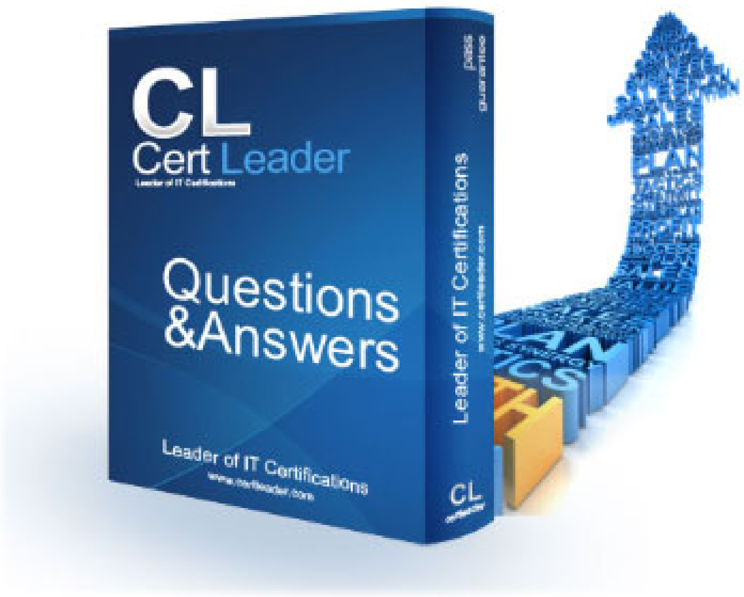
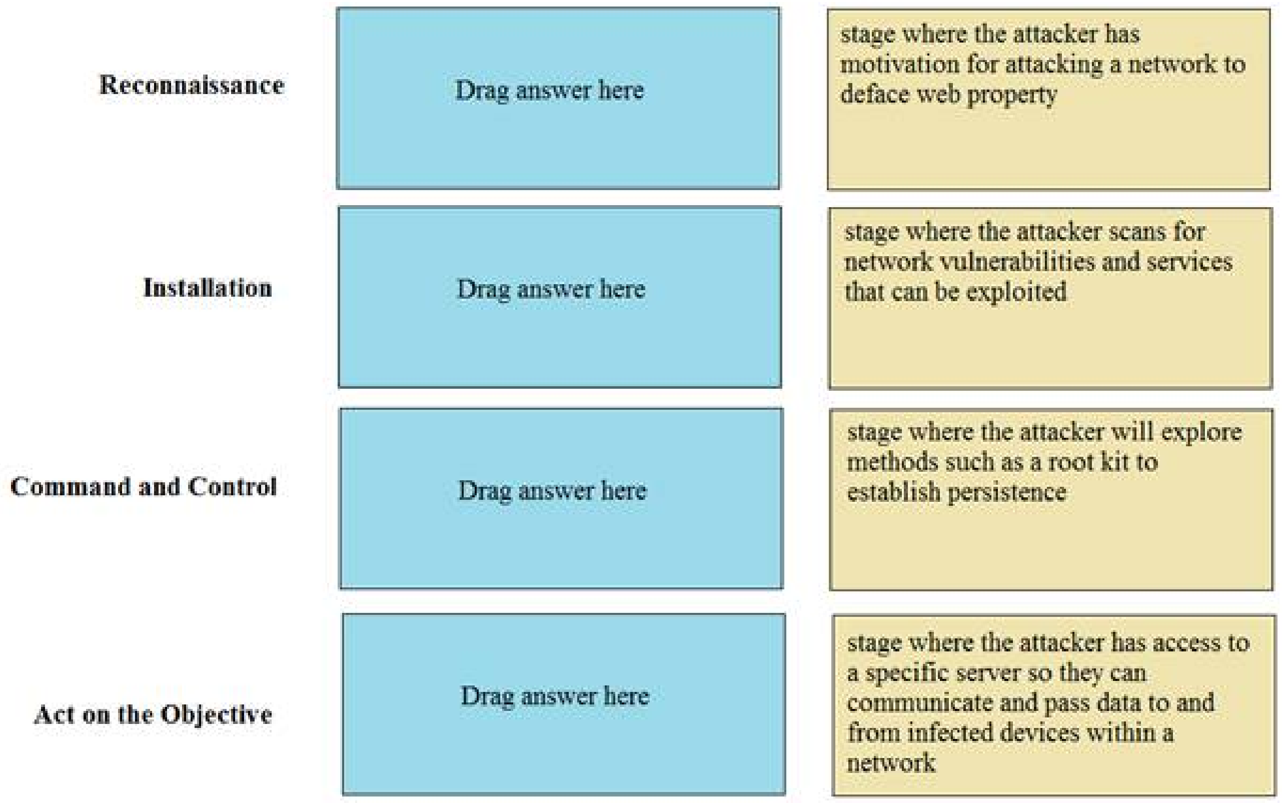
PCNSA Dumps

Palo Alto Networks Certified Network Security Administrator

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



NEW QUESTION 1
DRAG DROP
Match the Cyber-Attack Lifecycle stage to its correct description.



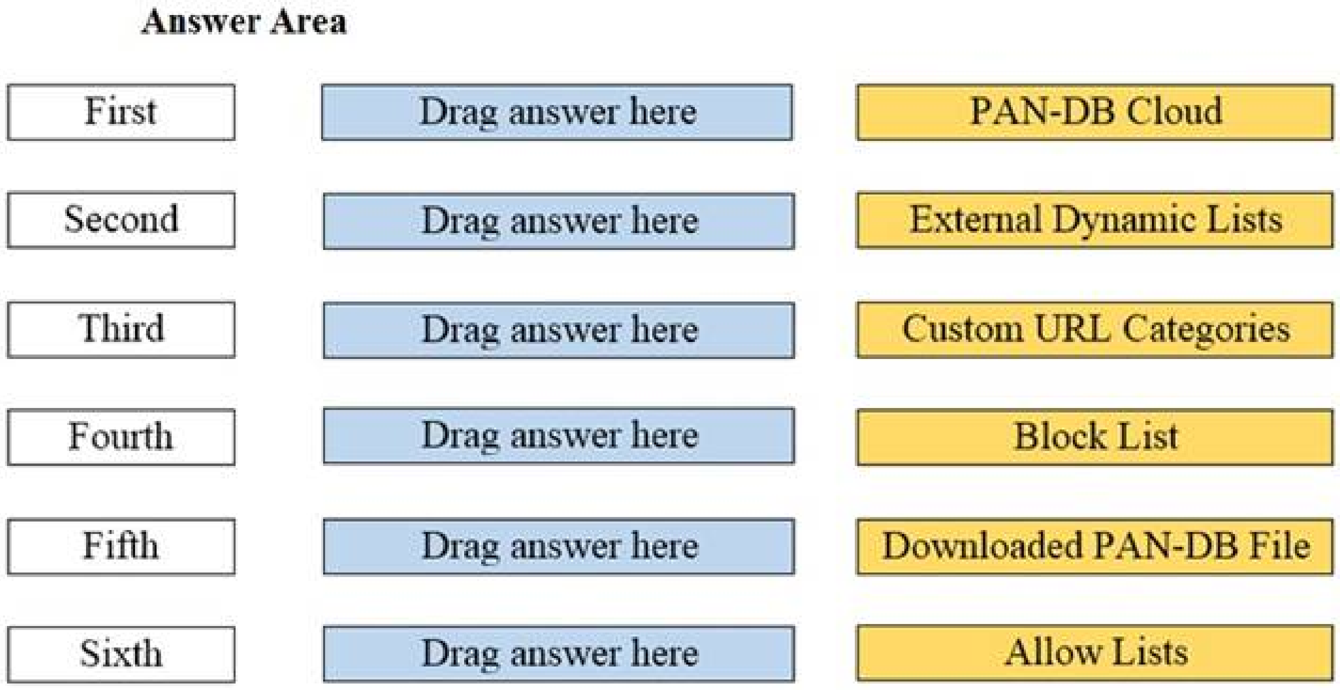
Reconnaissance	Drag answer here	stage where the attacker has motivation for attacking a network to deface web property
Installation	Drag answer here	stage where the attacker scans for network vulnerabilities and services that can be exploited
Command and Control	Drag answer here	stage where the attacker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

A. Mastered
B. Not Mastered

Answer: A

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

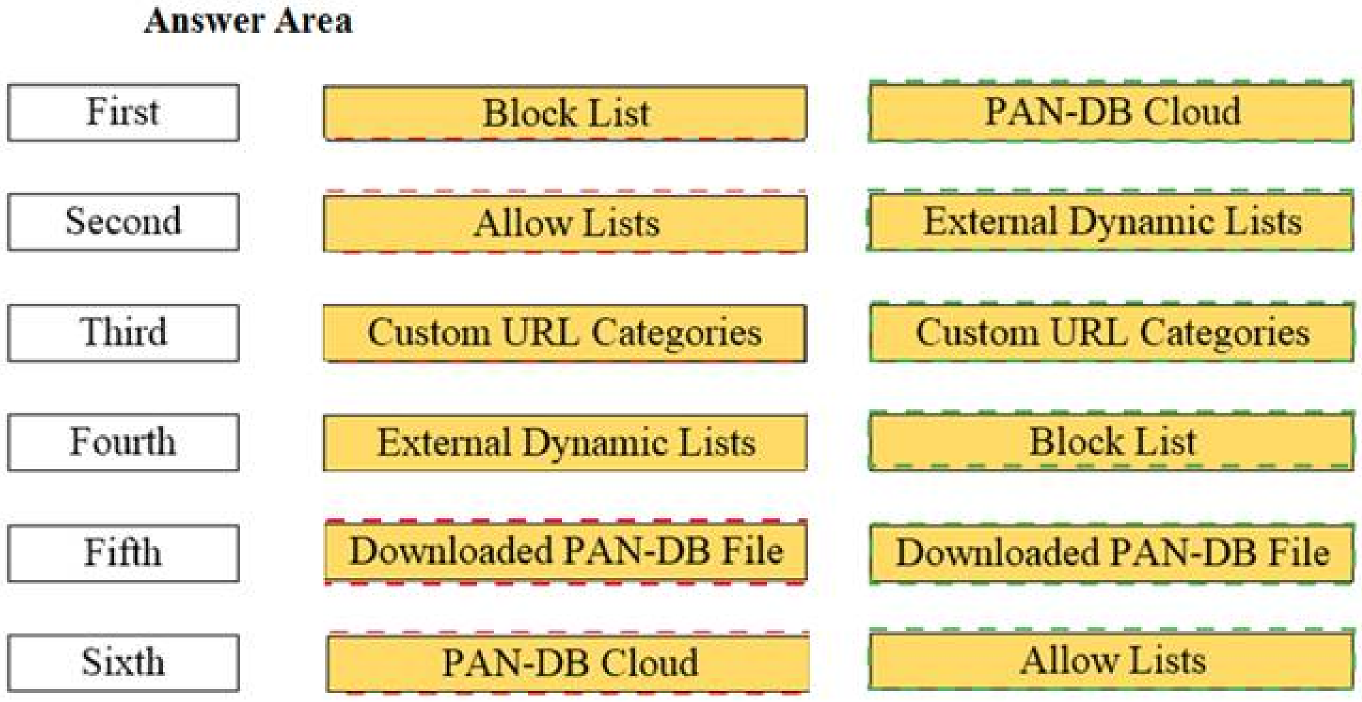
NEW QUESTION 2
DRAG DROP
Arrange the correct order that the URL classifications are processed within the system.



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

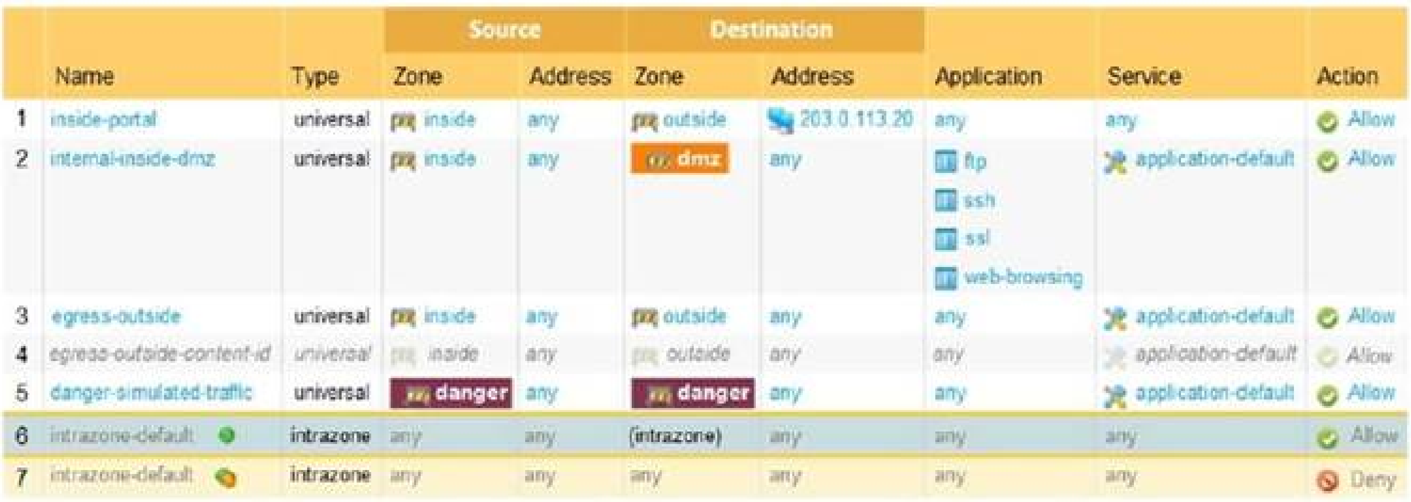
First	Block List	PAN-DB Cloud
Second	Allow Lists	External Dynamic Lists
Third	Custom URL Categories	Custom URL Categories
Fourth	External Dynamic Lists	Block List
Fifth	Downloaded PAN-DB File	Downloaded PAN-DB File
Sixth	PAN-DB Cloud	Allow Lists

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 3
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 4
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 5
When HTTPS for management and GlobalProtect are enabled on the same interface, which TCP port is used for management access?

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 6
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 7
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 8
What two authentication methods on the Palo Alto Networks firewalls support authentication and authorization for role-based access control? (Choose two.)

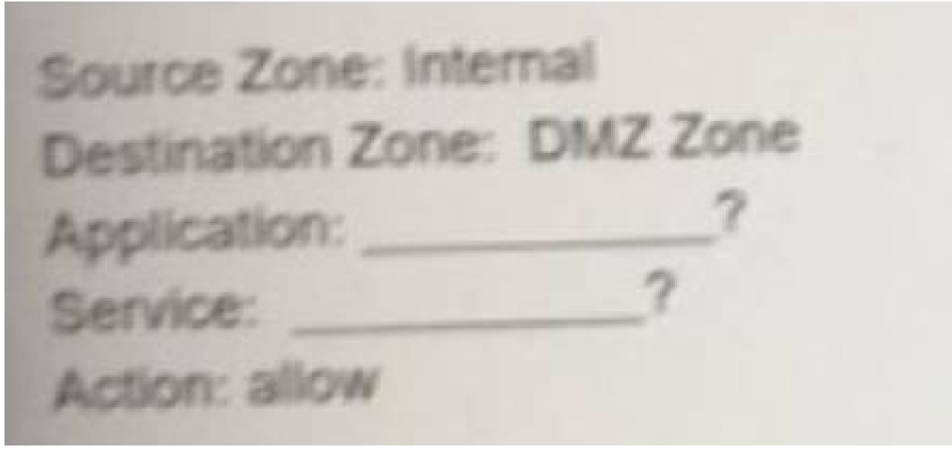
A. SAML
B. TACACS+
C. LDAP
D. Kerberos

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 9
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 10

Which built-in IP address EDL would be useful for preventing traffic from IP addresses that are verified as unsafe based on WildFire analysis Unit 42 research and data gathered from telemetry?

A.

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

Answer: D

Explanation:
? Palo Alto Networks Known Malicious IP Addresses
—Contains IP addresses that are verified malicious based on WildFire analysis, Unit 42 research, and data gathered from telemetry (Share ThreatIntelligence with Palo Alto Networks). Attackers use these IP addresses almost exclusively to distribute malware, initiate command-and-control activity, and launch attacks.
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/policy/use-an-external-dynamic-list-in-policy/built-in-edls

NEW QUESTION 10
You need to allow users to access the office–suite application of their choice. How should you configure the firewall to allow access to any office-suite application?

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

Answer: C

NEW QUESTION 11
Which dynamic update type includes updated anti-spyware signatures?

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

Answer: A

NEW QUESTION 14
The PowerBall Lottery has reached an unusually high value this week. Your company has decided to raise morale by allowing employees to access the PowerBall Lottery website (www.powerball.com) for just this week. However, the company does not want employees to access any other websites also listed in the URL filtering “gambling” category.
Which method allows the employees to access the PowerBall Lottery website but without unblocking access to the “gambling” URL category?

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

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

Answer: CD

NEW QUESTION 19
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 20
At which point in the app-ID update process can you determine if an existing policy rule is affected by an app-ID update?

A.

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

Answer: A

Explanation:
Reference:https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/device/device-dynamicupdates

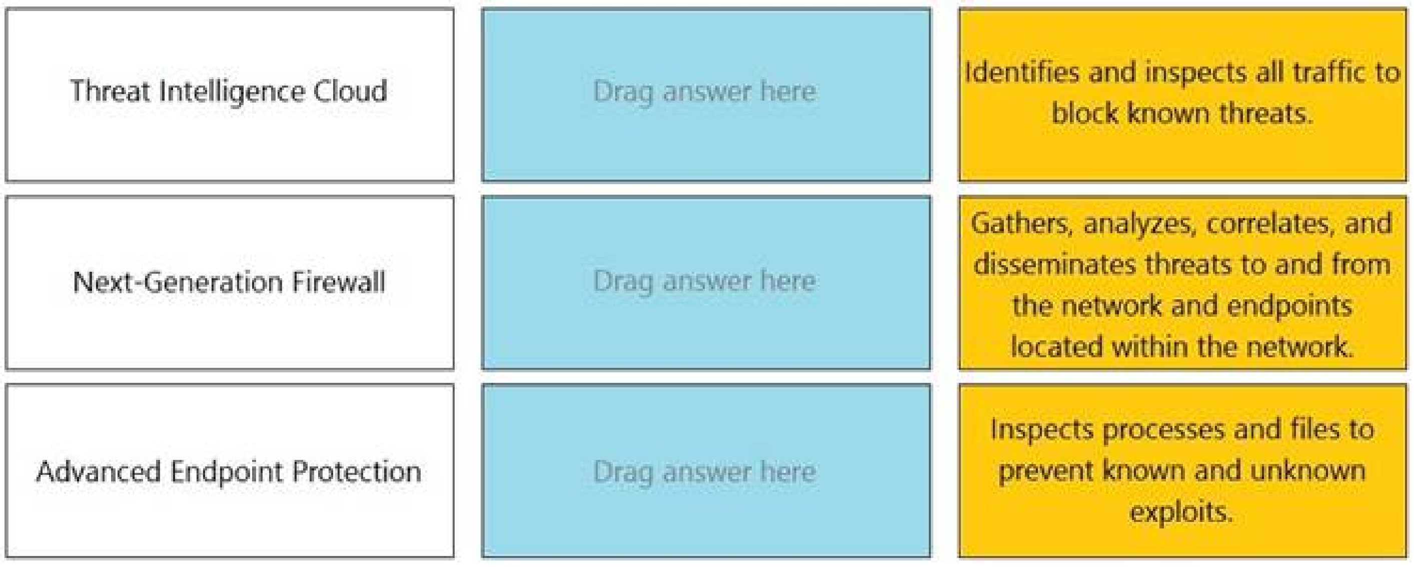
NEW QUESTION 24
Which feature would be useful for preventing traffic from hosting providers that place few restrictions on content, whose services are frequently used by attackers to distribute illegal or unethical material?

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 26
DRAG DROP
Match each feature to the DoS Protection Policy or the DoS Protection Profile.

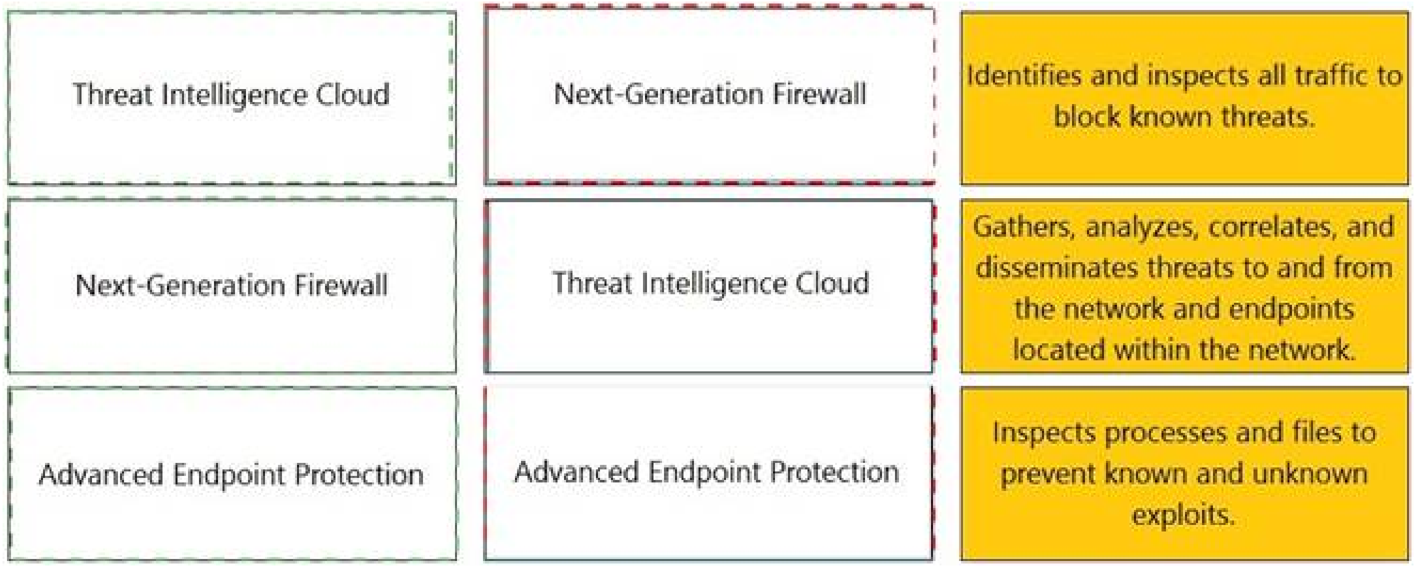


Threat Intelligence Cloud	Drag answer here	Identifies and inspects all traffic to block known threats.
Next-Generation Firewall	Drag answer here	Gathers, analyzes, correlates, and disseminates threats to and from the network and endpoints located within the network.
Advanced Endpoint Protection	Drag 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 29
In a security policy what is the quickest way to rest all policy rule hit counters to zero?

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

Answer: C

NEW QUESTION 34
Which solution is a viable option to capture user identification when Active Directory is not in use?

A. Cloud Identity Engine
B. group mapping
C. Directory Sync Service
D. Authentication Portal

Answer: D

NEW QUESTION 37
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 40
Which three statement describe the operation of Security Policy rules or Security Profiles? (Choose three)

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

Answer: BCE

NEW QUESTION 43
What is the minimum timeframe that can be set on the firewall to check for new WildFire signatures?

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

Answer: D

NEW QUESTION 48
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 51
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 53
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 55

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 58
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.

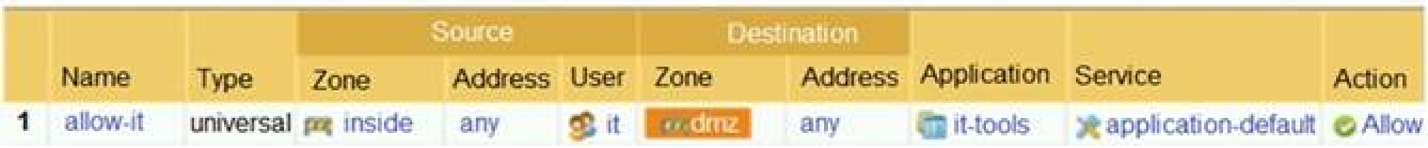
Answer: C

NEW QUESTION 63
An administrator wants to prevent access to media content websites that are risky
Which two URL categories should be combined in a custom URL category to accomplish this goal? (Choose two)

A. Mastered
B. Not Mastered

Answer: A

NEW QUESTION 65
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 66
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 67
What do dynamic user groups you to do?

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

Answer: C

Explanation:

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/user-id- features/dynamic-user-groups#:~:text=Dynamic%20user%20groups%20help%20you,activity%20while%20maintai ning%20user%20visibility.

NEW QUESTION 72
The Palo Alto Networks NGFW was configured with a single virtual router named VR-1 What changes are required on VR-1 to route traffic between two interfaces on the NGFW?

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

Answer: D

Explanation:

NEW QUESTION 76
What action will inform end users when their access to Internet content is being restricted?

Create a custom 'URL Category' object with notifications enabled.
A.
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 80
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 85
What are three valid information sources that can be used when tagging users to dynamic user groups? (Choose three.)

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

Answer: BCE

NEW QUESTION 89
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 94
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 97
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 102
Which Security profile must be added to Security policies to enable DNS Signatures to be checked?

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

Answer: D

NEW QUESTION 103
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 107
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 112
Which service protects cloud-based applications such as Dropbox and Salesforce by administering permissions and scanning files for sensitive information?

A. Aperture
B. AutoFocus
C. Parisma SaaS
D. GlobalProtect

Answer: C

NEW QUESTION 117
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 120
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 122
An administrator needs to allow users to use their own office applications. How should the administrator configure the firewall to allow multiple applications in a dynamic environment?

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 123
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.

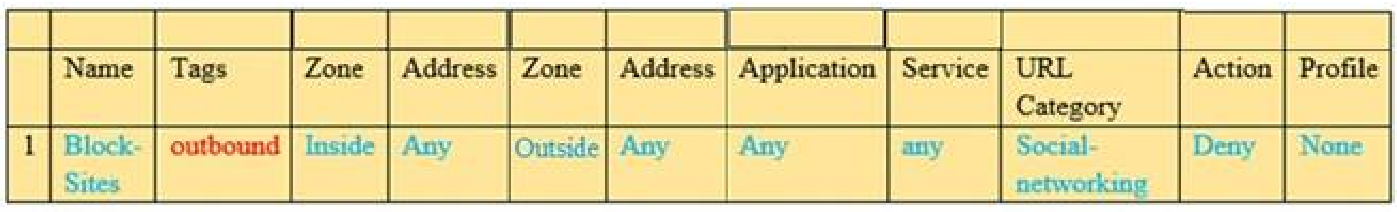
NEW QUESTION 125
Which User-ID agent would be appropriate in a network with multiple WAN links, limited network bandwidth, and limited firewall management plane resources?

A. Windows-based agent deployed on the internal network
B. PAN-OS integrated agent deployed on the internal network
C. Citrix terminal server deployed on the internal network
D. Windows-based agent deployed on each of the WAN Links

Answer: A

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

NEW QUESTION 129
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 131
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 135
What is the purpose of the automated commit recovery feature?

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

Answer: C

Explanation:
Reference:https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/administer-panorama/enable-automated-commit-recovery.html

NEW QUESTION 136
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 140
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 145
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

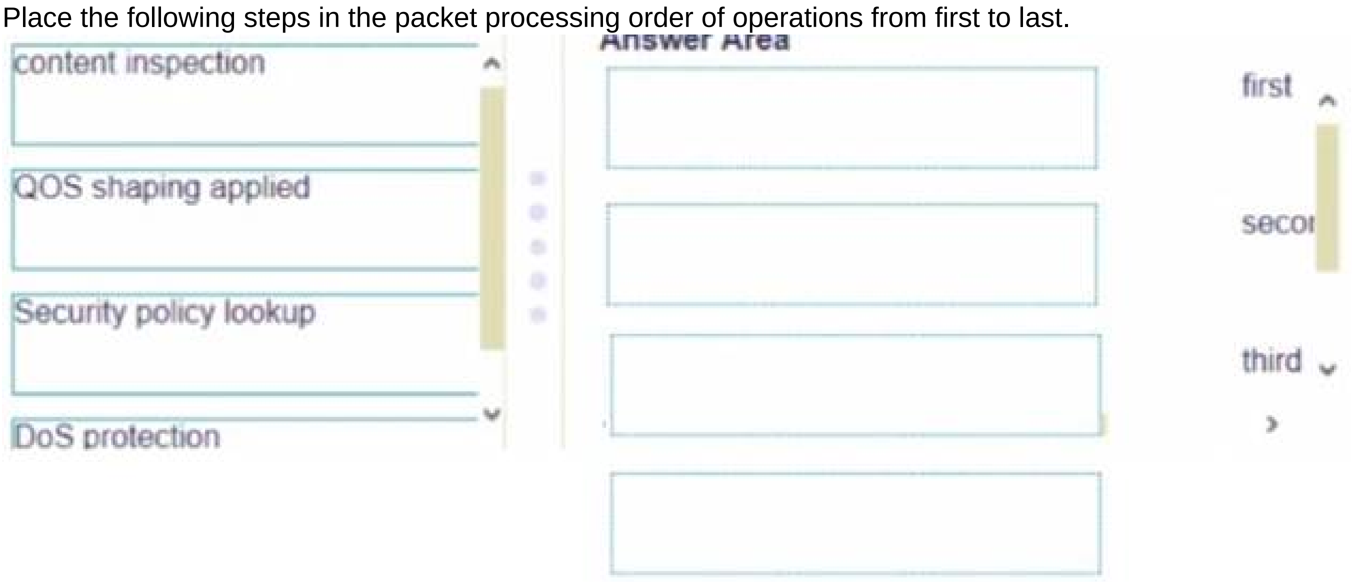
NEW QUESTION 150

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

A. vulnerability protection profile applied to outbound security policies
B. anti-spyware profile applied to outbound security policies
C. antivirus profile applied to outbound security policies
D. URL filtering profile applied to outbound security policies

Answer: BD

NEW QUESTION 152
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 154
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 159
Which statement is true regarding a Best Practice Assessment?

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

Answer: C

NEW QUESTION 163
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.

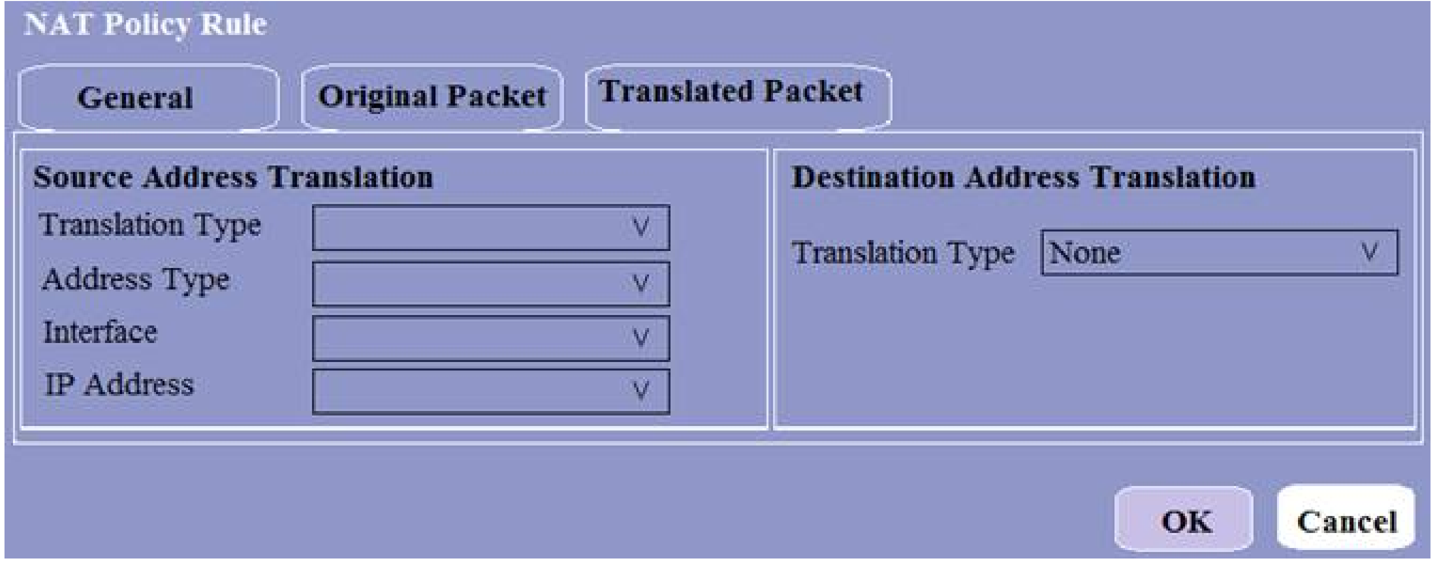
Answer: C

NEW QUESTION 168
An administrator is investigating a log entry for a session that is allowed and has the end reason of aged-out. Which two fields could help in determining if this is normal? (Choose
two.)

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

Answer: BD

NEW QUESTION 173
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?



NAT Policy Rule

Source Address Translation
Translation Type
Address Type
Interface
IP Address

Destination Address Translation
Translation Type: None

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

Answer: A

NEW QUESTION 174
A network administrator is required to use a dynamic routing protocol for network connectivity.
Which three dynamic routing protocols are supported by the NGFW Virtual Router for this purpose? (Choose three.)

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

Answer: ABE

NEW QUESTION 175
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 176
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 177
How often does WildFire release dynamic updates?

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

D. every 30 minutes

Answer: A

NEW QUESTION 181
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 185
When is the content inspection performed in the packet flow process?

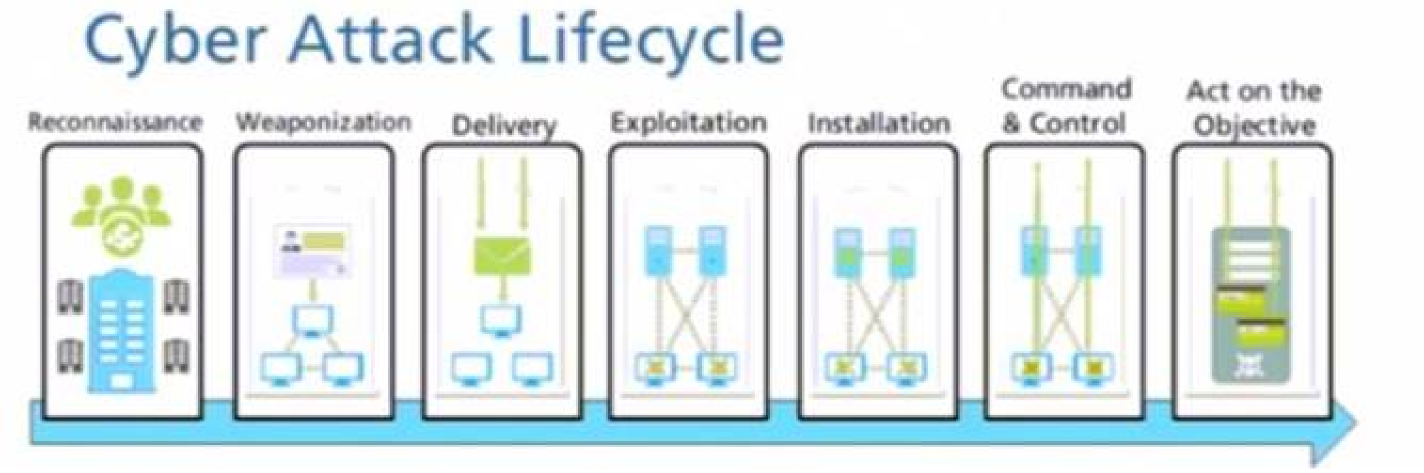
A. after the application has been identified
B. after the SSL Proxy re-encrypts the packet
C. before the packet forwarding process
D. before session lookup

Answer: A

Explanation:

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

NEW QUESTION 190
Given the cyber-attack lifecycle diagram identify the stage in which the attacker can run malicious code against a vulnerability in a targeted machine.



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

Answer: A

NEW QUESTION 191
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:

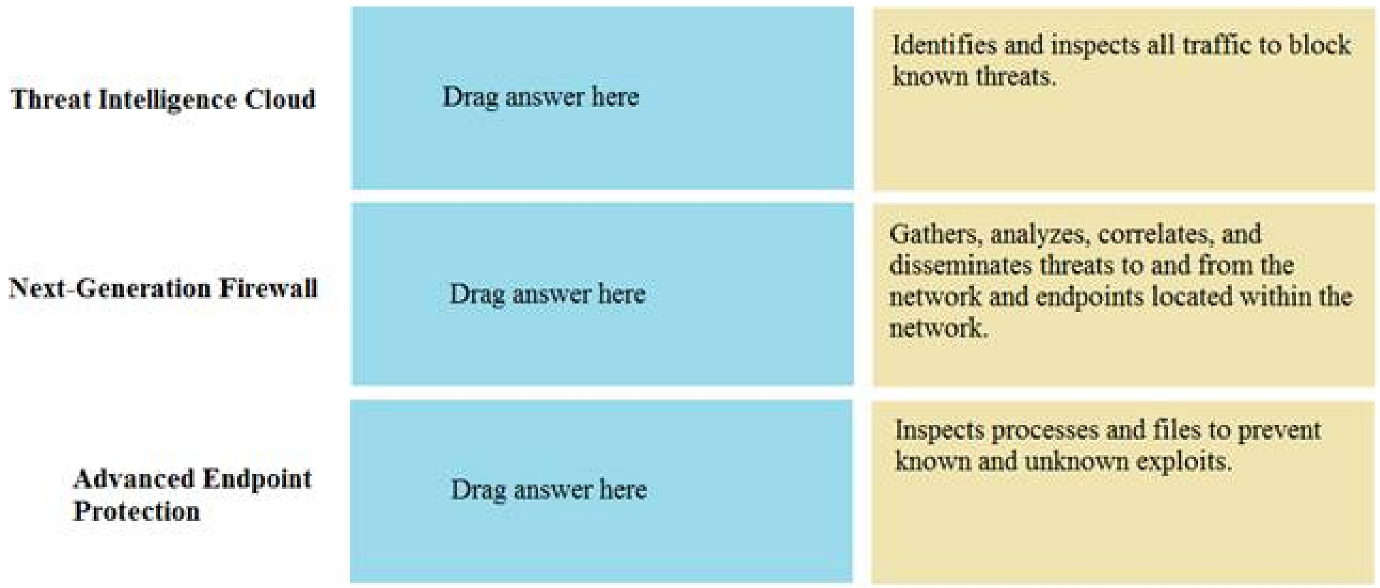
Reference:https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/url-filtering/url-filtering-concepts/url-category-as-policy-match-criteria.html

NEW QUESTION 194
What are the two default behaviors for the intrazone-default policy? (Choose two.)

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

Answer: AB

NEW QUESTION 197
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 199
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 200
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

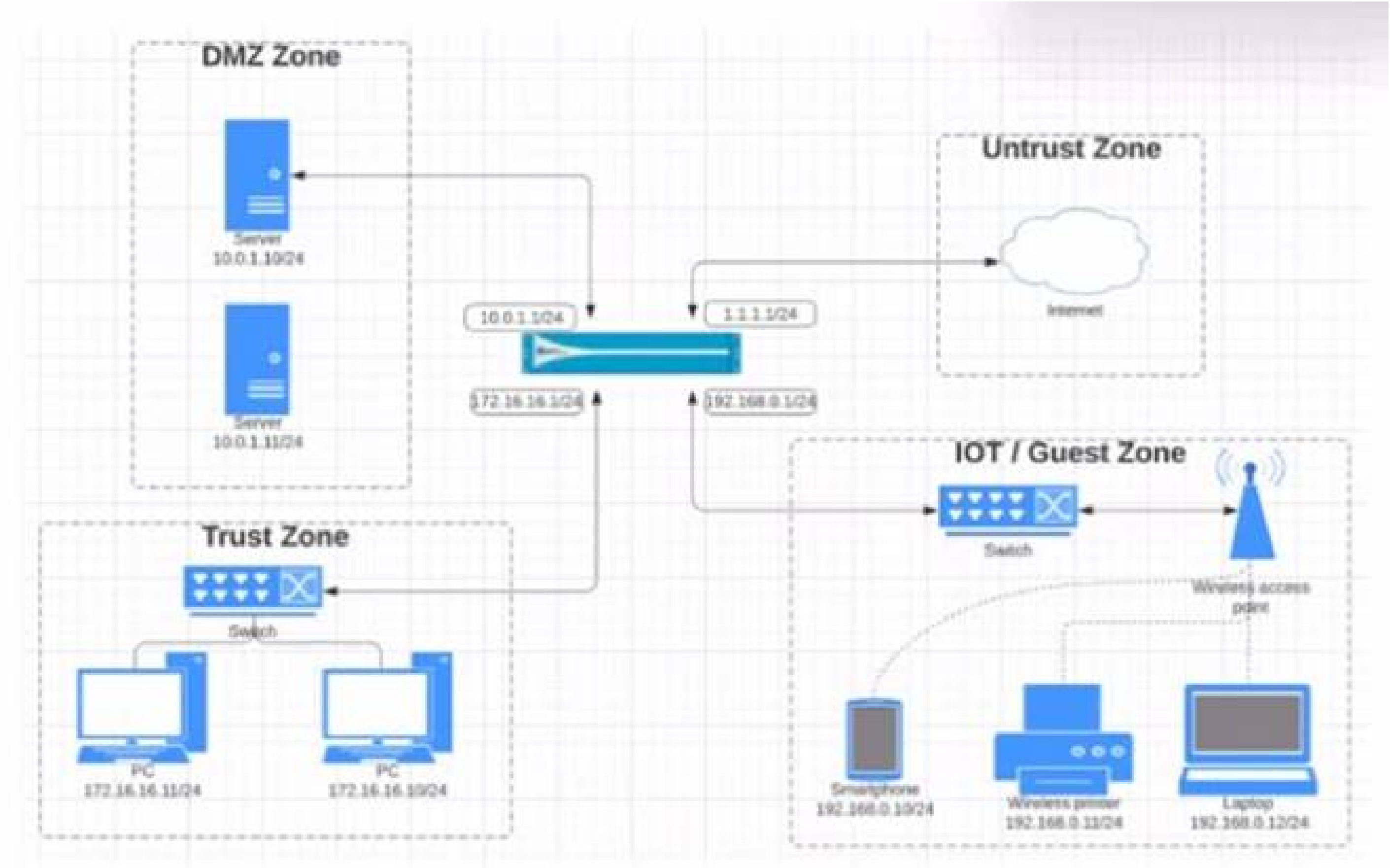
Answer: A

NEW QUESTION 201
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

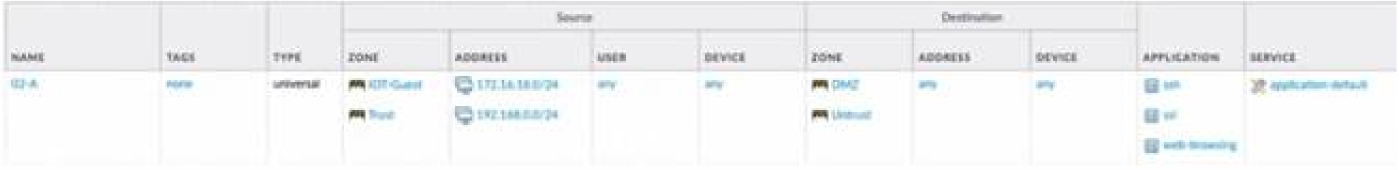
Answer: BD

NEW QUESTION 203
View the diagram.



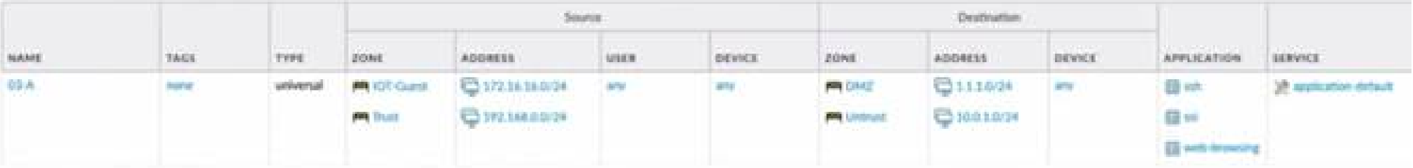
What is the most restrictive, yet fully functional rule, to allow general Internet and SSH traffic into both the DMZ and Untrust/lnternet zones from each of the IOT/Guest and Trust Zones?

A)



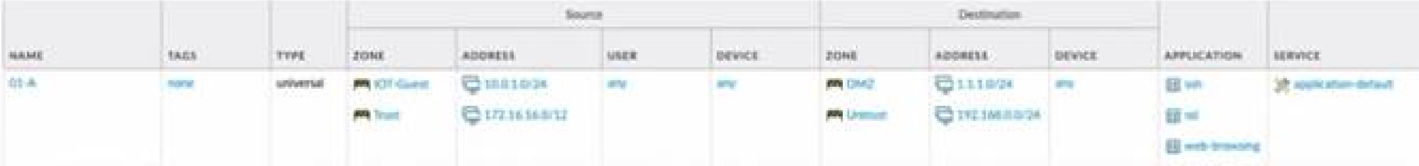
			Source				Destination				
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE
02-A	none	universal	IOT-Guest Trust	172.16.16.0/24 192.168.0.0/24	any	any	DMZ Untrust	any	any	ssh ssl web-browsing	application-default

B)



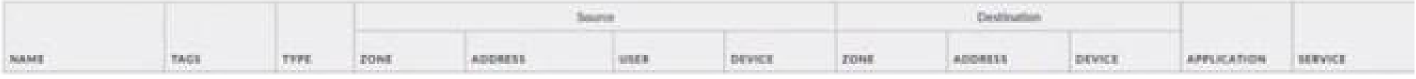
			Source				Destination				
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE
03-A	none	universal	IOT-Guest Trust	172.16.16.0/24 192.168.0.0/24	any	any	DMZ Untrust	1.1.1.0/24 10.0.1.0/24	any	ssh ssl web-browsing	application-default

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 205
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 209
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

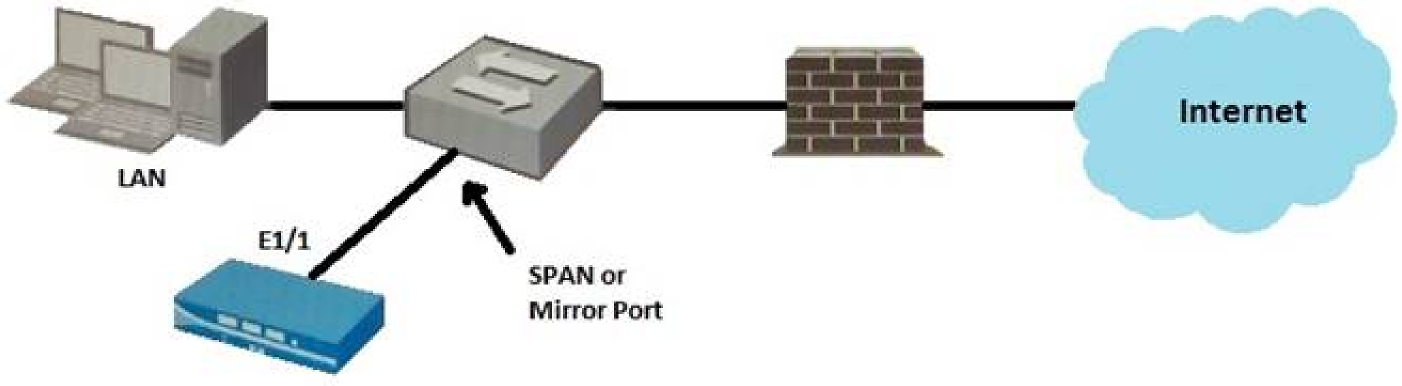
Answer: ACDEF

NEW QUESTION 213
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 215
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 218
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 221
......