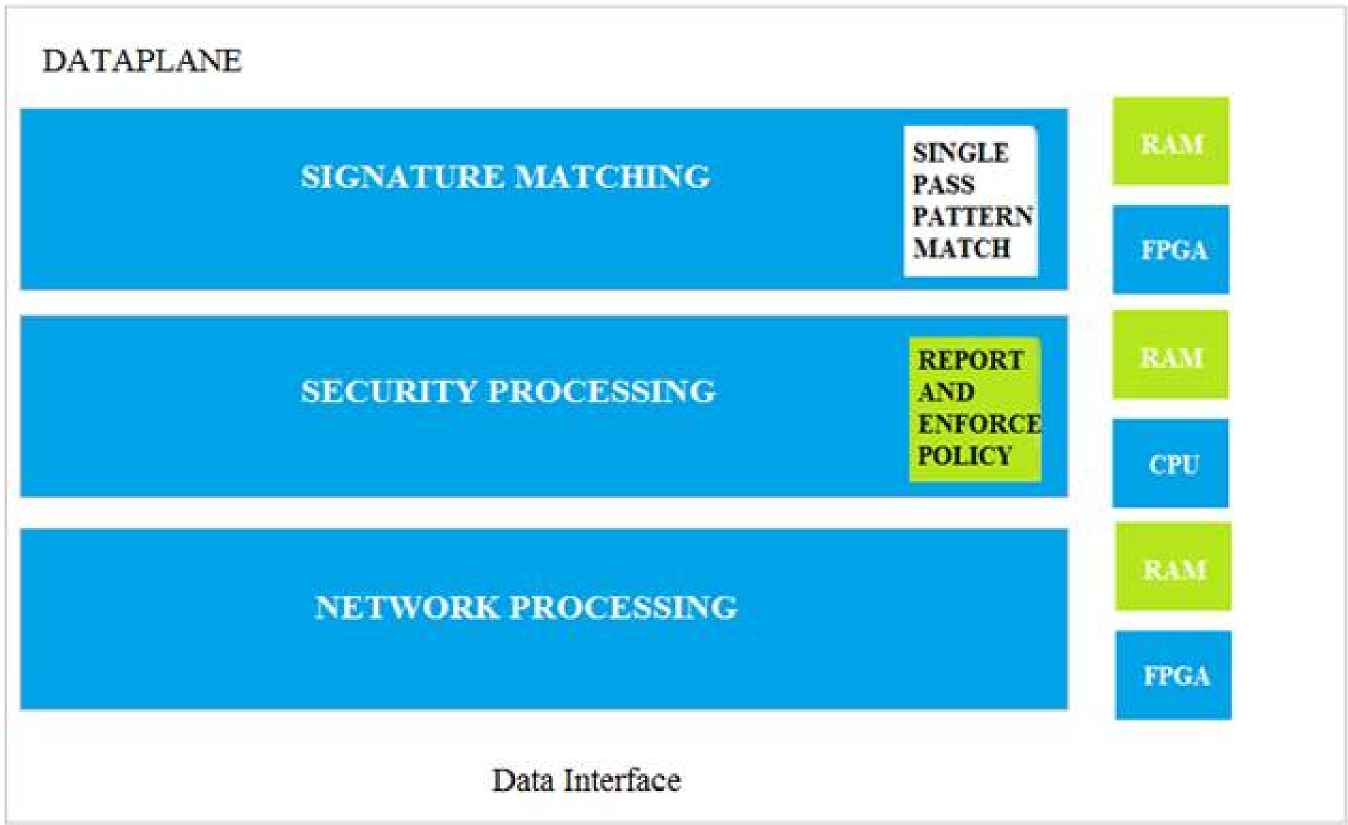
Which DNS Query action is recommended for traffic that is allowed by Security policy and matches Palo Alto Networks Content DNS Signatures?

A. block
B. sinkhole
C. alert
D. allow

Answer: B

Explanation:
To enable DNS sinkholing for domain queries using DNS security, you must activate your DNS Security subscription, create (or modify) an Anti-Spyware policy to reference the DNS Security service, configure the log severity and policy settings for each DNS signature category, and then attach the profile to a security policy rule. https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/threat-prevention/dns- security/enable-dns-security

NEW QUESTION 97
Which data-plane processor layer of the graphic shown provides uniform matching for spyware and vulnerability exploits on a Palo Alto Networks Firewall?



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

Answer: A

NEW QUESTION 98
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+

Answer: ABD

NEW QUESTION 103
You must configure which firewall feature to enable a data-plane interface to submit DNS queries on behalf of the control plane?

A. Admin Role profile
B. virtual router
C. DNS proxy
D. service route

Answer: A

NEW QUESTION 108
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 Protection profile applied to outbound Security policy rules.

Answer: C

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

NEW QUESTION 113
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 118
Which interface does not require a MAC or IP address?

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

Answer: A

NEW QUESTION 122
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 125
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

Answer: B

NEW QUESTION 129
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

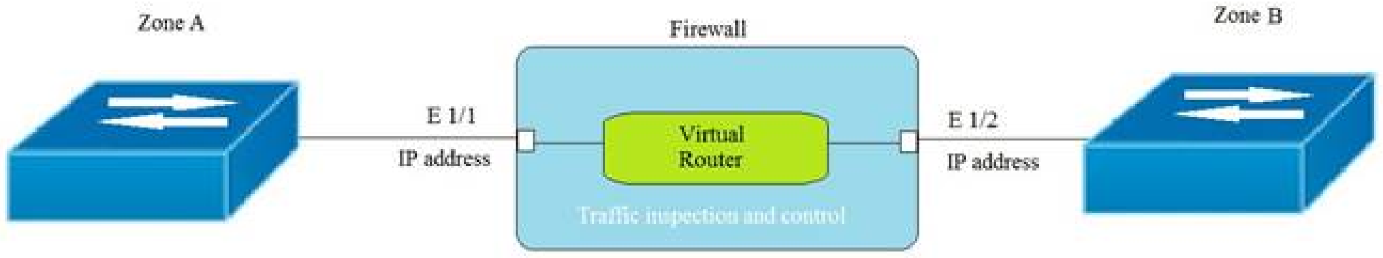
Answer: C

NEW QUESTION 131
An administrator has configured a Security policy where the matching condition includes a single application and the action is deny
If the application s default deny action is reset-both what action does the firewall take*?

A. It sends a TCP reset to the client-side and server-side devices
B. It silently drops the traffic and sends an ICMP unreachable code
C. It silently drops the traffic
D. It sends a TCP reset to the server-side device

Answer: A

NEW QUESTION 135
Given the topology, which zone type should zone A and zone B to be configured with?



A. Layer3
B. Tap
C. Layer2

Virtual Wire

D.

Answer: A

NEW QUESTION 137
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

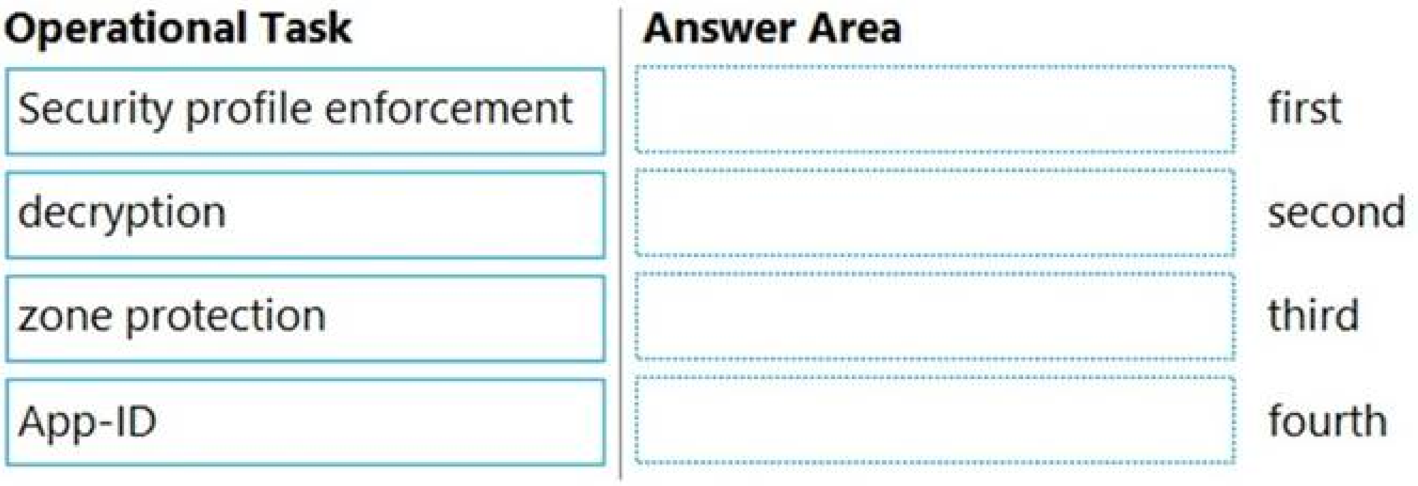
Answer: A

NEW QUESTION 141
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

Answer: A

NEW QUESTION 145
DRAG DROP
Place the steps in the correct packet-processing order of operations.



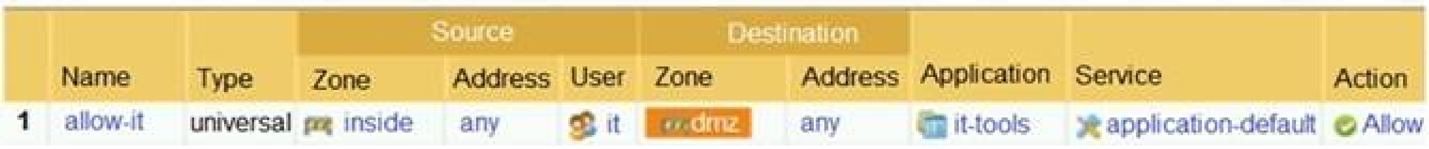
Operational Task	Answer Area	
Security profile enforcement		first
decryption		second
zone protection		third
App-ID		fourth

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 149
Based on the screenshot what is the purpose of the included groups?



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

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

Answer: B

Explanation:

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

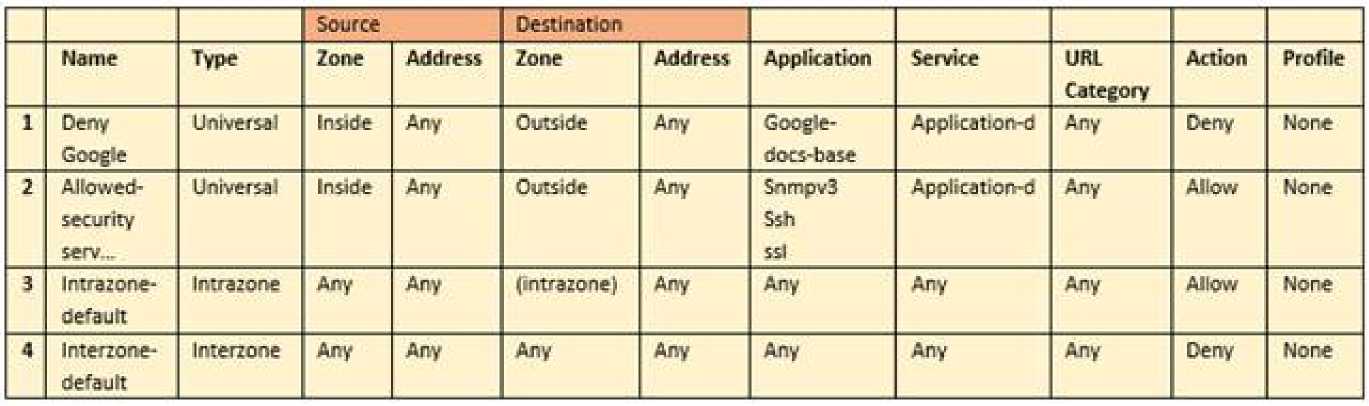
NEW QUESTION 153
During the packet flow process, which two processes are performed in application identification? (Choose two.)

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 158
Based on the security policy rules shown, ssh will be allowed on which port?



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

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

Answer: C

Explanation:

NEW QUESTION 161
The CFO found a USB drive in the parking lot and decide to plug it into their corporate laptop. The USB drive had malware on it that loaded onto their computer and then contacted a known command and control (CnC) server, which ordered the infected machine to begin Exfiltrating data from the laptop.
Which security profile feature could have been used to prevent the communication with the CnC server?

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

Answer: A

Explanation:

NEW QUESTION 162
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

Answer: A

NEW QUESTION 164
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 165
What is the correct process tor creating a custom URL category?

A. Objects > Security Profiles > URL Category > Add
B. Objects > Custom Objects > URL Filtering > Add
C. Objects > Security Profiles > URL Filtering > Add
D. Objects > Custom Objects > URL Category > Add

Answer: D

Explanation:

NEW QUESTION 169
What must be configured before setting up Credential Phishing Prevention?

A. Anti Phishing Block Page
B. Threat Prevention
C. Anti Phishing profiles
D. User-ID

Answer: B

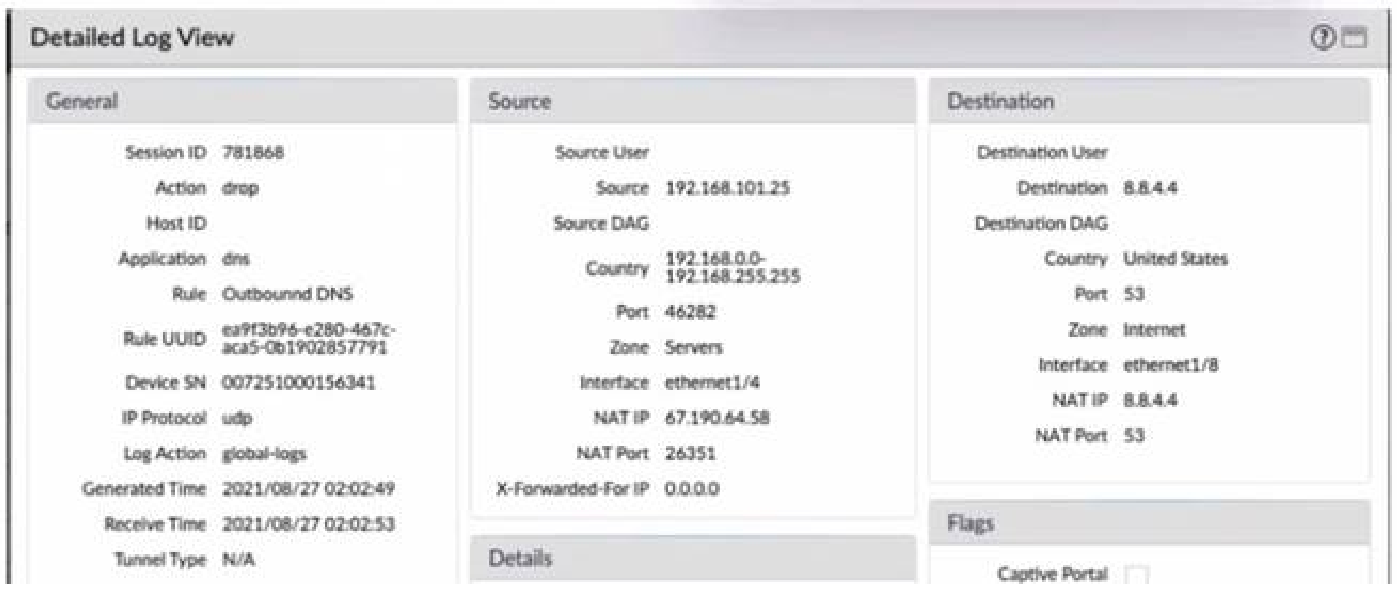
Explanation:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/threat- prevention/prevent-credential-phishing/set-up-credential-phishing-prevention

NEW QUESTION 170
Which interface type can use virtual routers and routing protocols?

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

Answer: B

NEW QUESTION 173
Given the detailed log information above, what was the result of the firewall traffic inspection?



Detailed Log View

General
Session ID 781868
Action drop
Host ID
Application dns
Rule Outbounnd DNS
Rule UUID ea9f3b96-e280-467c-aca5-0b1902857791
Device SN 007251000156341
IP Protocol udp
Log Action global-logs
Generated Time 2021/08/27 02:02:49
Receive Time 2021/08/27 02:02:53
Tunnel Type N/A

Source
Source User
Source 192.168.101.25
Source DAG
Country 192.168.0.0-192.168.255.255
Port 46282
Zone Servers
Interface ethernet1/4
NAT IP 67.190.64.58
NAT Port 26351
X-Forwarded-For IP 0.0.0.0

Details

Destination
Destination User
Destination 8.8.4.4
Destination DAG
Country United States
Port 53
Zone Internet
Interface ethernet1/8
NAT IP 8.8.4.4
NAT Port 53

Flags
Captive Portal □

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

Answer: B

NEW QUESTION 176
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 178
Which license must an Administrator acquire prior to downloading Antivirus Updates for use with the firewall?

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

Answer: A

NEW QUESTION 181
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?

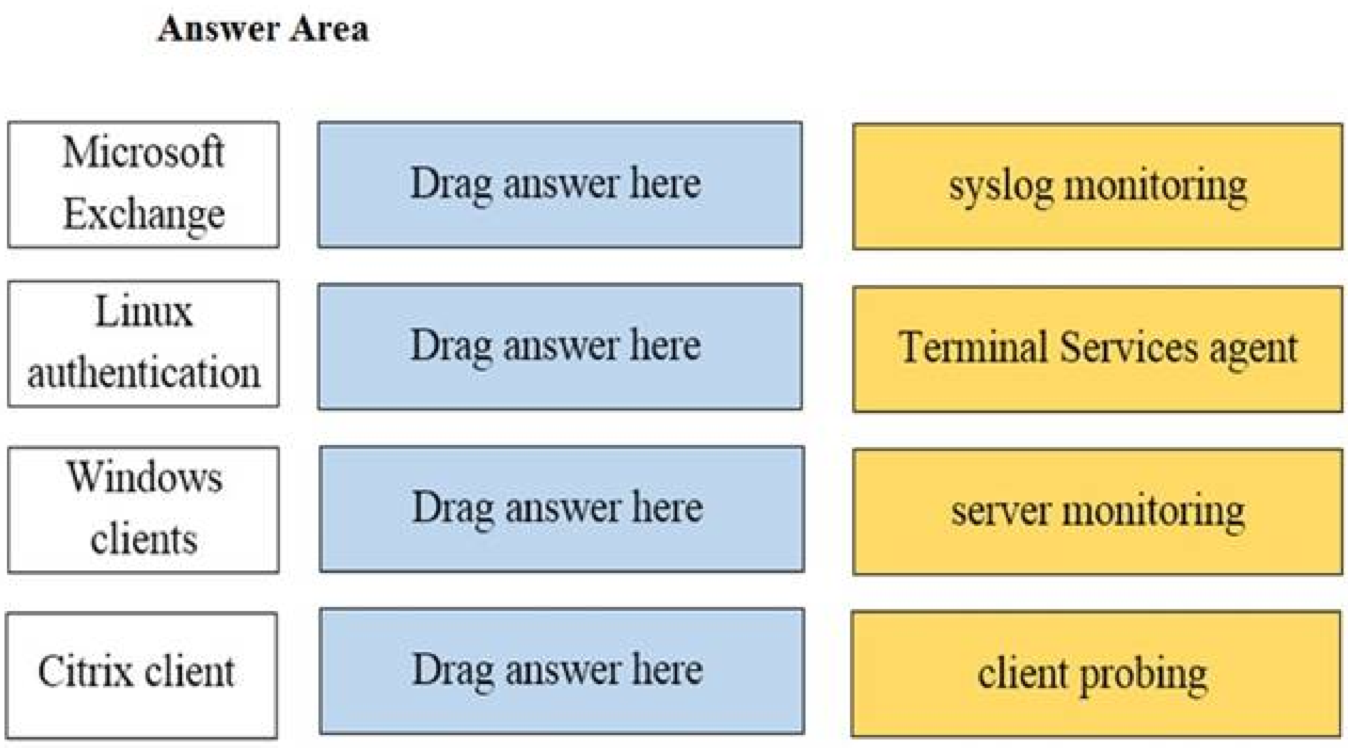
A. override
B. authorization
C. authentication
D. continue

Answer: B

Explanation:

Reference:
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/url-filtering/url-filtering- concepts/url- filteringprofile-actions.html

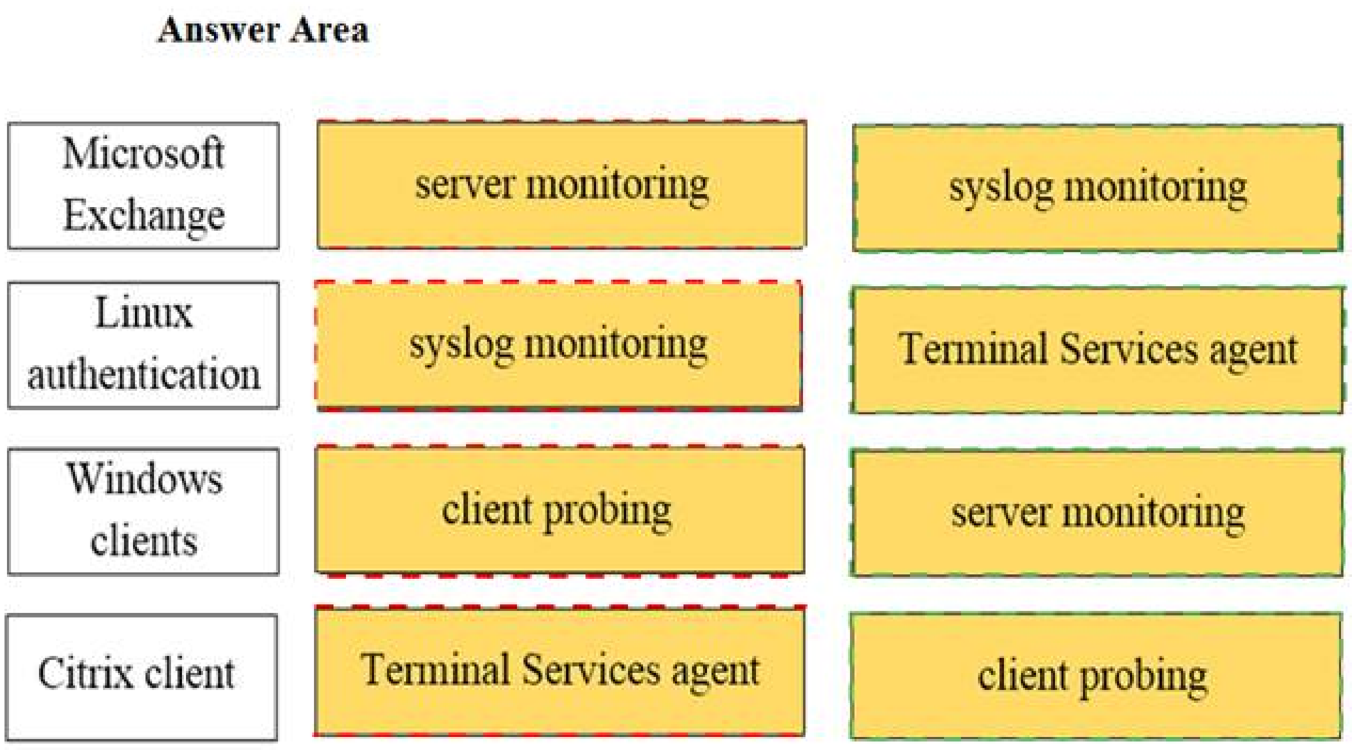
NEW QUESTION 186
DRAG DROP
Match the network device with the correct User-ID technology.



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 188
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 191
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 196
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

Answer: A

Explanation:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/app-id/security-policy-rule-optimization/migrate-port-based-to-app-id-based-security-policy-rules.html

NEW QUESTION 201
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”

Answer: D

NEW QUESTION 206
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.

Answer: B

NEW QUESTION 208
Complete the statement. A security profile can block or allow traffic

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

D. after it is matched by a security policy that allows or blocks traffic

Answer: B

Explanation:
Security profiles are objects added to policy rules that are configured with an action of allow.

NEW QUESTION 211
Which two security profile types can be attached to a security policy? (Choose two.)

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

Answer: AD

NEW QUESTION 215
Which two DNS policy actions in the anti-spyware security profile can prevent hacking attacks through DNS queries to malicious domains? (Choose two.)

A. Deny
B. Sinkhole
C. Override
D. Block

Answer: BD

Explanation:
? A DNS policy action is a setting in an Anti-Spyware security profile that defines
how the firewall handles DNS queries to malicious domains. A malicious domain is a domain name that is associated with a known threat, such as malware, phishing, or botnet1.
? There are four possible DNS policy actions: alert, allow, block, and sinkhole1.
? The alert action logs the DNS query and allows it to proceed to the intended destination. This action does not prevent hacking attacks, but only notifies the administrator of the potential threat1.
? The allow action allows the DNS query to proceed to the intended destination without logging it. This action does not prevent hacking attacks, but only bypasses the DNS security inspection2.
? The block action blocks the DNS query and sends a response to the client with an NXDOMAIN (non-existent domain) error code. This action prevents hacking attacks by preventing the client from resolving the malicious domain1.
? The sinkhole action redirects the DNS query to a predefined IP address (the sinkhole IP address) that is under the control of the administrator. This action prevents hacking attacks by isolating the client from the malicious domain and allowing the administrator to monitor and remediate the infected host1.
? The override action is not a valid DNS policy action, but a setting in an Anti- Spyware security profile that allows the administrator to create exceptions for specific spyware signatures that they want to override the default action or log settings3.
Therefore, the two DNS policy actions that can prevent hacking attacks through DNS queries to malicious domains are block and sinkhole.
References:
1: Enable DNS Security - Palo Alto Networks 2: How To Disable the DNS Security Feature from an Anti-Spyware Profile - Palo Alto Networks 3: Security Profile: Anti-Spyware - Palo Alto Networks

NEW QUESTION 216
Access to which feature requires the PAN-OS Filtering license?

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

Answer: A

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

NEW QUESTION 221
What is a recommended consideration when deploying content updates to the firewall from Panorama?

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

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 223
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

Answer: A

NEW QUESTION 225
Which protocol used to map username to user groups when user-ID is configured?

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

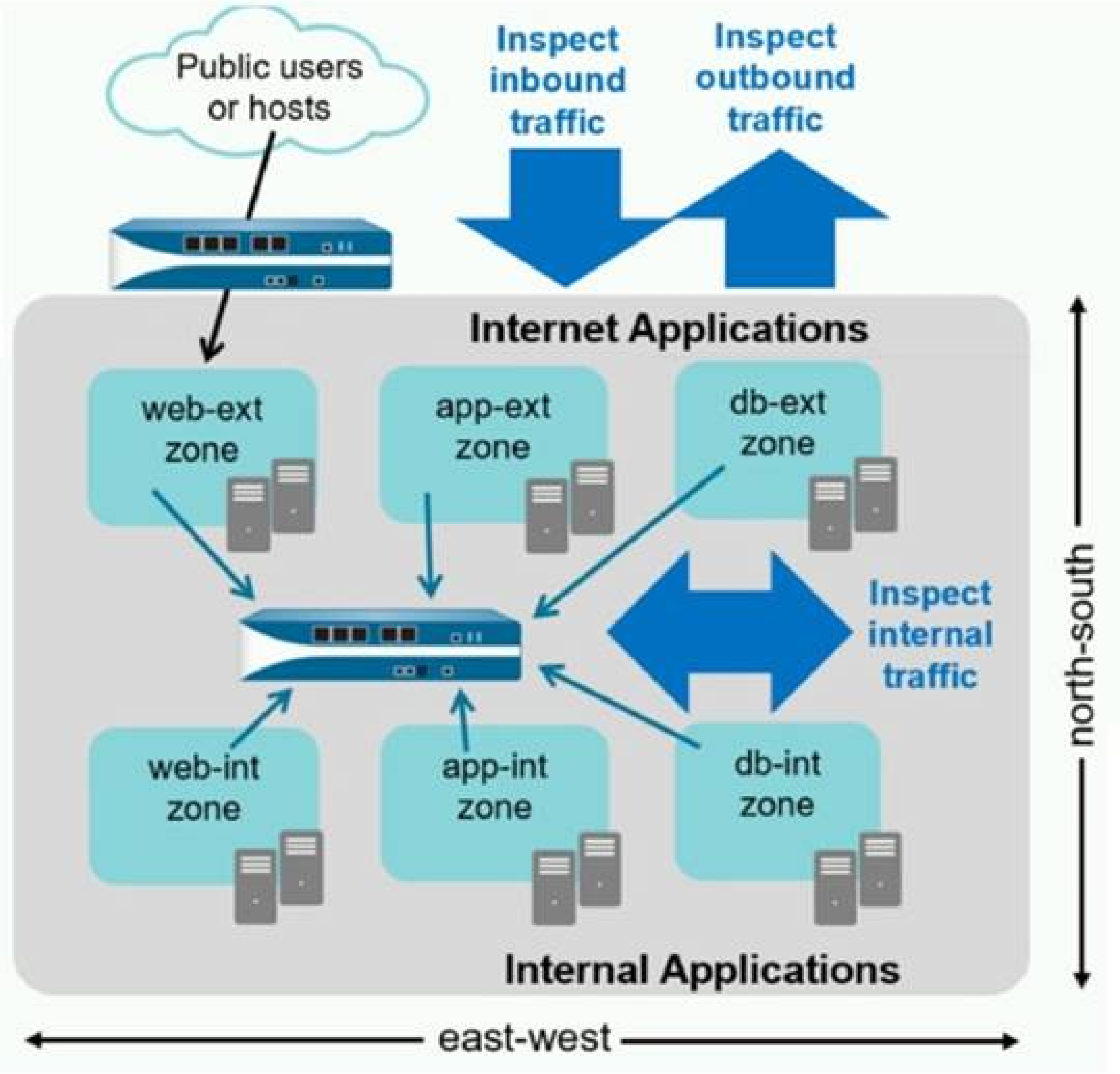
Answer: D

NEW QUESTION 228
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

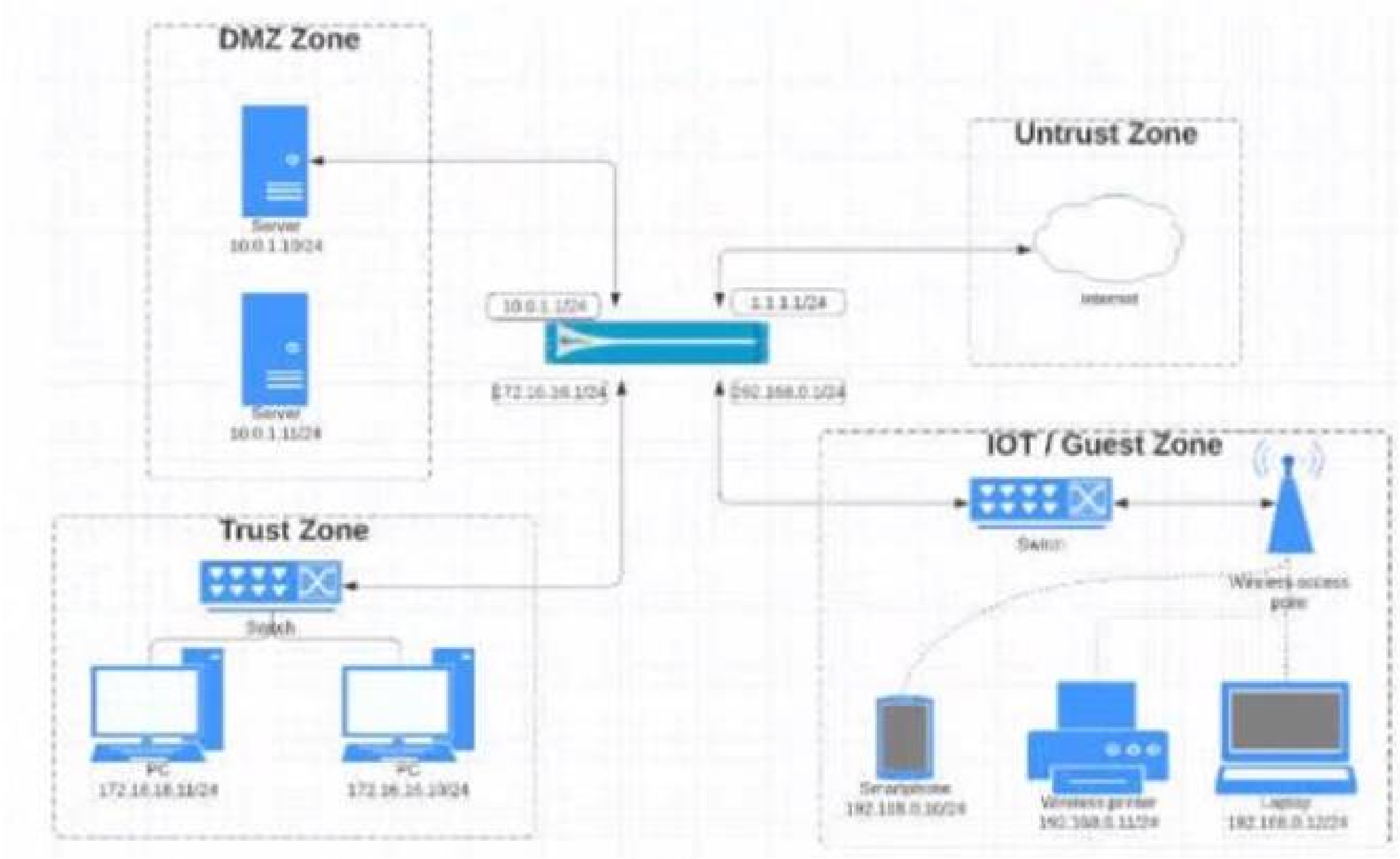
NEW QUESTION 230
An administrator notices that protection is needed for traffic within the network due to malicious lateral movement activity. Based on the image shown, which traffic would the administrator need to monitor and block to mitigate the malicious activity?



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

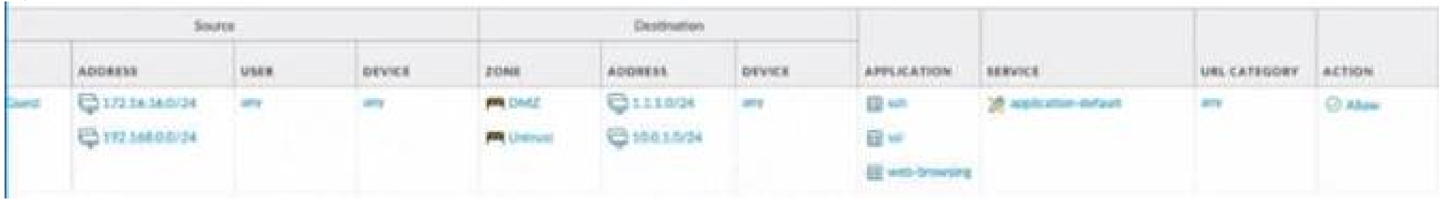
Answer: D

NEW QUESTION 233
View the diagram.



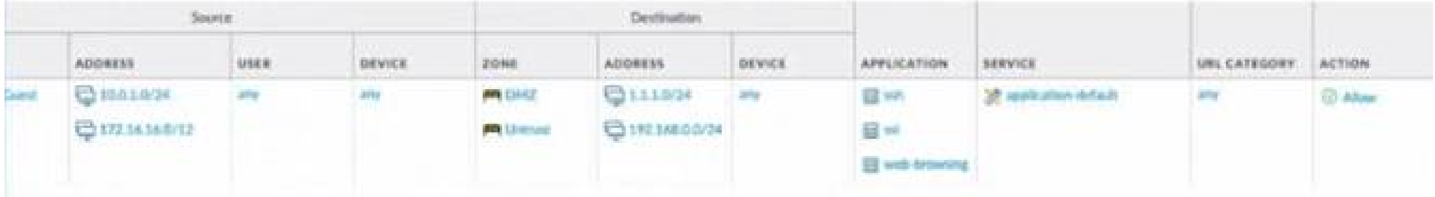
What is the most restrictive yet fully functional rule to allow general Internet and SSH traffic into both the DMZ and Untrust/Internet zones from each of the IOT/Guest and Trust Zones?

A)



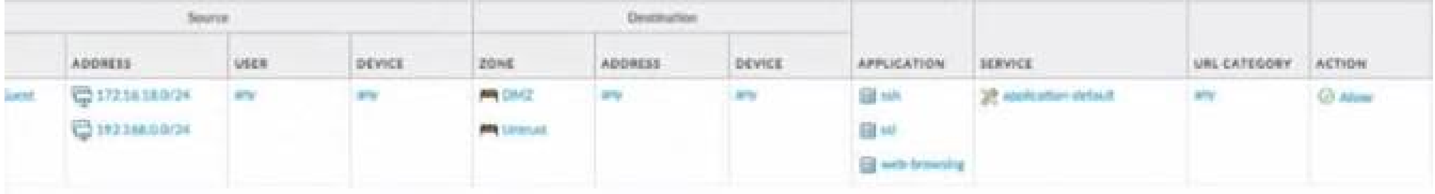
Source				Destination						
	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	URL CATEGORY	ACTION
Guest	172.16.16.0/24 192.168.0.0/24	any	any	DMZ Untrust	1.1.1.0/24 10.0.1.0/24	any	ssh ssl web-browsing	application-default	any	Allow

B)



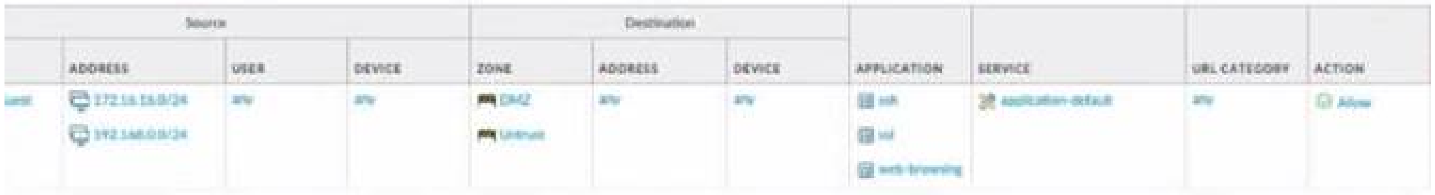
Source				Destination						
	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	URL CATEGORY	ACTION
Guest	10.0.1.0/24 172.16.16.0/12	any	any	DMZ Untrust	1.1.1.0/24 192.168.0.0/24	any	ssh ssl web-browsing	application-default	any	Allow

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
Option D
D.

Answer: C

NEW QUESTION 235
How are service routes used in PAN-OS?

A. By the OSPF protocol, as part of Dijkstra's algorithm, to give access to the various services offered in the network
B. To statically route subnets so they are joinable from, and have access to, the Palo Alto Networks external services
C. For routing, because they are the shortest path selected by the BGP routing protocol
D. To route management plane services through data interfaces rather than the management interface

Answer: D

Explanation:
? Service routes are a feature of PAN-OS that allows the administrator to customize the interface that the firewall uses to send requests to external services, such as DNS, email, Palo Alto Networks updates, User-ID agent, syslog, Panorama, dynamic updates, URL updates, licenses, and AutoFocus1.
? By default, the firewall uses the management interface for all service routes, unless the packet destination IP address matches the configured destination service route, in which case the source IP address is set to the source address configured for the destination1.
? However, in some scenarios, the administrator may want to use a different interface for service routes, such as when the management interface does not have public internet access, or when the administrator wants to isolate or monitor the traffic for certain services23.

? To configure service routes, the administrator can select Device > Setup > Services > Service Route Configuration and customize each service with a source interface and a source address. The administrator can also configure destination service routes to specify a destination IP address and a gateway for each service1.
? Service routes are not related to routing protocols such as OSPF or BGP, which are used to exchange routing information between routers and determine the best path to reach a network destination. Service routes are only used to change the interface that the firewall uses to communicate with external services. Therefore, service routes are used to route management plane services through data interfaces rather than the management interface.
References:
1: Configure Service Routes - Palo Alto Networks 2: Setting a Service Route for Services to Use a Dataplane’s Interface - Palo Alto Networks 3: How to Perform Updates when Management Interface does not have Public Internet Access - Palo Alto Networks

NEW QUESTION 240
What are three differences between security policies and security profiles? (Choose three.)

A. Security policies are attached to security profiles
B. Security profiles are attached to security policies
C. Security profiles should only be used on allowed traffic
D. Security profiles are used to block traffic by themselves
E. Security policies can block or allow traffic

Answer: BCE

NEW QUESTION 243
An administrator would like to silently drop traffic from the internet to a ftp server. Which Security policy action should the administrator select?

A. Reset-server
B. Block
C. Deny
D. Drop

Answer: D

NEW QUESTION 247
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 251
Which firewall plane provides configuration, logging, and reporting functions on a separate processor?

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

Answer: A

NEW QUESTION 254
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

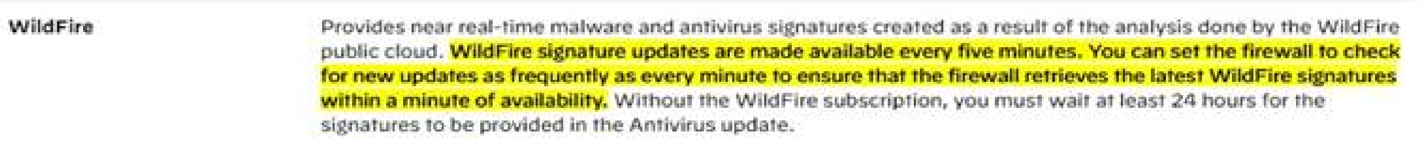
Explanation:
An administrator can configure URL Filtering profiles in the Objects section of the PAN-OS GUI. A URL Filtering profile is a collection of URL filtering controls that you can apply to individual Security policy rules that allow access to the internet1. You can set site access for URL categories, 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 257
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

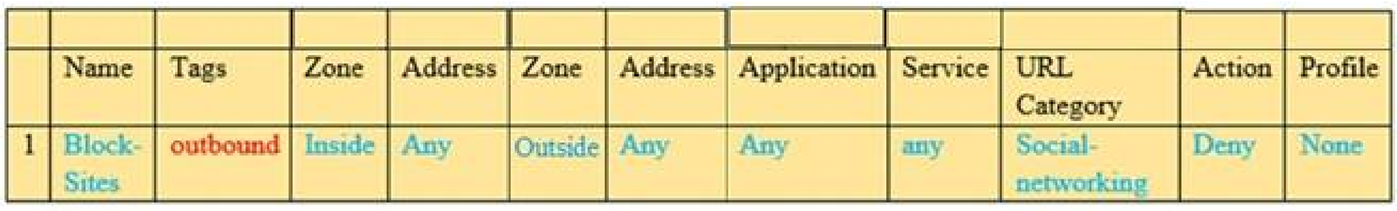
Explanation:



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 259

In the example security policy shown, which two websites fcked? (Choose two.)



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

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

Answer: AB

NEW QUESTION 263

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

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

Answer: D

Explanation:

NEW QUESTION 268

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 271

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

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

Answer: B

Explanation:

NEW QUESTION 274
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

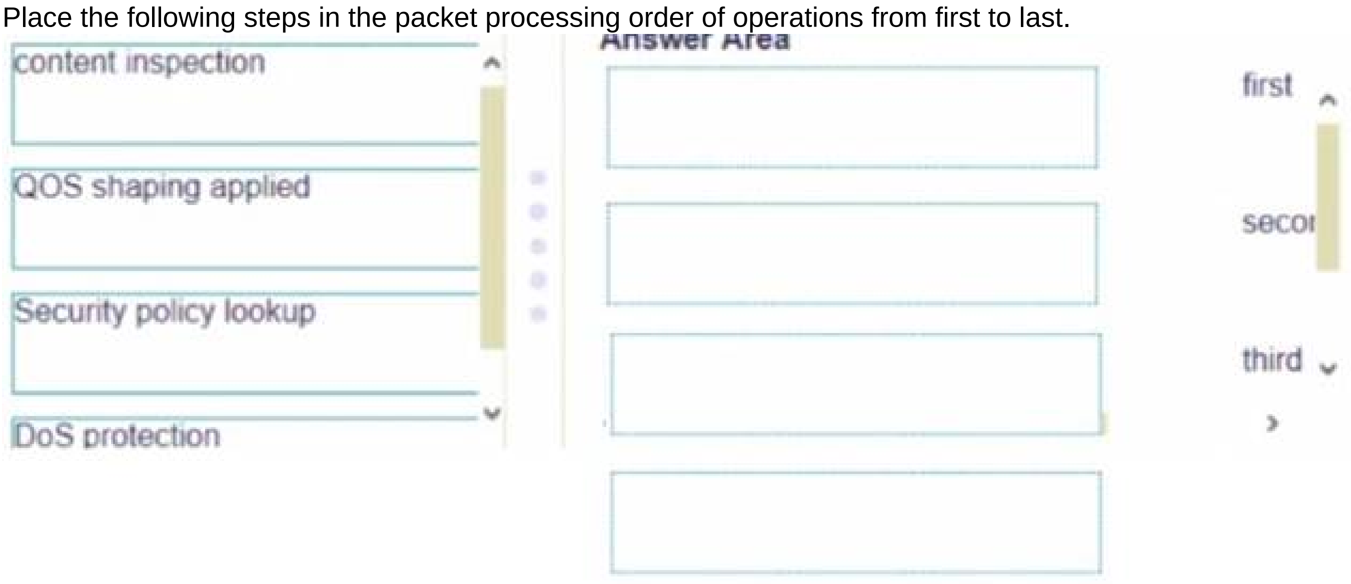
Answer: A

NEW QUESTION 278
What is a function of application tags?

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

Answer: C

NEW QUESTION 280
DRAG DROP
Place the following steps in the packet processing order of operations from first to last.



A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 282
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

Answer: BD

NEW QUESTION 284
Which action can be set in a URL Filtering Security profile to provide users temporary access to all websites in a given category using a provided password?

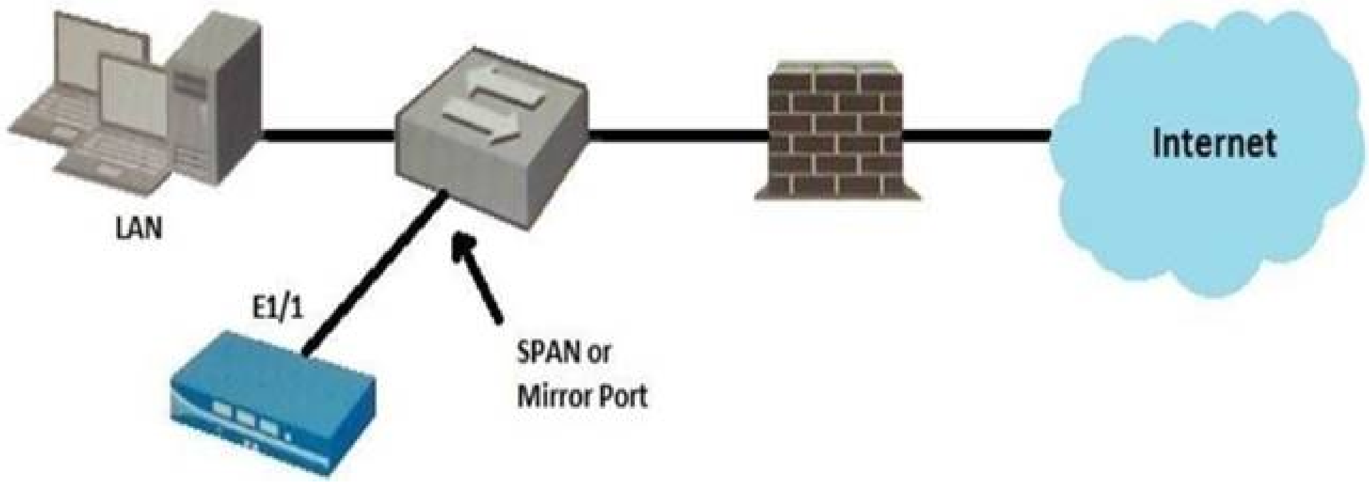
A. Mastered
B. Not Mastered

Answer: A

Explanation:
The user will see a response page indicating that a password is required to allow access to websites in the given category. With this option, the security administrator or help-desk person would provide a password granting temporary access to all websites in the given category. A log entry is generated in the URL

Filtering log. The Override webpage doesn’t display properly on client systems configured to use a proxy server.

NEW QUESTION 285
Given the topology, which zone type should you configure for firewall interface E1/1?



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

Answer: A

NEW QUESTION 289
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 lis
D. A column will open with the IP addresse
E. Select the entry to exclude.
F. Add the specific IP address from the address range to the Manual Exceptions list by using regular expressions to define the entry.

Answer: D

NEW QUESTION 293
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 298
For the firewall to use Active Directory to authenticate users, which Server Profile is required in the Authentication Profile?

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

Answer: C

Explanation:

Reference:
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/authentication/configure-an-authenticationprofile-and-sequence

NEW QUESTION 299
Choose the option that correctly completes this statement. A Security Profile can block or allow traffic .

A. on either the data place or the management plane.
B. after it is matched by a security policy rule that allows traffic.
C. before it is matched to a Security policy rule.
D. after it is matched by a security policy rule that allows or blocks traffic.

Answer: B

Explanation:

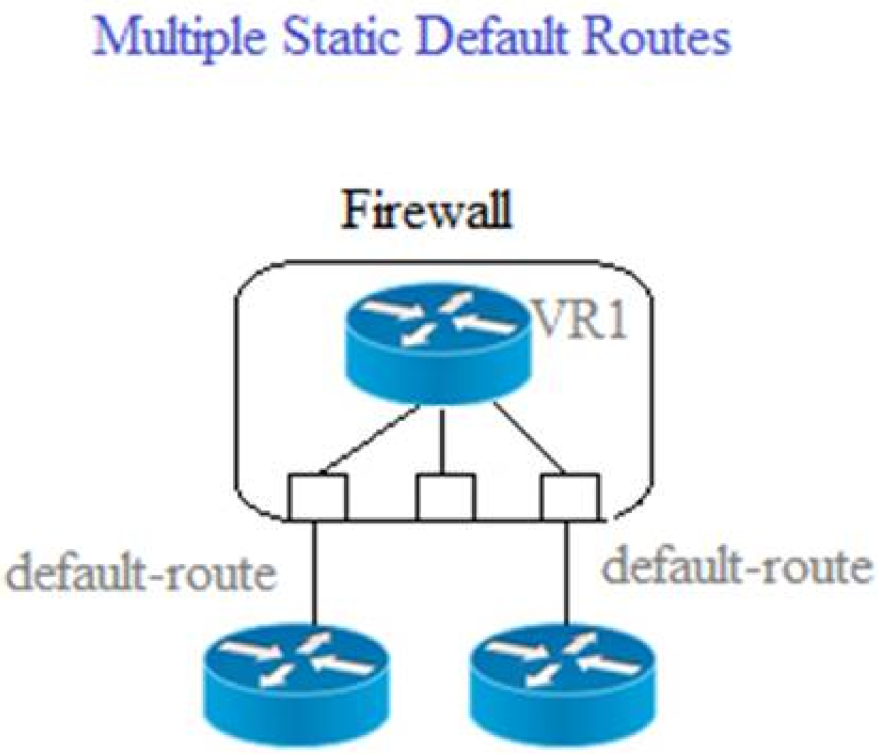
Reference:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/security-policy.html
After a packet has been allowed by the Security policy, Security Profiles are used to scan packets for threats, vulnerabilities, viruses, spyware, malicious URLs, data exfiltration, and exploitation software.

NEW QUESTION 304
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 305
Given the scenario, which two statements are correct regarding multiple static default routes? (Choose two.)



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

Answer: CD

NEW QUESTION 309
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 314
Which type of address object is "10 5 1 1/0 127 248 2"?

A. IP subnet
B. IP wildcard mask
C. IP netmask
D. IP range

Answer: B

NEW QUESTION 318
Palo Alto Networks firewall architecture accelerates content map minimizing latency using which two components'? (Choose two)

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

Answer: B

NEW QUESTION 322
Your company requires positive username attribution of every IP address used by wireless devices to support a new compliance requirement. You must collect IP –to-user mappings as soon as possible with minimal downtime and minimal configuration changes to the wireless devices themselves. The wireless devices are from various manufactures.
Given the scenario, choose the option for sending IP-to-user mappings to the NGFW.

A. syslog
B. RADIUS
C. UID redistribution
D. XFF headers

Answer: A

NEW QUESTION 327
An administrator wishes to follow best practices for logging traffic that traverses the firewall Which log setting is correct?

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

Answer: B

Explanation:

Reference:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Clt5CAC

NEW QUESTION 332
An administrator would like to override the default deny action for a given application and instead would like to block the traffic and send the ICMP code "communication with the destination is administratively prohibited"
Which security policy action causes this?

A. Drop
B. Drop, send ICMP Unreachable
C. Reset both
D. Reset server

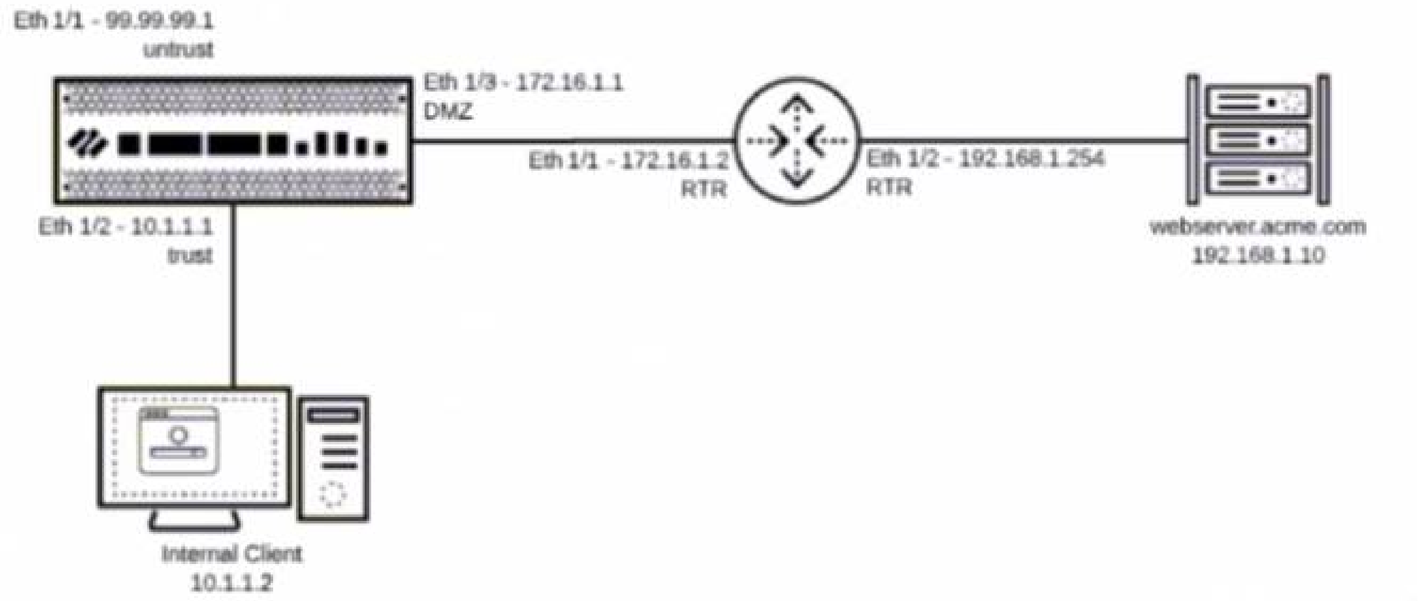
Answer: B

NEW QUESTION 333
An administrator wants to create a NAT policy to allow multiple source IP addresses to be translated to the same public IP address. What is the most appropriate NAT policy to achieve this?

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

Answer: A

NEW QUESTION 338
You have been tasked to configure access to a new web server located in the DMZ
Based on the diagram what configuration changes are required in the NGFW virtual router to route traffic from the 10 1 1 0/24 network to 192 168 1 0/24?



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

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

Answer: C

NEW QUESTION 342
Your company is highly concerned with their Intellectual property being accessed by unauthorized resources. There is a mature process to store and include metadata tags for all confidential documents.
Which Security profile can further ensure that these documents do not exit the corporate network?

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

Answer: B

Explanation:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/objects/objects-security-profiles-data-filtering

NEW QUESTION 347
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

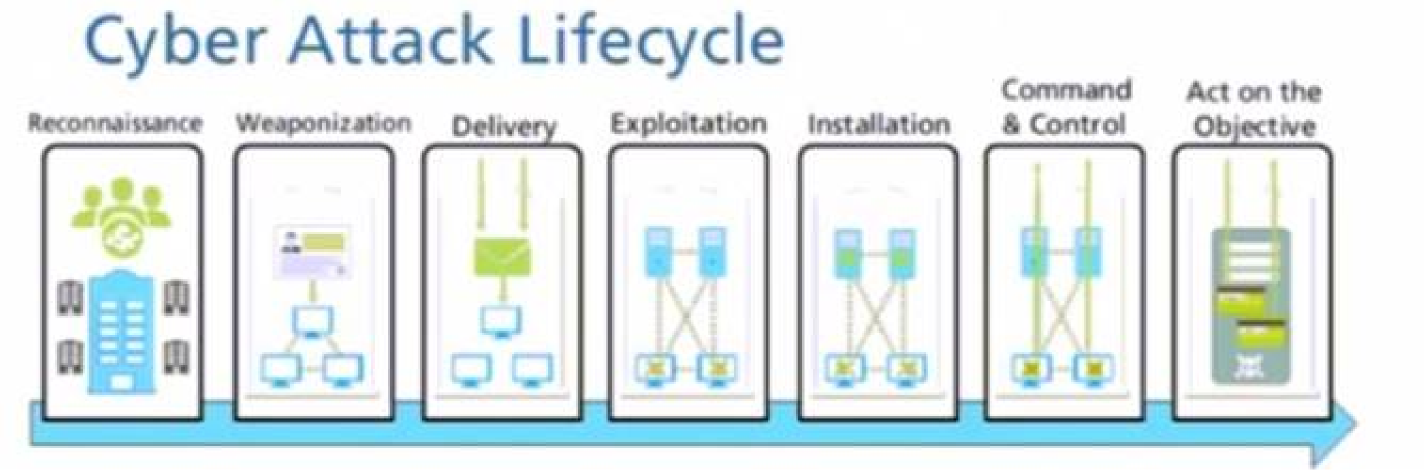
Vulnerability Protection Security Profiles protect against threats entering the network. For example, Vulnerability Protection Security Profiles protect against buffer overflows, illegal code execution, and other attempts to exploit system vulnerabilities. The default Vulnerability Protection Security 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 348
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 350
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

Answer: A

NEW QUESTION 354

Which type firewall configuration contains in-progress configuration changes?

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

Answer: C

NEW QUESTION 356
A network administrator created an intrazone Security policy rule on the firewall. The source zones were set to IT. Finance, and HR.
Which two types of traffic will the rule apply to? (Choose two)

A. Mastered
B. Not Mastered

Answer: A

NEW QUESTION 361
URL categories can be used as match criteria on which two policy types? (Choose two.)

A. authentication
B. decryptionC application override
C. NAT

Answer: AB

Explanation:

Reference:https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/url-filtering/url-filtering-concepts/url-category-as-policy-match-criteria.html

NEW QUESTION 365
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 368
How frequently can wildfire updates be made available to firewalls?

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

Answer: D

NEW QUESTION 370
Which object would an administrator create to block access to all high-risk applications?

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Reference:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClKECA0

NEW QUESTION 373
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 376
The compliance officer requests that all evasive applications need to be blocked on all perimeter firewalls out to the internet The firewall is configured with two zones;
* 1. trust for internal networks
* 2. untrust to the internet
Based on the capabilities of the Palo Alto Networks NGFW, what are two ways to configure a security policy using App-ID to comply with this request? (Choose two)

A. Create a deny rule at the top of the policy from trust to untrust with service application- default and add an application filter with the evasive characteristic
B. Create a deny rule at the top of the policy from trust to untrust over any service and select evasive as the application
C. Create a deny rule at the top of the policy from trust to untrust with service application- default and select evasive as the application
D. Create a deny rule at the top of the policy from trust to untrust over any service and add an application filter with the evasive characteristic

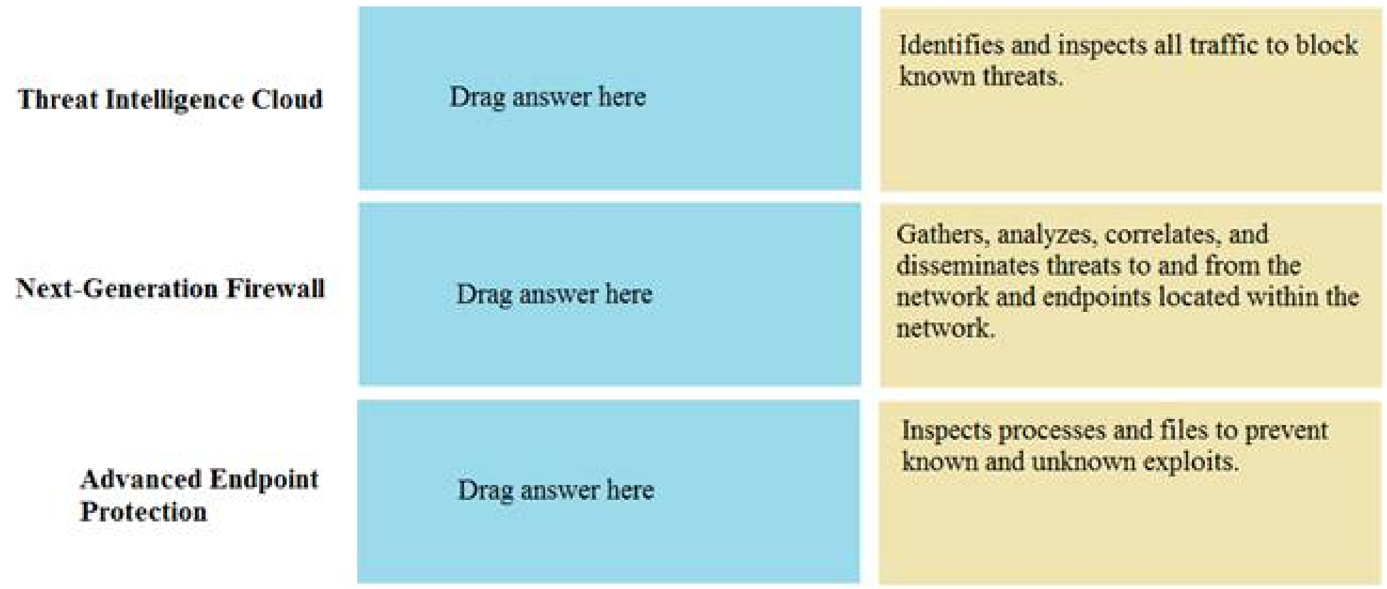
Answer: AD

NEW QUESTION 381
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 383
DRAG DROP
Match the Palo Alto Networks Security Operating Platform architecture to its description.



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

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 384
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 387
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 390
Starting with PAN_OS version 9.1 which new type of object is supported for use within the user field of a security policy rule?

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

Answer: B

NEW QUESTION 394
An administrator is troubleshooting an issue with traffic that matches the intrazone-default rule, which is set to default configuration.
What should the administrator do?

A. Mastered
B. Not Mastered

Answer: A

NEW QUESTION 396
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

Answer: BD

NEW QUESTION 399
Files are sent to the WildFire cloud service via the WildFire Analysis Profile. How are these files used?

A. WildFire signature updates
B. Malware analysis
C. Domain Generation Algorithm (DGA) learning
D. Spyware analysis

Answer: B

NEW QUESTION 401
An administrator would like to determine the default deny action for the application dns- over-https
Which action would yield the information?

A. View the application details in beacon paloaltonetworks.com
B. Check the action for the Security policy matching that traffic
C. Check the action for the decoder in the antivirus profile
D. View the application details in Objects > Applications

Answer: D

Explanation:

NEW QUESTION 403
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

Answer: ACDEF

NEW QUESTION 407
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

Answer: B

NEW QUESTION 408
Which administrator type utilizes predefined roles for a local administrator account?

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

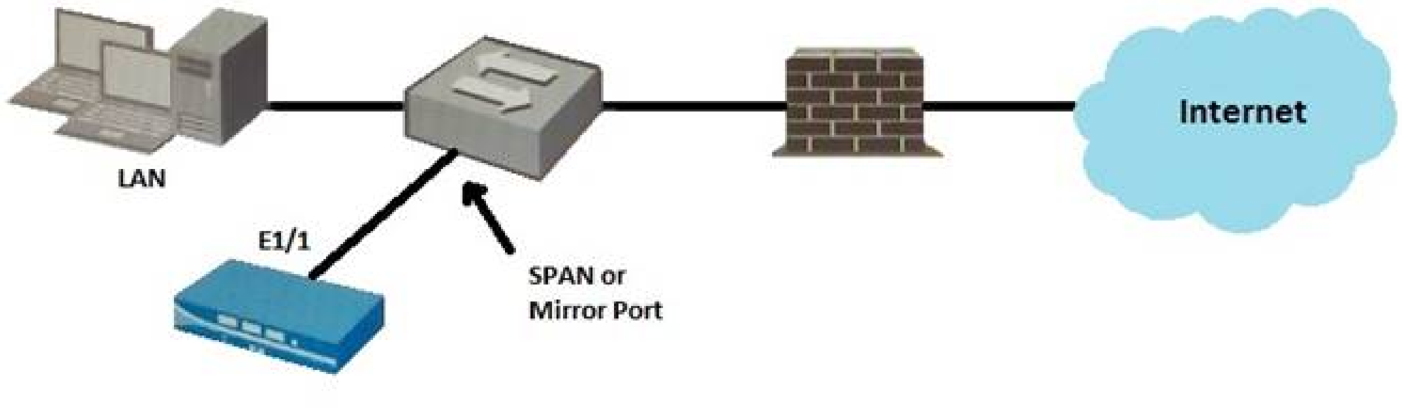
Answer: C

NEW QUESTION 412
An administrator is troubleshooting traffic that should match the interzone-default rule. However, the administrator doesn't see this traffic in the traffic logs on the firewall. The interzone-default was never changed from its default configuration.
Why doesn't the administrator see the traffic?

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

Answer: A

NEW QUESTION 414
Given the topology, which zone type should interface E1/1 be configured with?



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

Answer: A

NEW QUESTION 416
Recently changes were made to the firewall to optimize the policies and the security team wants to see if those changes are helping.
What is the quickest way to reset the hit counter to zero in all the security policy rules?

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

Answer: D

NEW QUESTION 418
An administrator would like to see the traffic that matches the interzone-default rule in the traffic logs.
What is the correct process to enable this logging1?

A. Select the interzone-default rule and edit the rule on the Actions tab select Log at Session Start and click OK
B. Select the interzone-default rule and edit the rule on the Actions tab select Log at Session End and click OK
C. This rule has traffic logging enabled by default no further action is required
D. Select the interzone-default rule and click Override on the Actions tab select Log at Session End and click OK

Answer: D

NEW QUESTION 422
......