Paloalto-Networks

Exam Questions PCNSA

Palo Alto Networks Certified Network Security Administrator

NEW QUESTION 1
What are three ways application characteristics are used? (Choose three.)

A. As an attribute to define an application group
B. As a setting to define a new custom application
C. As an Object to define Security policies
D. As an attribute to define an application filter
E. As a global filter in the Application Command Center (ACC)

Answer: ABD

Explanation:

NEW QUESTION 2
Which attribute can a dynamic address group use as a filtering condition to determine its membership?

A. tag
B. wildcard mask
C. IP address
D. subnet mask

Answer: A

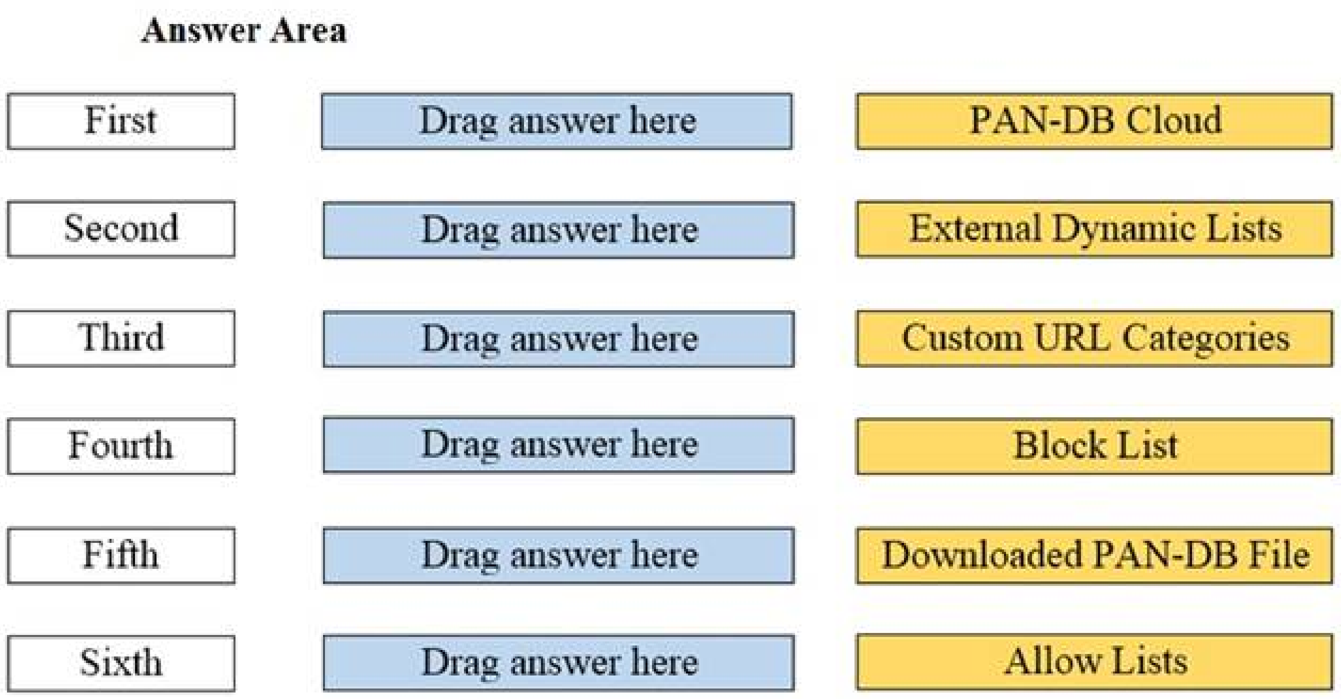
Explanation:
Dynamic Address Groups: A dynamic address group populates its members dynamically using looks ups for tags and tag-based filters. Dynamic address groups are very useful if you have an extensive virtual infrastructure where changes in virtual machine location/IP address are frequent. For example, you have a sophisticated failover setup or provision new virtual machines frequently and would like to apply policy to traffic from or to the new machine without modifying the configuration/rules on the firewall. https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface-help/objects/objects- address-groups

NEW QUESTION 3
Which Security policy action will message a user's browser thai their web session has been terminated?

A. Mastered
B. Not Mastered

Answer: A

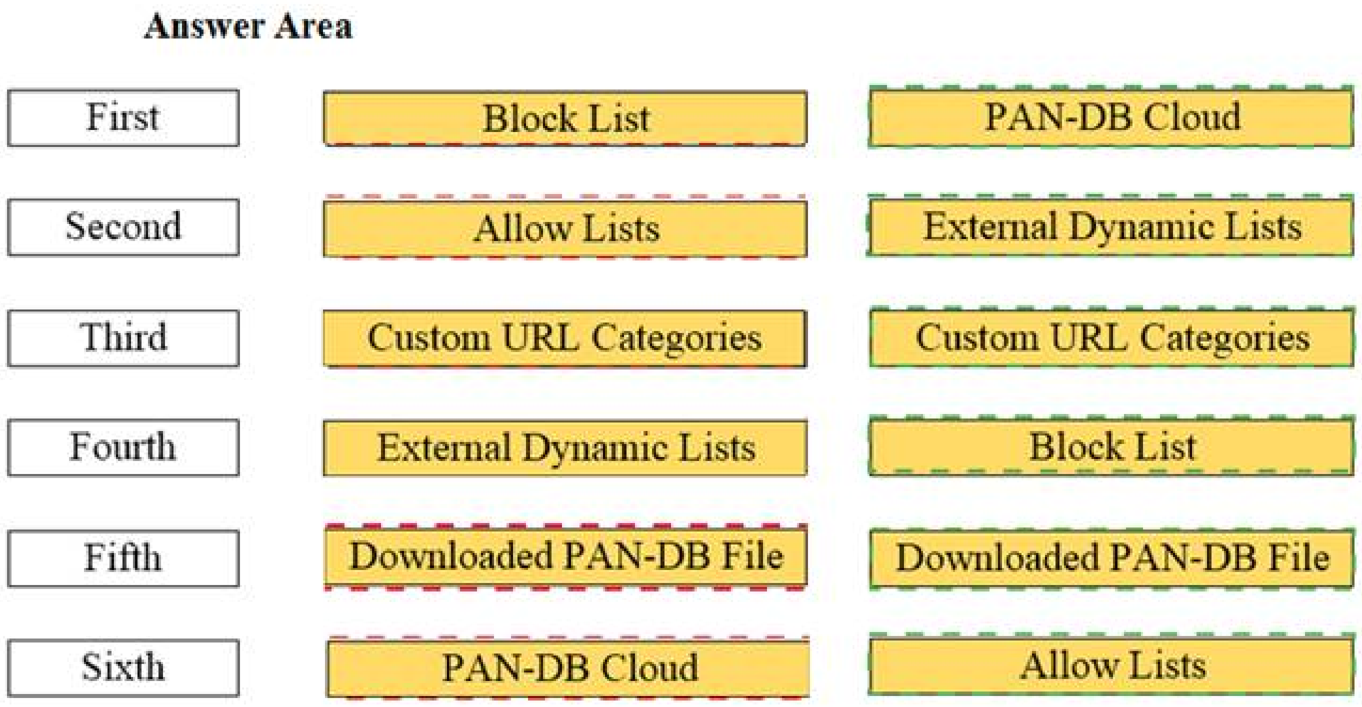
NEW QUESTION 4
DRAG DROP
Arrange the correct order that the URL classifications are processed within the system.



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

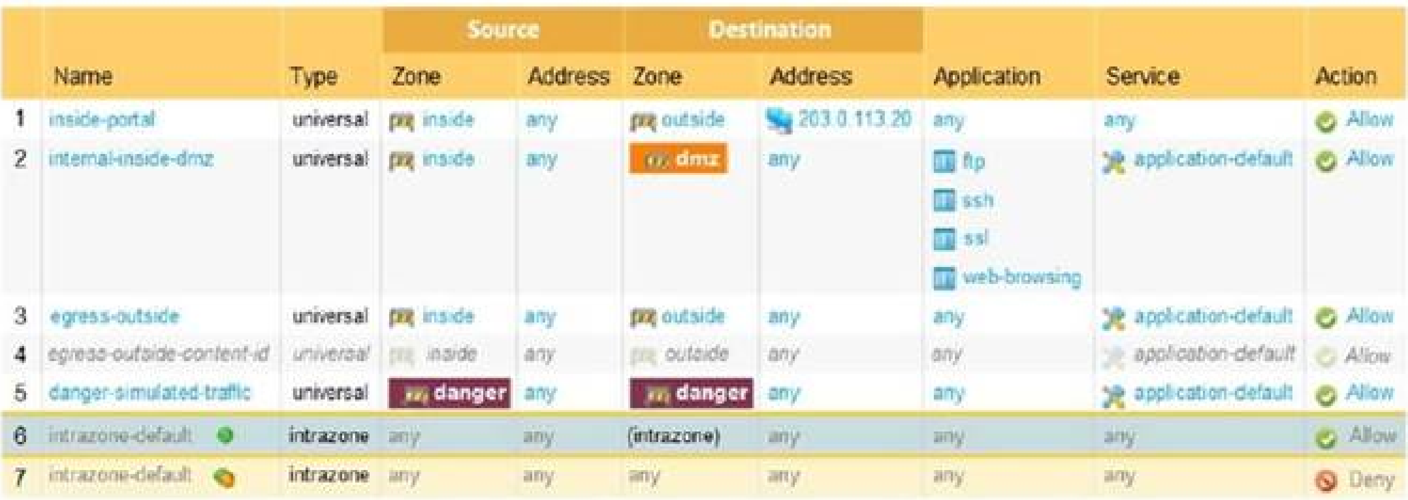
First	Block List	PAN-DB Cloud
Second	Allow Lists	External Dynamic Lists
Third	Custom URL Categories	Custom URL Categories
Fourth	External Dynamic Lists	Block List
Fifth	Downloaded PAN-DB File	Downloaded PAN-DB File
Sixth	PAN-DB Cloud	Allow Lists

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 5
Based on the show security policy rule would match all FTP traffic from the inside zone to the outside zone?



			Source		Destination				
	Name	Type	Zone	Address	Zone	Address	Application	Service	Action
1	inside-portal	universal	inside	any	outside	203.0.113.20	any	any	Allow
2	internal-inside-dmz	universal	inside	any	dmz	any	ftp ssh ssl web-browsing	application-default	Allow
3	egress-outside	universal	inside	any	outside	any	any	application-default	Allow
4	egress-outside-content-id	universal	inside	any	outside	any	any	application-default	Allow
5	danger-simulated-traffic	universal	danger	any	danger	any	any	application-default	Allow
6	intrazone-default	intrazone	any	any	(intrazone)	any	any	any	Allow
7	intrazone-default	intrazone	any	any	any	any	any	any	Deny

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

Answer: B

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 two rule types allow the administrator to modify the destination zone? (Choose two)

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

Answer: AC

NEW QUESTION 8
Which action related to App-ID updates will enable a security administrator to view the existing security policy rule that matches new application signatures?

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

Answer: A

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

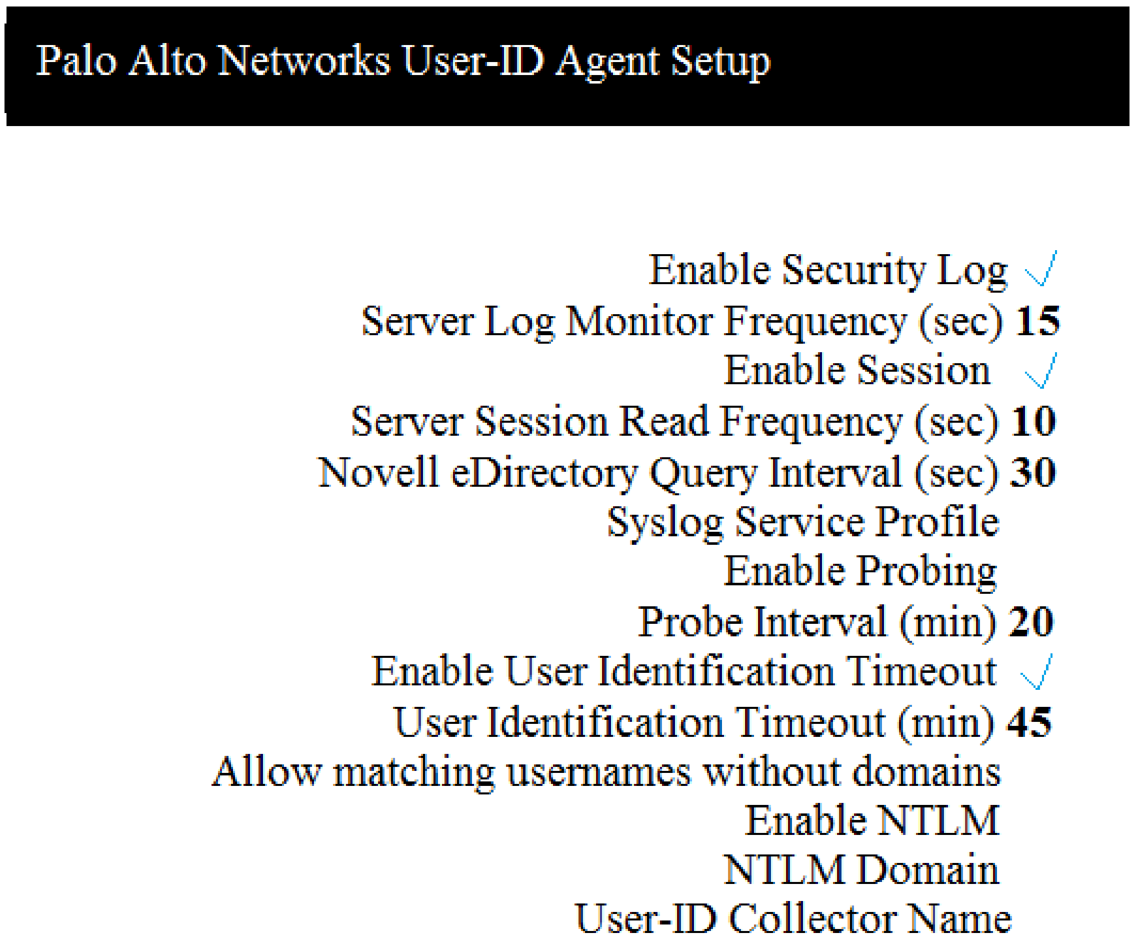
NEW QUESTION 9
What is considered best practice with regards to committing configuration changes?

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 10

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 10
What can be achieved by selecting a policy target prior to pushing policy rules from Panorama?

A. Doing so limits the templates that receive the policy rules
B. Doing so provides audit information prior to making changes for selected policy rules
C. You can specify the firewalls m a device group to which to push policy rules
D. You specify the location as pre can - or post-rules to push policy rules

Answer: C

NEW QUESTION 12
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 13
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 15
What two authentication methods on the Palo Alto Networks firewalls support authentication and authorization for role-based access control? (Choose two.)

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

Answer: AB

Explanation:

Reference:https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/firewall-administration/manage-firewall-administrators/administrative-authentication.html

The administrative accounts are defined on an external SAML, TACACS+, or RADIUS server. The server performs both authentication and authorization. For authorization, you define Vendor-Specific Attributes (VSAs) on the TACACS+ or RADIUS server, or SAML attributes on the SAML server. PAN-OS maps the attributes to administrator roles, access domains, user groups, and virtual systems that you define on the firewall.

NEW QUESTION 19

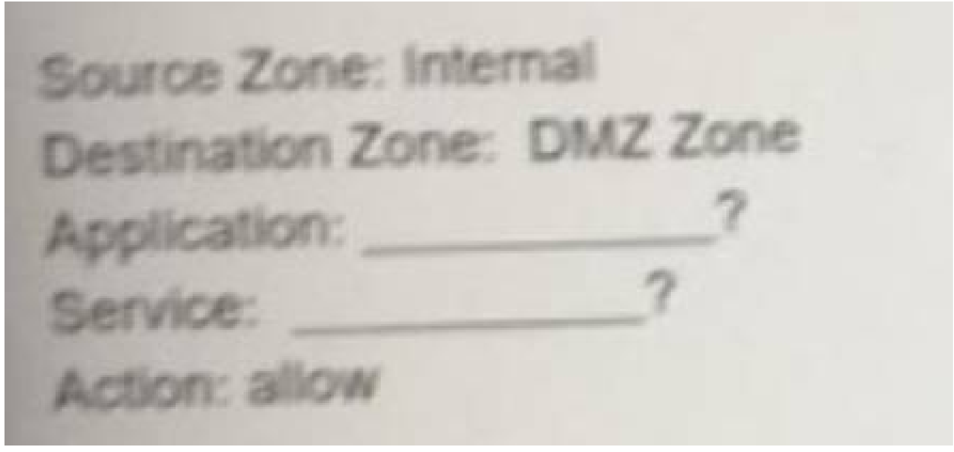
What do you configure if you want to set up a group of objects based on their ports alone?

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

Answer: B

NEW QUESTION 20

All users from the internal zone must be allowed only Telnet access to a server in the DMZ zone. Complete the two empty fields in the Security Policy rules that permits only this type of access.



Source Zone: Internal
Destination Zone: DMZ Zone
Application: ________________?
Service: ________________?
Action: allow

Choose two.

A.

Service = "any"
B. Application = "Telnet"
C. Service - "application-default"
D. Application = "any"

Answer: BC

NEW QUESTION 23
An administrator configured a Security policy rule where the matching condition includes a single application and the action is set to deny. What deny action will the firewall perform?

A. Drop the traffic silently
B. Perform the default deny action as defined in the App-ID database for the application
C. Send a TCP reset packet to the client- and server-side devices
D.

Discard the session's packets and send a TCP reset packet to let the client know the session has been terminated

Answer: D

NEW QUESTION 26
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 27
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 29
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 30
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

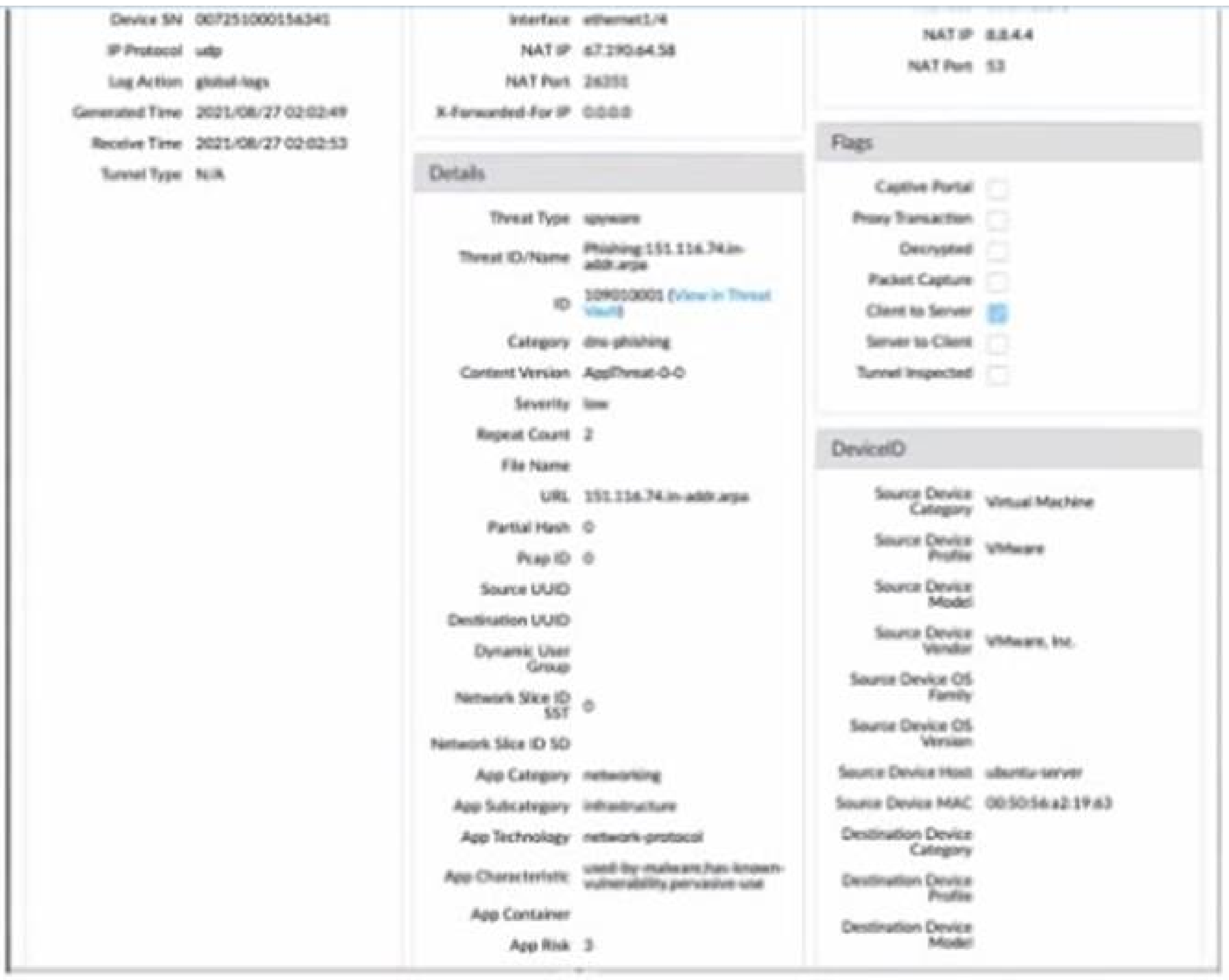
Answer: B

NEW QUESTION 33
Which three interface deployment methods can be used to block traffic flowing through the Palo Alto Networks firewall? (Choose three.)

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

Answer: BDE

NEW QUESTION 34
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 26251
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

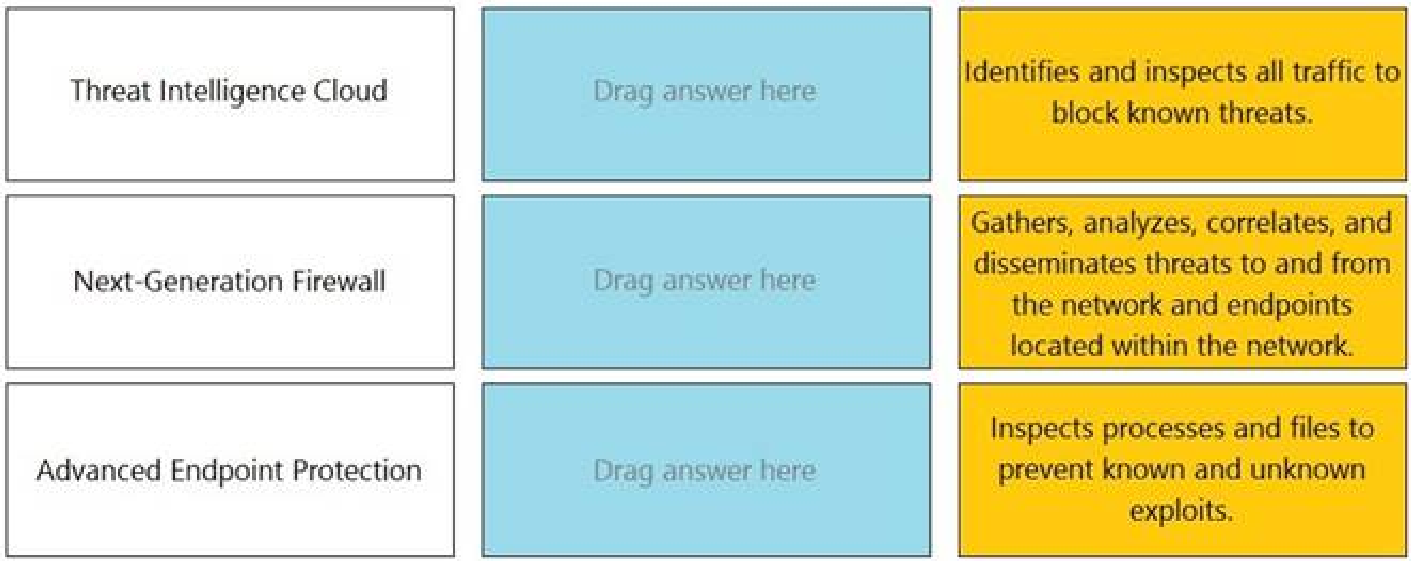
NEW QUESTION 36
Which feature would be useful for preventing traffic from hosting providers that place few restrictions on content, whose services are frequently used by attackers to distribute illegal or unethical material?

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 37
DRAG DROP
Match each feature to the DoS Protection Policy or the DoS Protection Profile.

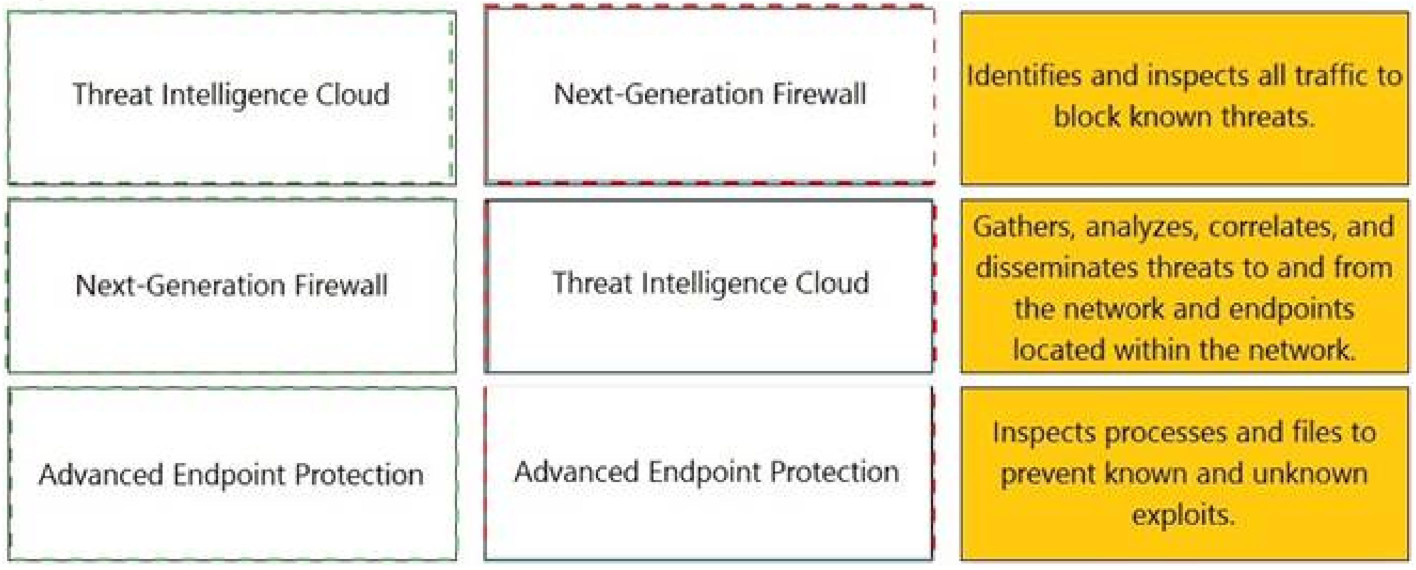


Threat Intelligence Cloud	Drag answer here	Identifies and inspects all traffic to block known threats.
Next-Generation Firewall	Drag answer here	Gathers, analyzes, correlates, and disseminates threats to and from the network and endpoints located within the network.
Advanced Endpoint Protection	Drag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

A. Mastered
B. Not Mastered

Answer: A

Explanation:



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

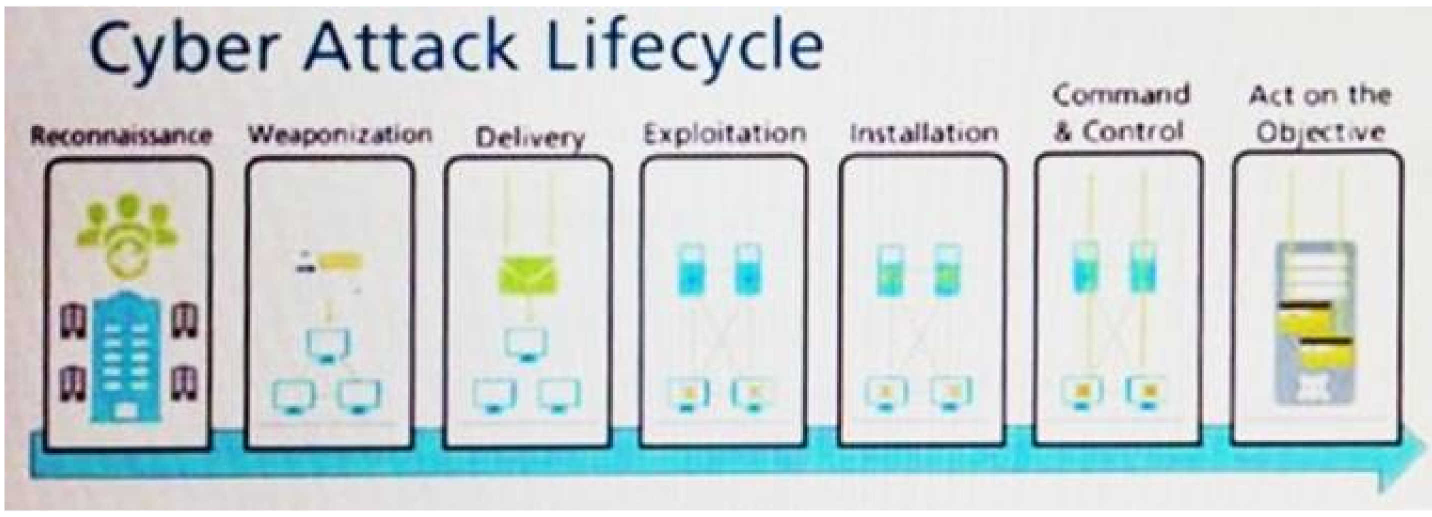
NEW QUESTION 39
Which two features can be used to tag a username so that it is included in a dynamic user group? (Choose two.)

A. GlobalProtect agent
B. XML API
C.

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

Answer: BC

NEW QUESTION 41
Given the Cyber-Attack Lifecycle diagram, identify the stage in which the attacker can initiate malicious code against a targeted machine.



A.

Exploitation

B. Installation
C. Reconnaissance
D. Act on Objective

Answer: A

NEW QUESTION 43
To use Active Directory to authenticate administrators, which server profile is required in the authentication profile?

A. Mastered
B. Not Mastered

Answer: A

NEW QUESTION 48
Which statement is true about Panorama managed devices?

A. Panorama automatically removes local configuration locks after a commit from Panorama
B. Local configuration locks prohibit Security policy changes for a Panorama managed device
C. Security policy rules configured on local firewalls always take precedence
D. Local configuration locks can be manually unlocked from Panorama

Answer: D

Explanation:
Explanation Explanation/Reference: Reference:
https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/administer- panorama/manage- locks-forrestricting-configuration-changes.html

NEW QUESTION 49
An address object of type IP Wildcard Mask can be referenced in which part of the configuration?

A. Security policy rule
B. ACC global filter
C. external dynamic list
D. NAT address pool

Answer: A

Explanation:
You can use an address object of type IP Wildcard Mask only in a Security policy rule.
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/objects/objects- addresses
IP Wildcard Mask—Enter an IP wildcard address in the format of an IPv4 address followed by a slash and a mask (which must begin with a zero); for example, 10.182.1.1/0.127.248.0. In the wildcard mask, a zero (0) bit indicates that the bit being compared must match the bit in the IP address that is covered by the 0. A one (1) bit in the mask is a wildcard bit, meaning the bit being compared need not match the bit in the IP address that is covered by the 1. Convert the IP address and the wildcard mask to binary. To illustrate the matching: on binary snippet 0011, a wildcard mask of 1010 results in four matches (0001, 0011, 1001, and 1011).

NEW QUESTION 51
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 55
Assume a custom URL Category Object of "NO-FILES" has been created to identify a specific website
How can file uploading/downloading be restricted for the website while permitting general browsing access to that website?

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

Answer: B

NEW QUESTION 59
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 64
What allows a security administrator to preview the Security policy rules that match new application signatures?

A. Review Release Notes
B. Dynamic Updates-Review Policies
C. Dynamic Updates-Review App
D. Policy Optimizer-New App Viewer

Answer: B

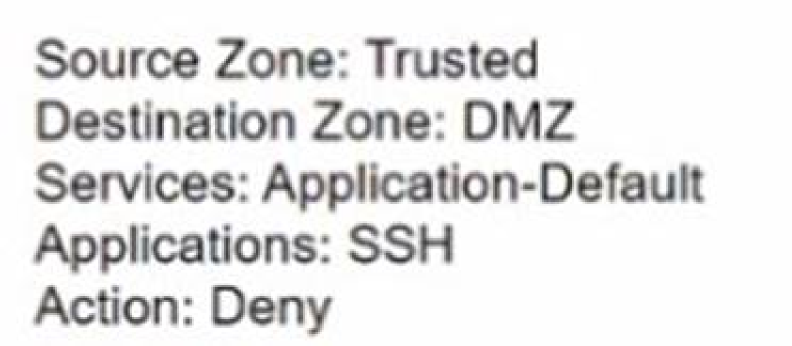
Explanation:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/app-id/manage- new-app-ids-introduced-in-content-releases/review-new-app-id-impact-on-existing-policy- rules

NEW QUESTION 65
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

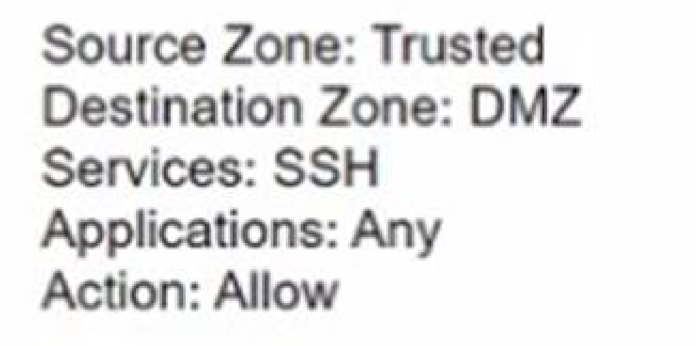
Answer: D

NEW QUESTION 70
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)



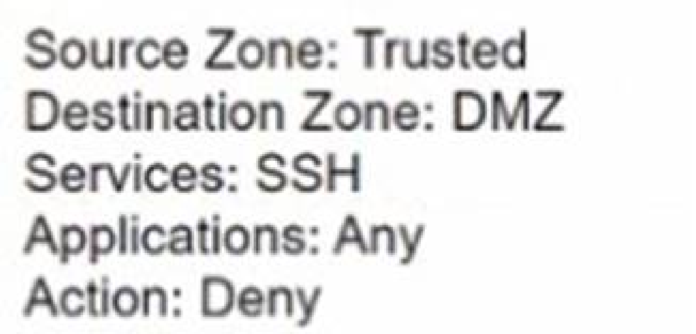
Source Zone: Trusted
Destination Zone: DMZ
Services: Application-Default
Applications: SSH
Action: Deny

B)



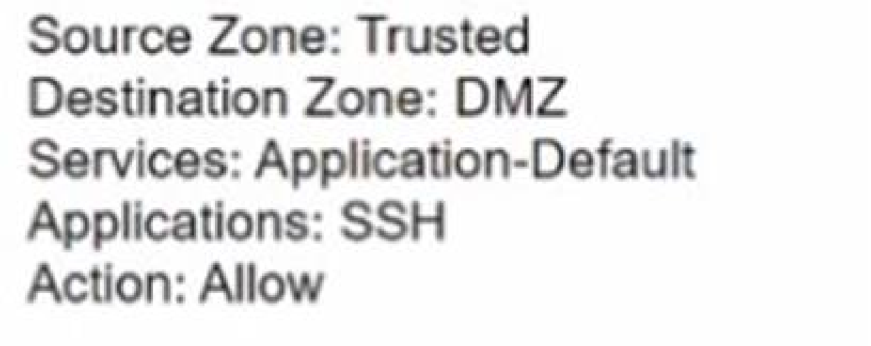
Source Zone: Trusted
Destination Zone: DMZ
Services: SSH
Applications: Any
Action: Allow

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 75

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 80
What is the main function of the Test Policy Match function?

A. verify that policy rules from Expedition are valid
B. confirm that rules meet or exceed the Best Practice Assessment recommendations
C. confirm that policy rules in the configuration are allowing/denying the correct traffic
D. ensure that policy rules are not shadowing other policy rules

Answer: D

NEW QUESTION 81
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 83
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 88
What does an application filter help you to do?

A. It dynamically provides application statistics based on network, threat, and blocked activity,
B. It dynamically filters applications based on critical, high, medium, 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 90
What are three valid ways to map an IP address to a username? (Choose three.)

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

Answer: ACD

NEW QUESTION 93
A server-admin in the USERS-zone requires SSH-access to all possible servers in all current and future Public Cloud environments. All other required connections have already been enabled between the USERS- and the OUTSIDE-zone. What configuration-changes should the Firewall-admin make?

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

Answer: B

NEW QUESTION 94
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

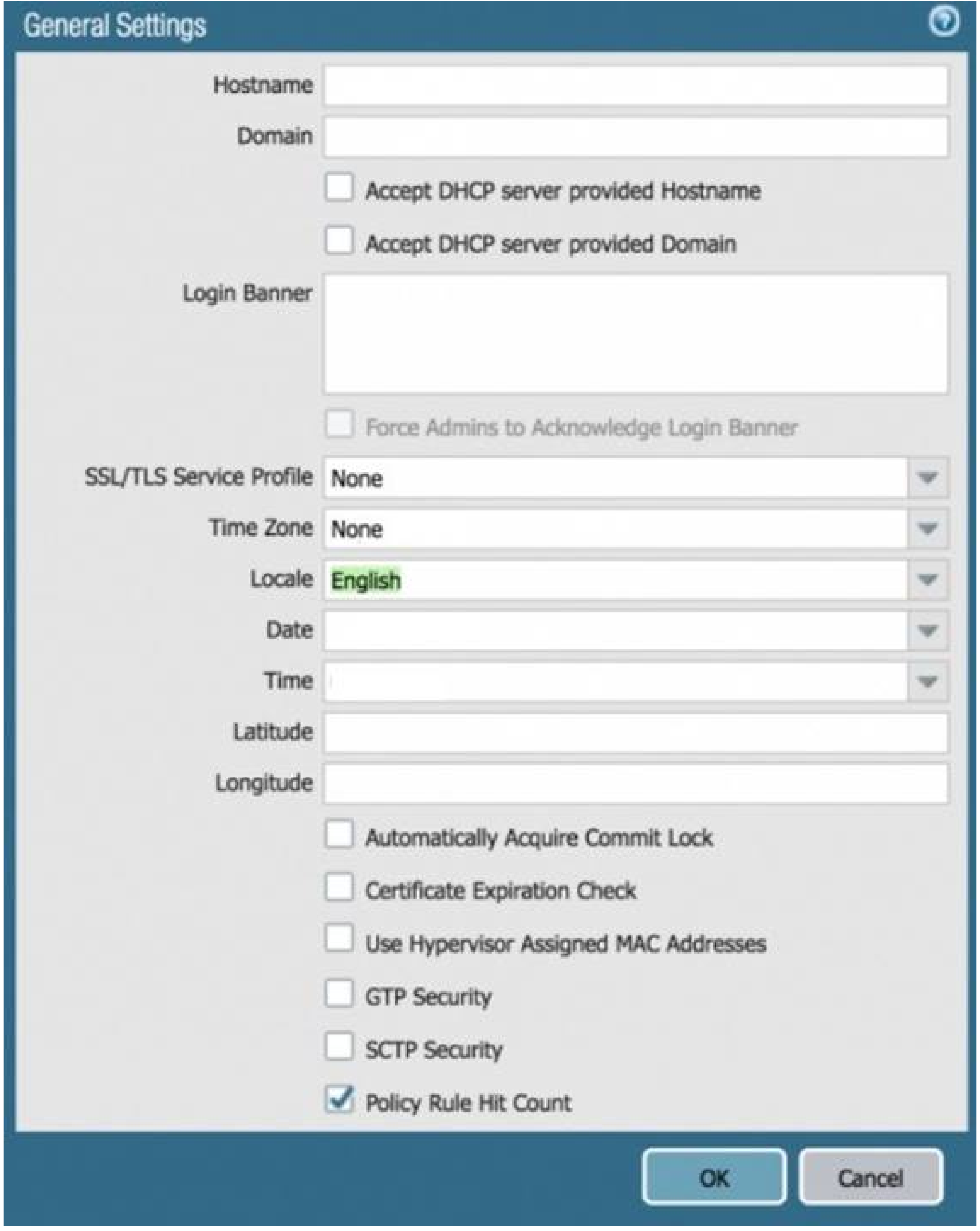
NEW QUESTION 99
Which interface type is part of a Layer 3 zone with a Palo Alto Networks firewall?

A. Management

B. High Availability
C. Aggregate
D. Aggregation

Answer: C

NEW QUESTION 103
Based on the graphic, what is the purpose of the SSL/TLS Service profile configuration option?



General Settings

Hostname

Domain

□ Accept DHCP server provided Hostname

□ Accept DHCP server provided Domain

Login Banner

□ Force Admins to Acknowledge Login Banner

SSL/TLS Service Profile: None

Time Zone: None

Locale: English

Date

Time

Latitude

Longitude

□ Automatically Acquire Commit Lock

□ Certificate Expiration Check

□ Use Hypervisor Assigned MAC Addresses

□ GTP Security

□ SCTP Security

☑ Policy Rule Hit Count

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

Answer: C

Explanation:
Reference:https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g00000 0ClFGCA0

NEW QUESTION 107
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 111
If using group mapping with Active Directory Universal Groups, what must you do when configuring the User-ID?

A. Create an LDAP Server profile to connect to the root domain of the Global Catalog server on port 3268 or 3269 for SSL

B. Configure a frequency schedule to clear group mapping cache
C. Configure a Primary Employee ID number for user-based Security policies
D. Create a RADIUS Server profile to connect to the domain controllers using LDAPS on port 636 or 389

Answer: B

Explanation:
? If you have Universal Groups, create an LDAP server profile to connect to the root domain of the Global Catalog server on port 3268 or 3269 for SSL, then create another LDAP server profile to connect to the root domain controllers on port 389. This helps ensure that users and group information is available for all domains and subdomains.
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/user-id/map-users-to-groups

NEW QUESTION 113

Which plane on a Palo alto networks firewall provides configuration logging and reporting functions on a separate processor?

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

Answer: C

NEW QUESTION 116
The CFO found a malware infected USB drive in the parking lot, which when inserted infected their corporate laptop the malware contacted a known command-and-control server which exfiltrating corporate data.
Which Security profile feature could have been used to prevent the communications with the command-and-control server?

A. Create a Data Filtering Profile and enable its DNS sinkhole feature.
B. Create an Antivirus Profile and enable its DNS sinkhole feature.
C. Create an Anti-Spyware Profile and enable its DNS sinkhole feature.
D. Create a URL Filtering Profile and block the DNS sinkhole URL category.

Answer: C

NEW QUESTION 119
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

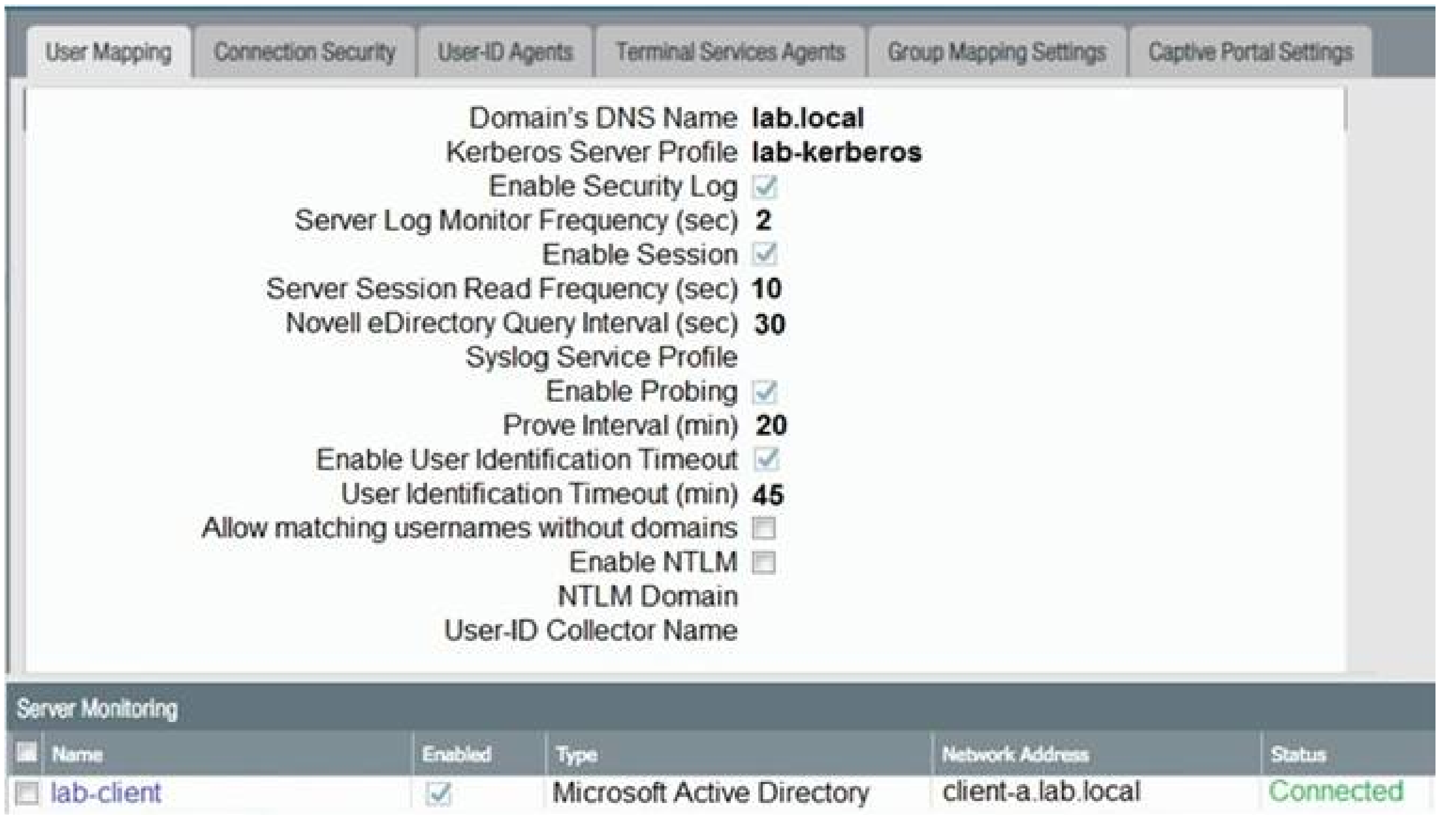
Answer: A

NEW QUESTION 120
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 124
Based on the graphic which statement accurately describes the output shown in the server monitoring panel?



Domain's DNS Name lab.local
Kerberos Server Profile lab-kerberos
Enable Security Log ☑
Server Log Monitor Frequency (sec) 2
Enable Session ☑
Server Session Read Frequency (sec) 10
Novell eDirectory Query Interval (sec) 30
Syslog Service Profile
Enable Probing ☑
Prove 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

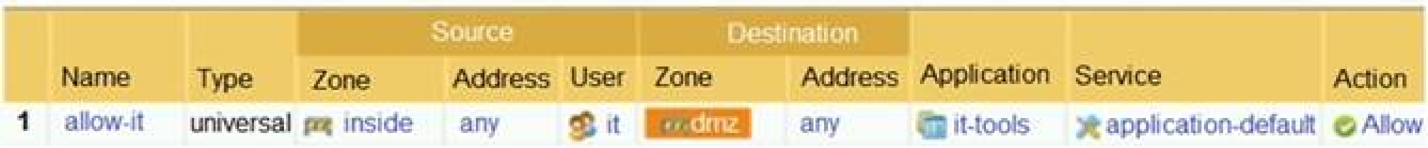
Server Monitoring

□ Name	Enabled	Type	Network Address	Status
□ lab-client	☑	Microsoft Active Directory	client-a.lab.local	Connected

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

Answer: A

NEW QUESTION 125
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:

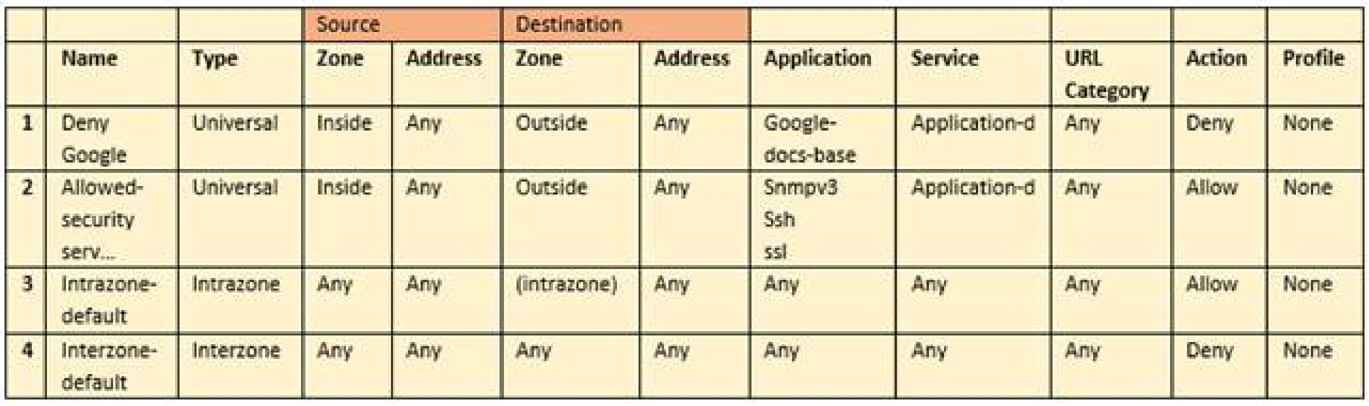
Reference:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/user-id/map-users-to- groups.html

NEW QUESTION 126
Selecting the option to revert firewall changes will replace what settings?

A. Mastered
B. Not Mastered

Answer: A

NEW QUESTION 128
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 130
Which definition describes the guiding principle of the zero-trust architecture?

A. never trust, never connect
B. always connect and verify
C. never trust, always verify
D. trust, but verity

Answer: C

Explanation:

Reference:
https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture

NEW QUESTION 131
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 135
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 137
During the App-ID update process, what should you click on to confirm whether an existing policy rule is affected by an App-ID update?

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

Answer: B

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

NEW QUESTION 138
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 140
Which three configuration settings are required on a Palo Alto networks firewall management interface?

A. default gateway
B. netmask

C. IP address
D. hostname
E. auto-negotiation

Answer: ABC

Explanation:

Reference:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClN7CAK

NEW QUESTION 142
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 144
Which tab would an administrator click to create an address object?

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

Answer: D

NEW QUESTION 149
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 152
Which action results in the firewall blocking network traffic without notifying the sender?

Deny

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

Answer: C

NEW QUESTION 153
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 156
By default, what is the maximum number of templates that can be added to a template stack?

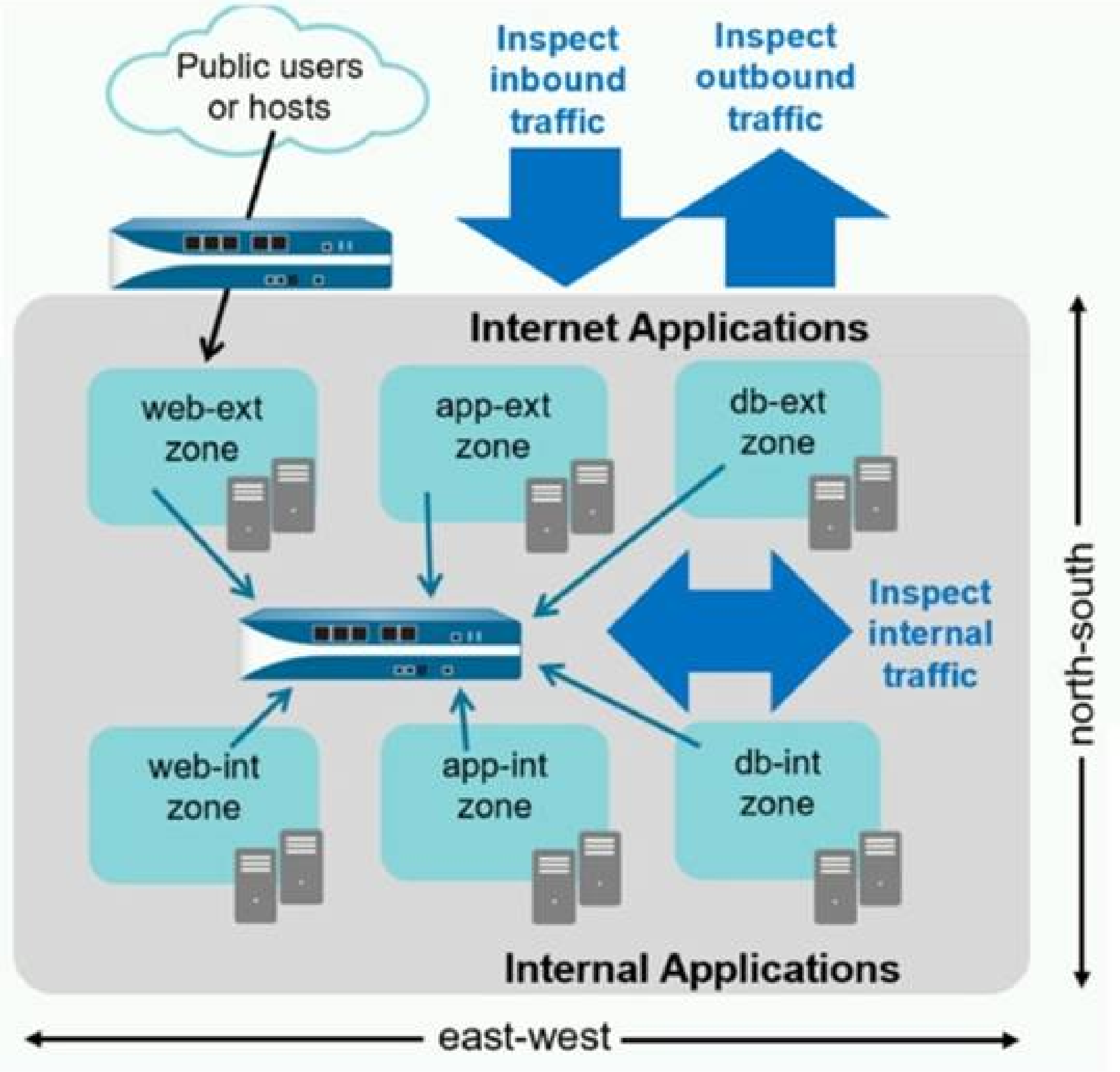
A. 6
B. 8

C. 10
D. 12

Answer: B

Explanation:
By default, the maximum number of templates that can be added to a template stack is 8. This is the recommended limit for performance reasons, as adding more templates may result in sluggish responses on the user interface. However, starting from PAN-OS 8.1.10 and 9.0.4, you can use a debug command to increase the maximum number of templates per stack to 16. This command requires a commit operation to take effect.
A template stack is a collection of templates that you can use to push common settings to multiple firewalls or Panorama managed collectors. A template contains the network and device settings that you want to share across devices, such as interfaces, zones, virtual routers, DNS, NTP, and login banners. You can create multiple templates for different device groups or locations and add them to a template stack in a hierarchical order. The settings in the lower templates override the settings in the higher templates if there are any conflicts. You can then assign a template stack to one or more devices and push the configuration changes.

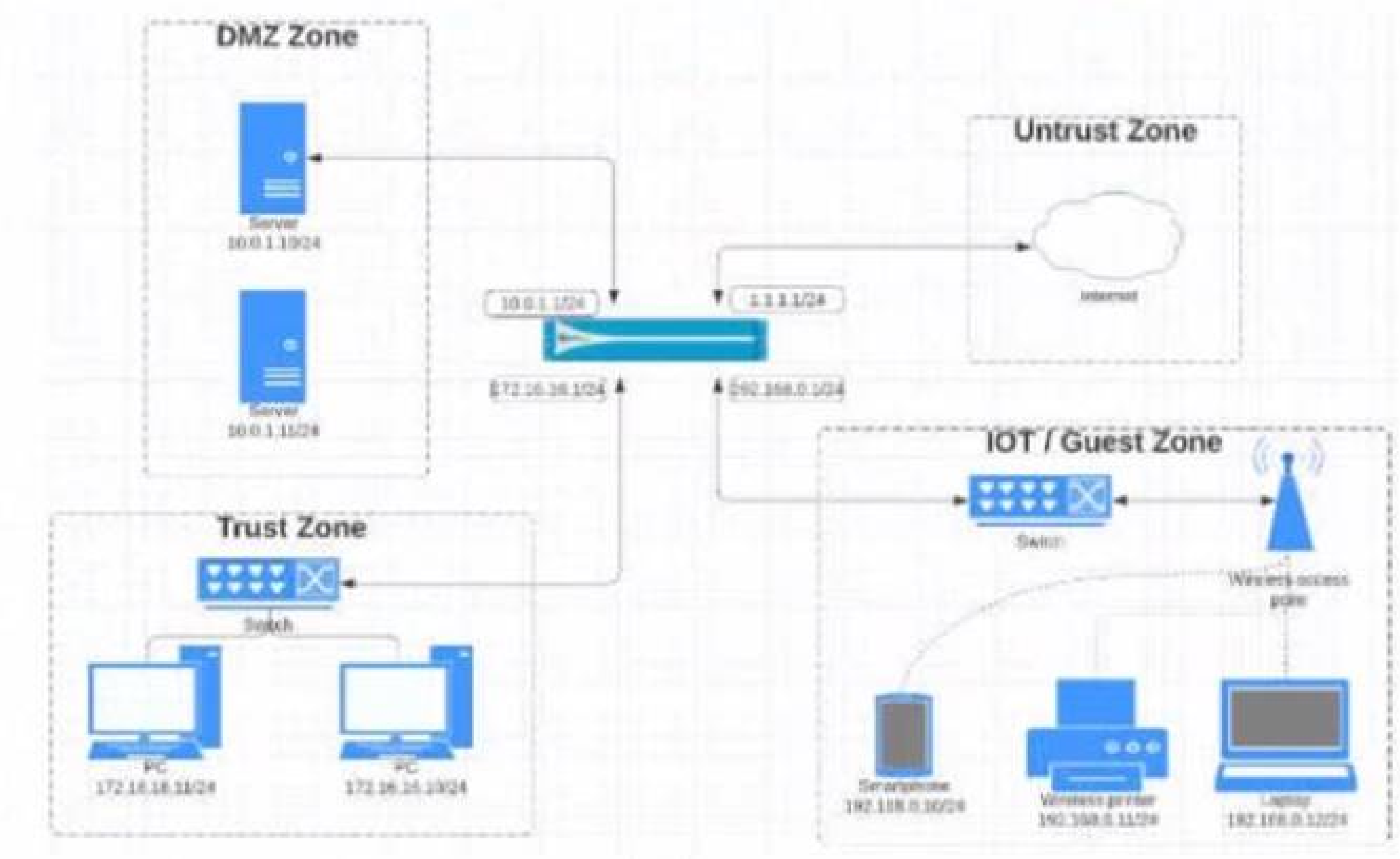
NEW QUESTION 161
An administrator notices that protection is needed for traffic within the network due to malicious lateral movement activity. Based on the image shown, which traffic would the administrator need to monitor and block to mitigate the malicious activity?



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

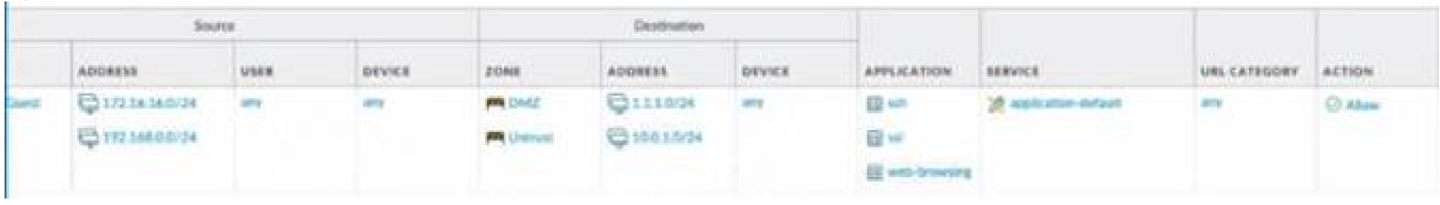
Answer: D

NEW QUESTION 165
View the diagram.



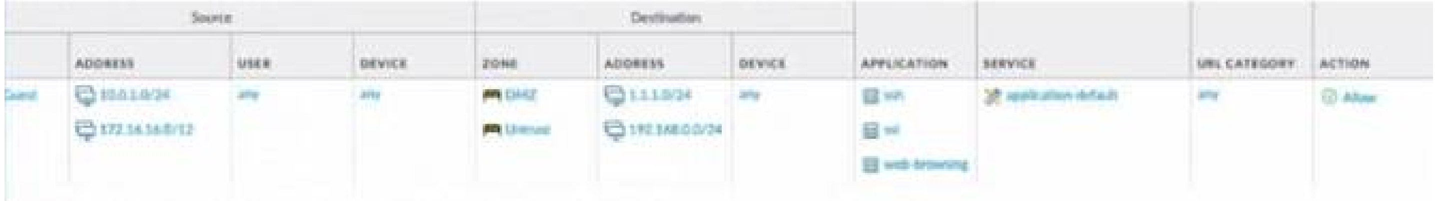
What is the most restrictive yet fully functional rule to allow general Internet and SSH traffic into both the DMZ and Untrust/Internet zones from each of the IOT/Guest and Trust Zones?

A)



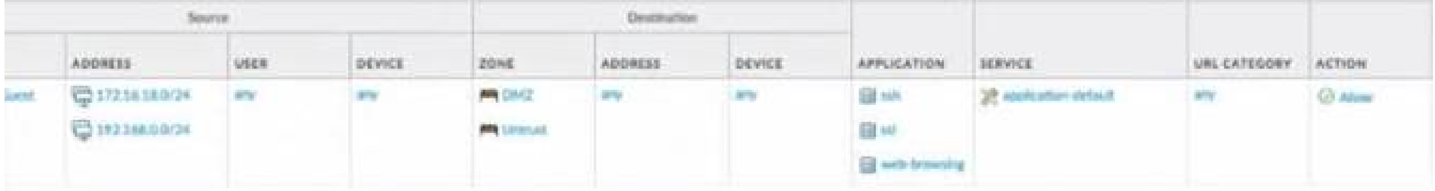
Source				Destination						
	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	URL CATEGORY	ACTION
Guest	172.16.16.0/24 192.168.0.0/24	any	any	DMZ Untrust	1.1.1.0/24 10.0.1.0/24	any	ssh ssl web-browsing	application-default	any	Allow

B)



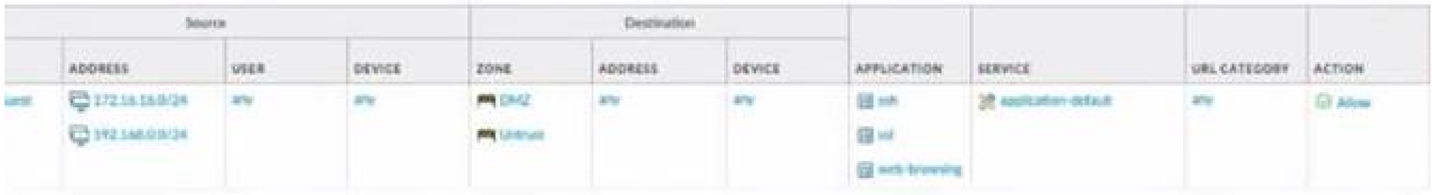
Source				Destination						
	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	URL CATEGORY	ACTION
Guest	10.0.1.0/24 172.16.16.0/12	any	any	DMZ Untrust	1.1.1.0/24 192.168.0.0/24	any	ssh ssl web-browsing	application-default	any	Allow

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 167
Within an Anti-Spyware security profile, which tab is used to enable machine learning based engines?

A. Inline Cloud Analysis
B. Signature Exceptions
C. Machine Learning Policies
D. Signature Policies

Answer: A

Explanation:
? An Anti-Spyware security profile is a set of rules that defines how the firewall detects and prevents spyware from compromising hosts on the network. Spyware is a type of malware that collects information from the infected system, such as keystrokes, browsing history, or personal data, and sends it to an external command-and-control (C2) server1.
? An Anti-Spyware security profile consists of four tabs: Signature Policies, Signature Exceptions, Machine Learning Policies, and Inline Cloud Analysis1.
? The Signature Policies tab allows you to configure the actions and log settings for each spyware signature category, such as adware, botnet, keylogger, phishing, or worm. You can also enable DNS Security to block malicious DNS queries and responses1.

? The Signature Exceptions tab allows you to create exceptions for specific spyware signatures that you want to override the default action or log settings. For example, you can allow a signature that is normally blocked by the profile, or block a signature that is normally alerted by the profile1.
? The Machine Learning Policies tab allows you to configure the actions and log settings for machine learning based signatures that detect unknown spyware variants. You can also enable WildFire Analysis to submit unknown files to the cloud for further analysis1.
? The Inline Cloud Analysis tab allows you to enable machine learning based engines that detect unknown spyware variants in real time. These engines use cloud-based models to analyze the behavior and characteristics of network traffic and identify malicious patterns. You can enable inline cloud analysis for HTTP/HTTPS traffic, SMTP/SMTPS traffic, or IMAP/IMAPS traffic1.
Therefore, the tab that is used to enable machine learning based engines is the Inline Cloud Analysis tab. References:
1: Security Profile: Anti-Spyware - Palo Alto Networks

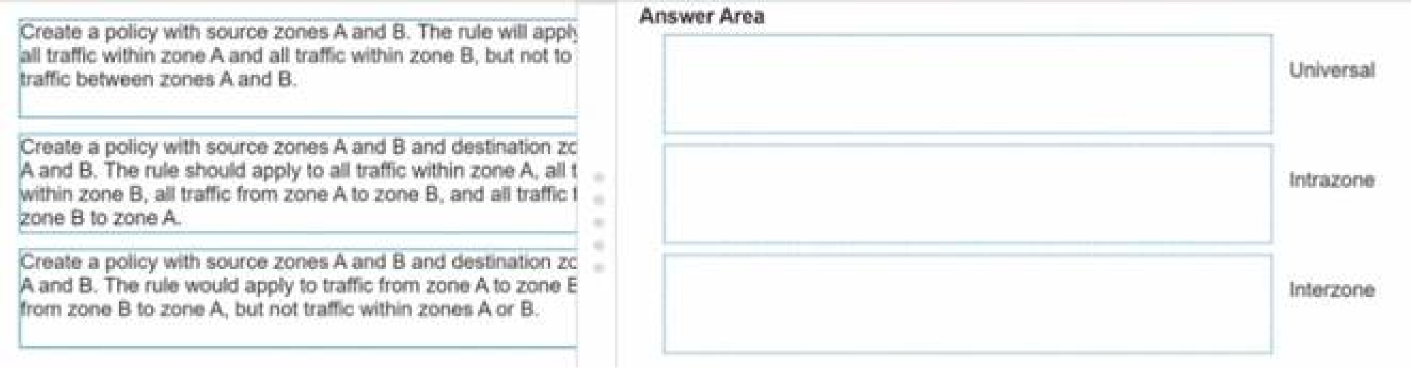
NEW QUESTION 169
How are service routes used in PAN-OS?

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 170
DRAG DROP
Match each rule type with its example



Create a policy with source zones A and B. The rule will apply all traffic within zone A and all traffic within zone B, but not to traffic between zones A and B.

Create a policy with source zones A and B and destination zc A and B. The rule should apply to all traffic within zone A, all t within zone B, all traffic from zone A to zone B, and all traffic t zone B to zone A.

Create a policy with source zones A and B and destination zc A and B. The rule would apply to traffic from zone A to zone E from zone B to zone A, but not traffic within zones A or B.

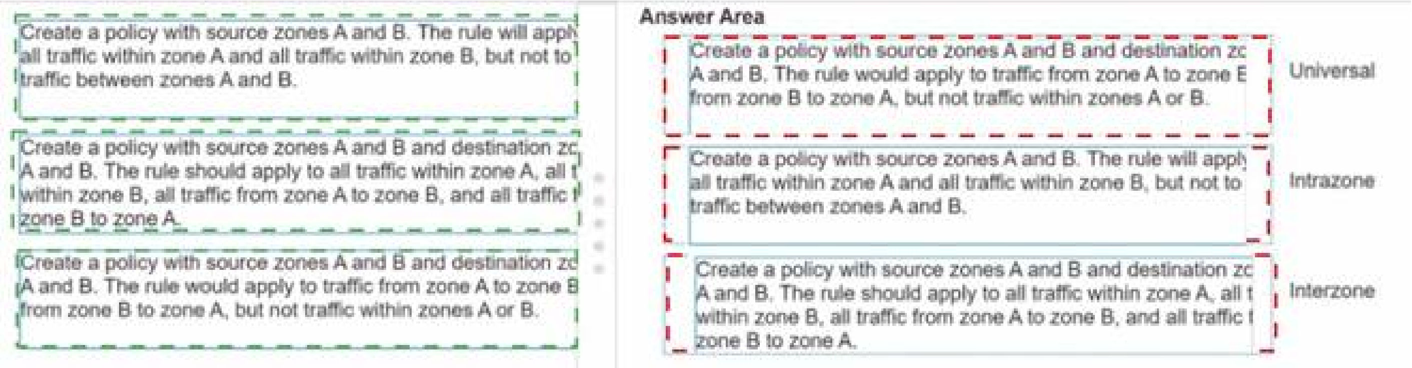
Answer Area

	Universal
	Intrazone
	Interzone

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Create a policy with source zones A and B. The rule will apply all traffic within zone A and all traffic within zone B, but not to traffic between zones A and B.

Create a policy with source zones A and B and destination zc A and B. The rule should apply to all traffic within zone A, all t within zone B, all traffic from zone A to zone B, and all traffic zone B to zone A.

Create a policy with source zones A and B and destination zc A and B. The rule would apply to traffic from zone A to zone B from zone B to zone A, but not traffic within zones A or B.

Answer Area

Create a policy with source zones A and B and destination zc A and B. The rule would apply to traffic from zone A to zone E from zone B to zone A, but not traffic within zones A or B.	Universal
Create a policy with source zones A and B. The rule will apply all traffic within zone A and all traffic within zone B, but not to traffic between zones A and B.	Intrazone
Create a policy with source zones A and B and destination zc A and B. The rule should apply to all traffic within zone A, all t within zone B, all traffic from zone A to zone B, and all traffic t zone B to zone A.	Interzone

NEW QUESTION 173
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 176
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 180
In which section of the PAN-OS GUI does an administrator configure URL Filtering profiles?

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

Answer: C

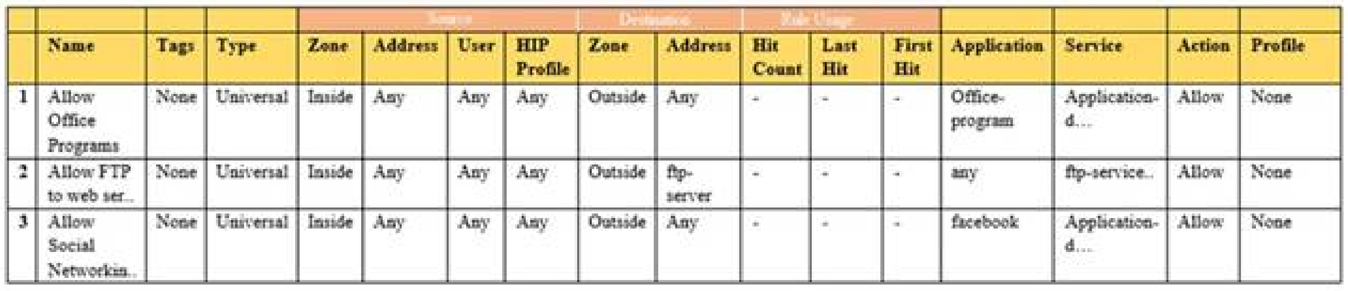
Explanation:
An administrator can configure URL Filtering profiles in the Objects section of the PAN-OS GUI. A URL Filtering profile is a collection of URL filtering controls that you can apply to individual Security policy rules that allow access to the internet1. You can set site access for URL categories, 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 185
Which path is used to save and load a configuration with a Palo Alto Networks firewall?

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

Answer: C

NEW QUESTION 187
Given the image, which two options are true about the Security policy rules. (Choose two.)



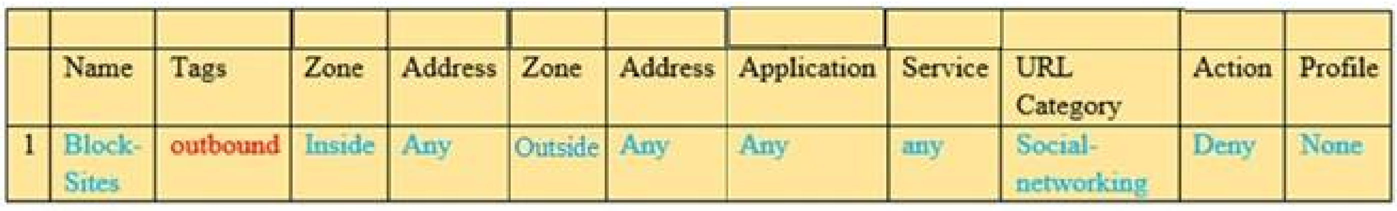
				Source				Destination		Rule Usage						
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Hit Count	Last Hit	First Hit	Application	Service	Action	Profile
1	Allow Office Programs	None	Universal	Inside	Any	Any	Any	Outside	Any	-	-	-	Office-program	Application-d...	Allow	None
2	Allow FTP to web ser..	None	Universal	Inside	Any	Any	Any	Outside	ftp-server	-	-	-	any	ftp-service..	Allow	None
3	Allow Social Networkin..	None	Universal	Inside	Any	Any	Any	Outside	Any	-	-	-	facebook	Application-d...	Allow	None

The Allow Office Programs rule is using an Application Filter
A.
B: In the Allow FTP to web server rule, FTP is allowed using App-ID
C. The Allow Office Programs rule is using an Application Group
D. In the Allow Social Networking rule, allows all of Facebook’s functions

Answer: AD

Explanation:
In the Allow FTP to web server rule, FTP is allowed using port based rule and not APP-ID.

NEW QUESTION 189
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 192
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 194
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 199
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 203
Which objects would be useful for combining several services that are often defined together?

A. shared service objects
B. service groups
C. application groups
D. application filters

Answer: B

Explanation:

Reference:
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface-help/objects/objects- services.html

NEW QUESTION 208
What are three Palo Alto Networks best practices when implementing the DNS Security Service? (Choose three.)

A. Implement a threat intel program.
B. Configure a URL Filtering profile.
C. Train your staff to be security aware.
D. Rely on a DNS resolver.
E. Plan for mobile-employee risk

Answer: ABD

NEW QUESTION 210
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 212
To what must an interface be assigned before it can process traffic?

A. Security Zone
B. Security policy
C. Security Protection
D. Security profile

Answer: A

NEW QUESTION 217
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 222
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

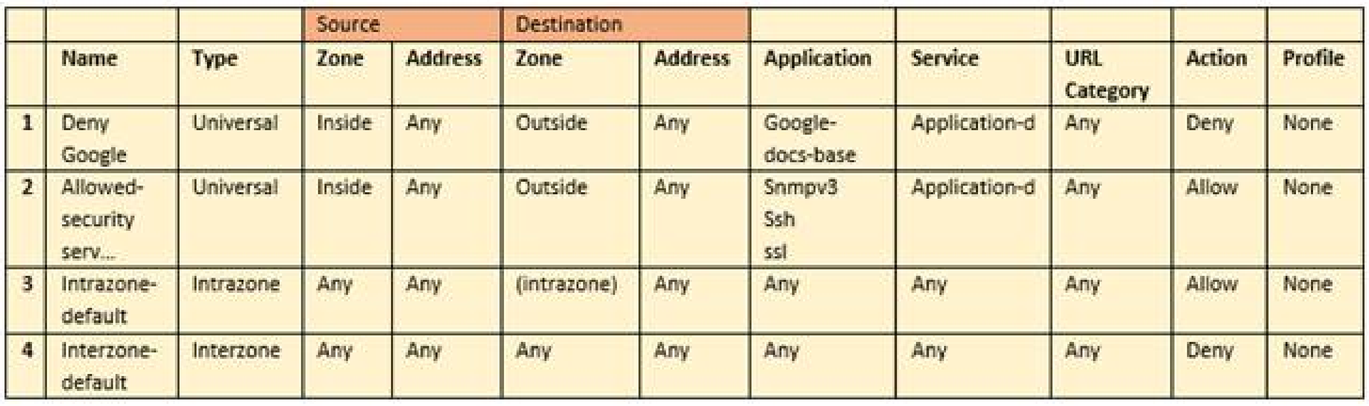
Explanation:
The user will see a response page indicating that a password is required to allow access to websites in the given category. With this option, the security administrator or help-desk person would provide a password granting temporary access to all websites in the given category. A log entry 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 225
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 226
The firewall sends employees an application block page when they try to access Youtube. Which Security policy rule is blocking the youtube application?



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

A. intrazone-default
B. Deny Google
C. allowed-security services
D. interzone-default

Answer: D

NEW QUESTION 229
Which statement best describes a common use of Policy Optimizer?

A. Policy Optimizer on a VM-50 firewall can display which Layer 7 App-ID Security policies have unused applications.
B. Policy Optimizer can add or change a Log Forwarding profile for each Security policy selected.

C. Policy Optimizer can display which Security policies have not been used in the last 90 days.
D. Policy Optimizer can be used on a schedule to automatically create a disabled Layer 7 App-ID Security policy for every Layer 4 policy that exist
E. Admins can then manually enable policies they want to keep and delete ones they want to remove.

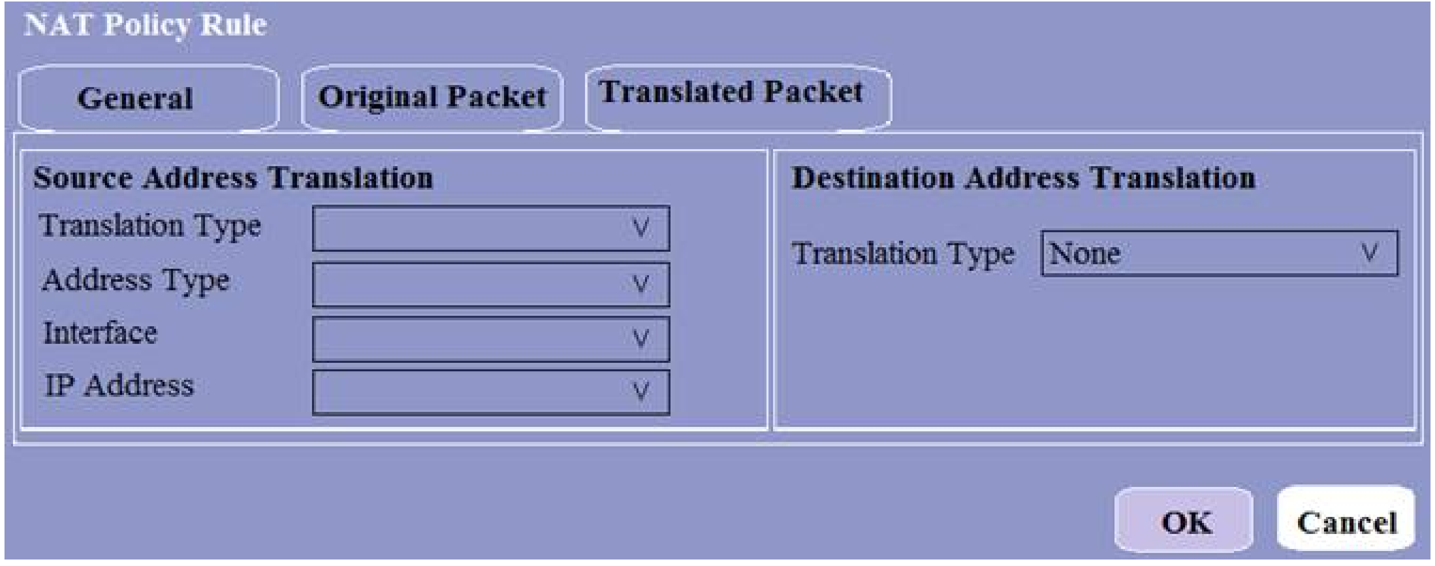
Answer: C

NEW QUESTION 232
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 235
When creating a Source NAT policy, which entry in the Translated Packet tab will display the options Dynamic IP and Port, Dynamic, Static IP, and None?



A. Translation Type
B. Interface
C. Address Type
D. IP Address

Answer: A

NEW QUESTION 239
Why should a company have a File Blocking profile that is attached to a Security policy?

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

Answer: A

NEW QUESTION 241
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 246
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 251
A website is unexpectedly allowed due to miscategorization.
What are two ways to resolve this issue for a proper response? (Choose two.)

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

Answer: CD

NEW QUESTION 253
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 254
Where within the firewall GUI can all existing tags be viewed?

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

Answer: C

NEW QUESTION 256
Which rule type is appropriate for matching traffic occurring within a specified zone?

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

Answer: C

NEW QUESTION 260
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 262
Which component is a building block in a Security policy rule?

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

Answer: D

Explanation:

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

NEW QUESTION 264
An administrator is configuring a NAT rule
At a minimum, which three forms of information are required? (Choose three.)

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

Answer: BDE

NEW QUESTION 265
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 270
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 274
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 276
An administrator is trying to enforce policy on some (but not all) of the entries in an external dynamic list. What is the maximum number of entries that they can be exclude?

A. 50
B. 100
C. 200
D. 1,000

Answer: B

NEW QUESTION 279
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 283
The NetSec Manager asked to create a new firewall Local Administrator profile with customized privileges named NewAdmin. This new administrator has to authenticate without inserting any username or password to access the WebUI.
What steps should the administrator follow to create the New_Admin Administrator profile?
A.
* 1. Select the "Use only client certificate authentication" check box.
* 2. Set Role to Role Based.
* 3. Issue to the Client a Certificate with Common Name = NewAdmin
B.
* 1. Select the "Use only client certificate authentication" check box.
* 2. Set Role to Dynamic.
* 3. Issue to the Client a Certificate with Certificate Name = NewAdmin
C.
* 1. Set the Authentication profile to Local.
* 2. Select the "Use only client certificate authentication" check box.
* 3. Set Role to Role Based.
D.
* 1. Select the "Use only client certificate authentication" check box.
* 2. Set Role to Dynamic.
* 3. Issue to the Client a Certificate with Common Name = New Admin

A.

Answer: B

NEW QUESTION 288
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 289
Which three filter columns are available when setting up an Application Filter? (Choose three.)

A. Parent App
B. Category
C. Risk
D. Standard Ports
E. Subcategory

Answer: BCE

Explanation:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/objects/objects- application-filters

NEW QUESTION 291
Which two statements are true for the DNS security service introduced in PAN-OS version 10.0?

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

Answer: AB

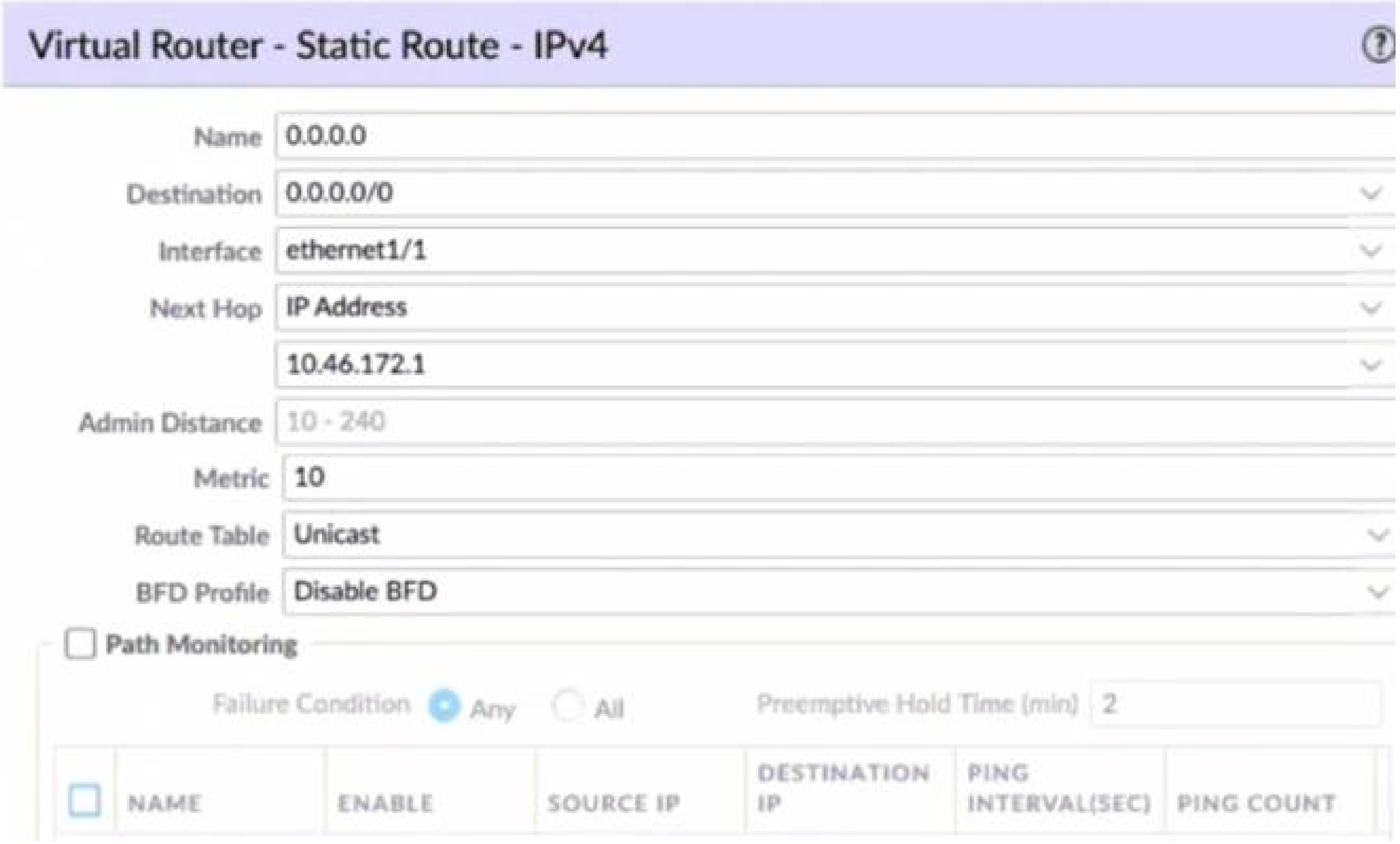
NEW QUESTION 296
In which stage of the Cyber-Attack Lifecycle would the attacker inject a PDF file within an email?

A. Weaponization
B. Reconnaissance
C. Installation
D. Command and Control
E. Exploitation

Answer: A

NEW QUESTION 301

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



Virtual Router - Static Route - IPv4

Name	0.0.0.0
Destination	0.0.0.0/0
Interface	ethernet1/1
Next Hop	IP Address
	10.46.172.1
Admin Distance	10 - 240
Metric	10
Route Table	Unicast
BFD Profile	Disable BFD

□ Path Monitoring

Failure Condition ● Any ○ All Preemptive Hold Time (min) 2

□	NAME	ENABLE	SOURCE IP	DESTINATION IP	PING INTERVAL(SEC)	PING COUNT

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

Answer: A

NEW QUESTION 302
Which interface type requires no routing or switching but applies Security or NAT policy rules before passing allowed traffic?

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

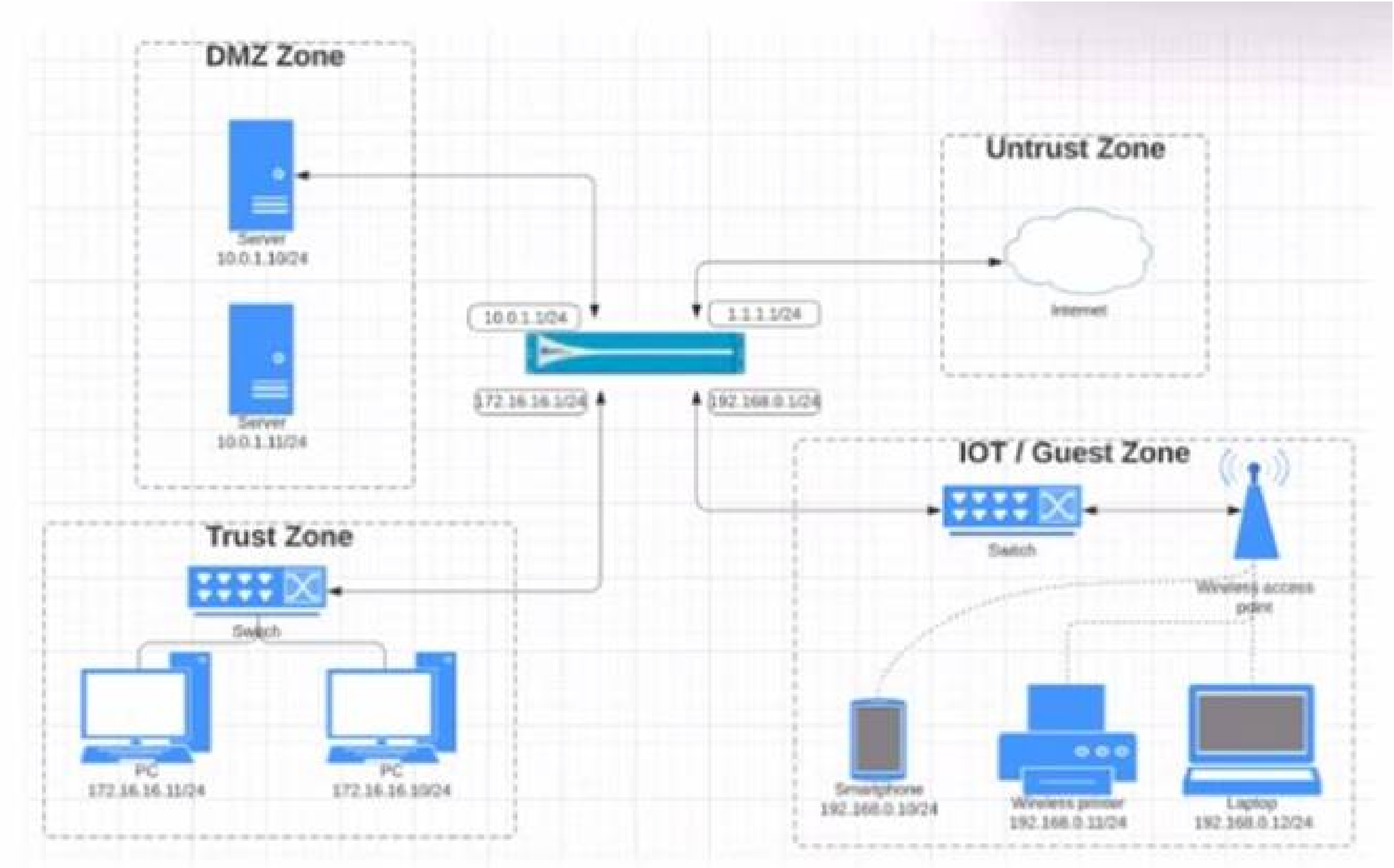
Answer: A

NEW QUESTION 304
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

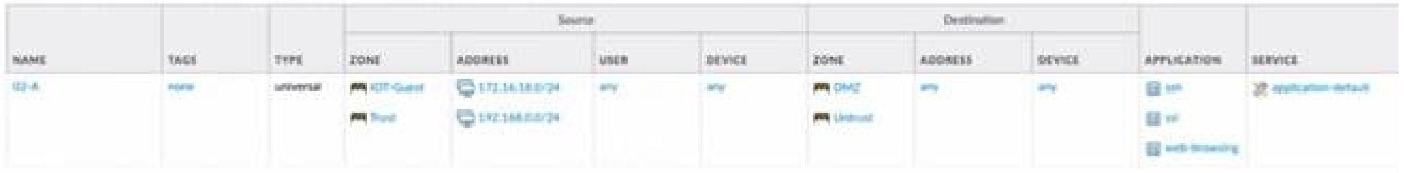
Answer: BD

NEW QUESTION 306
View the diagram.



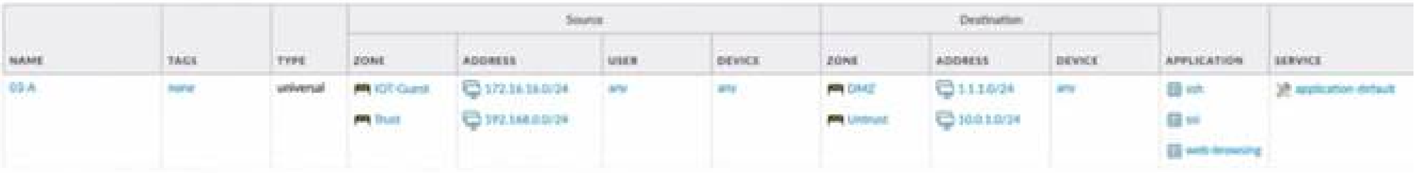
What is the most restrictive, yet fully functional rule, to allow general Internet and SSH traffic into both the DMZ and Untrust/lnternet zones from each of the lOT/Guest and Trust Zones?

A)



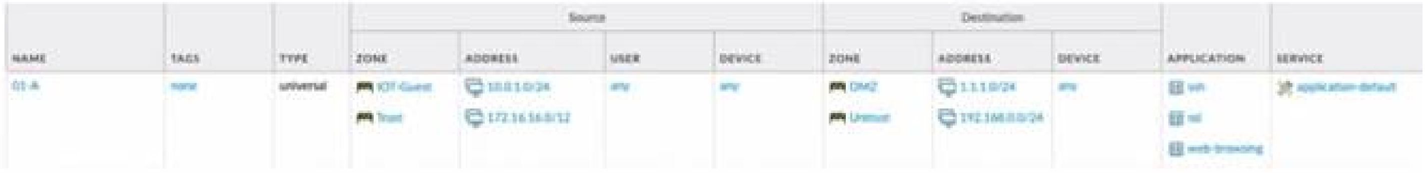
			Source				Destination				
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE
02-A	none	universal	IOT-Guest Trust	172.16.16.0/24 192.168.0.0/24	any	any	DMZ Untrust	any	any	ssh ssl web-browsing	application-default

B)



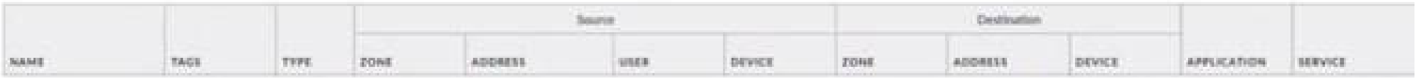
			Source				Destination				
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE
03-A	none	universal	IOT-Guest Trust	172.16.16.0/24 192.168.0.0/24	any	any	DMZ Untrust	1.1.1.0/24 10.0.1.0/24	any	ssh ssl web-browsing	application-default

C)



			Source				Destination				
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE
01-A	none	universal	IOT-Guest Trust	10.0.1.0/24 172.16.16.0/12	any	any	DMZ Untrust	1.1.1.0/24 192.168.0.0/24	any	ssh ssl web-browsing	application-default

D)



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

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

Answer: C

NEW QUESTION 308
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 309
In which profile should you configure the DNS Security feature?

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

Answer: B

Explanation:

Reference:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/threat-prevention/dns- security/enable- dnssecurity.html

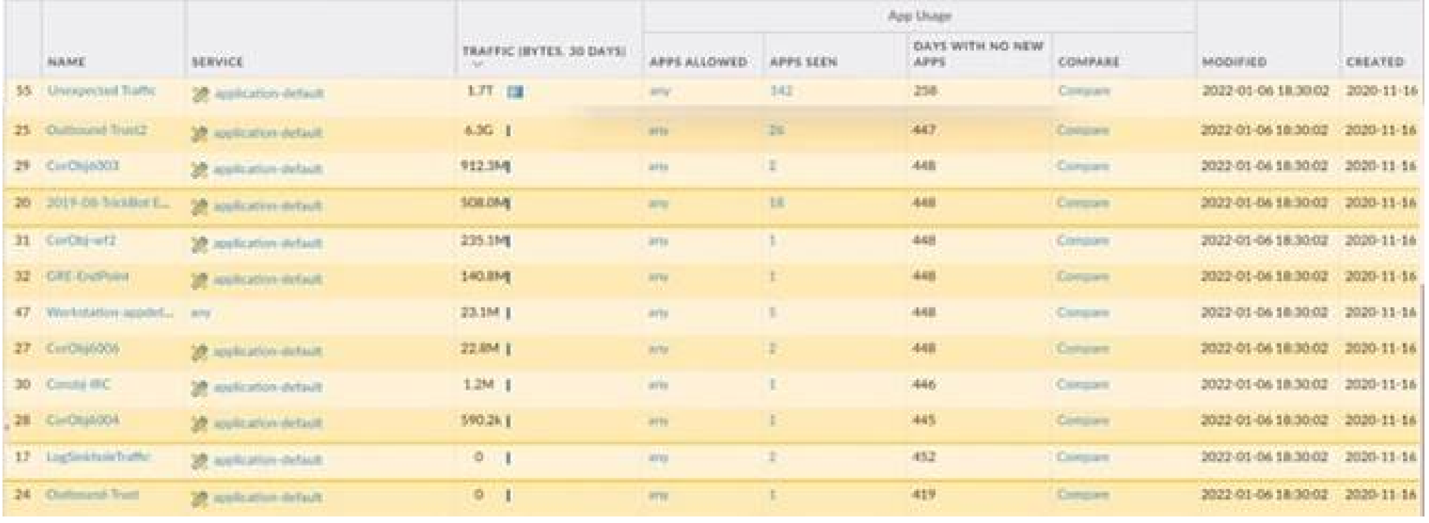
NEW QUESTION 311
An administrator would like to determine the default deny action for the application dns- over-https
Which action would yield the information?

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 316
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 318
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 319
An administrator is reviewing another administrator s Security policy log settings Which log setting configuration is consistent with best practices tor normal traffic?

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

Answer: B

NEW QUESTION 321
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 325

......

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

PCNSA Practice Exam Features:

* PCNSA Questions and Answers Updated Frequently

* PCNSA Practice Questions Verified by Expert Senior Certified Staff

* PCNSA Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* PCNSA Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The PCNSA Practice Test Here