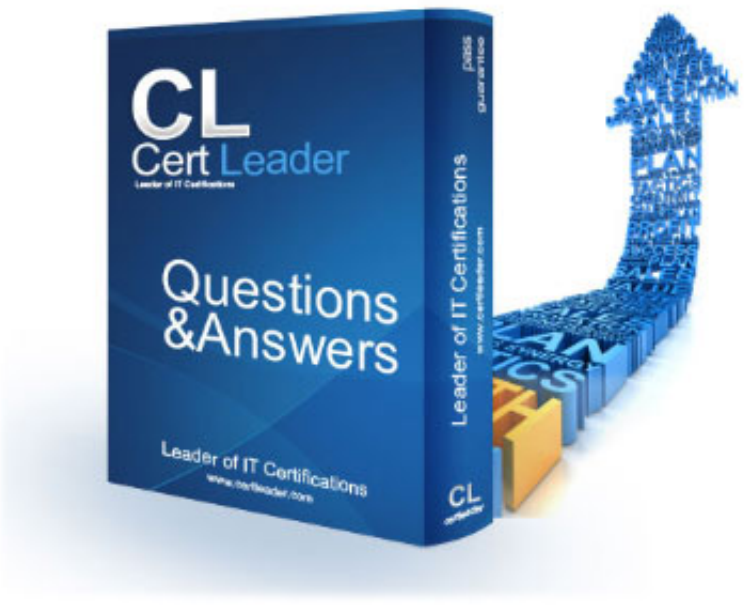
PCNSA Dumps

Palo Alto Networks Certified Network Security Administrator

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



NEW QUESTION 1
Which security policy rule would be needed to match traffic that passes between the Outside zone and Inside zone, but does not match traffic that passes within the zones?

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

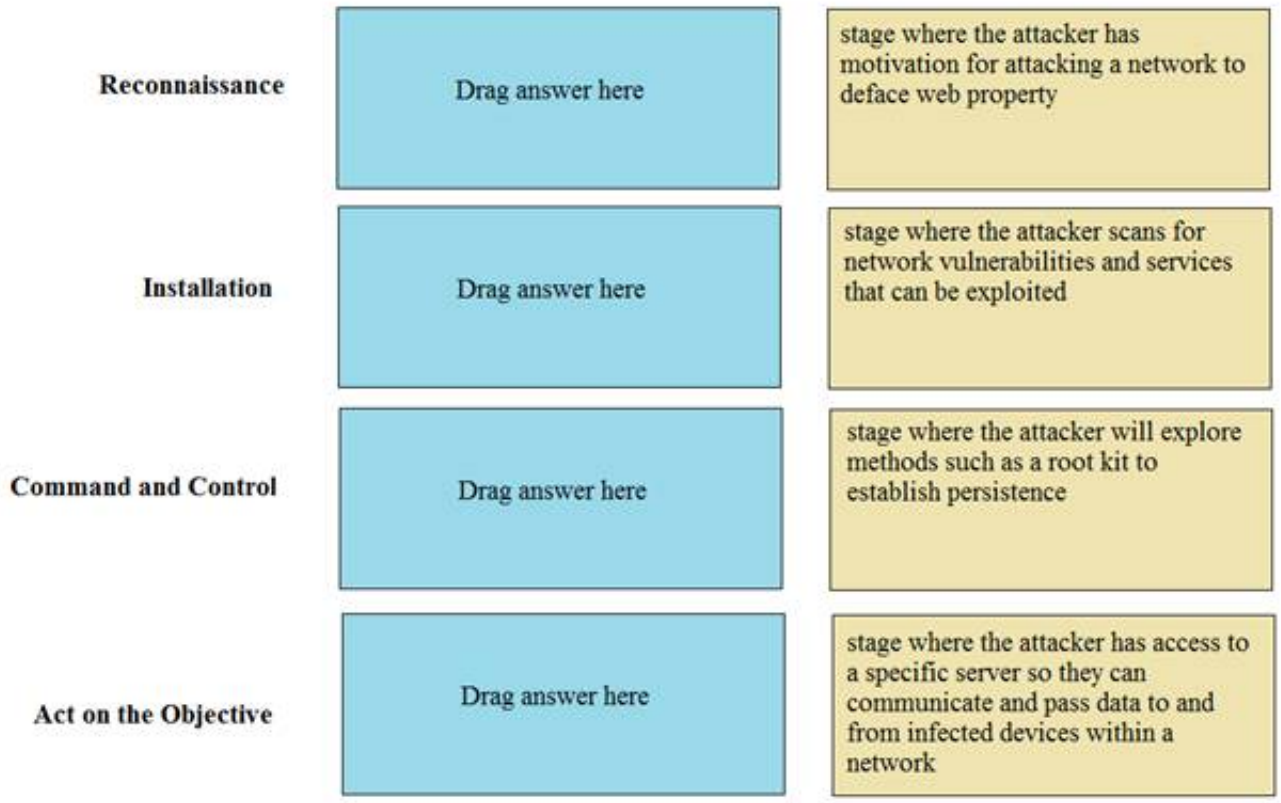
Answer: B

NEW QUESTION 2
Which operations are allowed when working with App-ID application tags?

A. Predefined tags may be deleted.
B. Predefined tags may be augmented by custom tags.
C. Predefined tags may be modified.
D. Predefined tags may be updated by WildFire dynamic updates.

Answer: B

NEW QUESTION 3
DRAG DROP
Match the Cyber-Attack Lifecycle stage to its correct description.



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

A. Mastered
B. Not Mastered

Answer: A

NEW QUESTION 5
Based on the screenshot presented which column contains the link that when clicked opens a window to display all applications matched to the policy rule?

A. Apps Allowed
B. Name
C. Apps Seen
D. Service

Answer: C

NEW QUESTION 6
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 7
What are two differences between an implicit dependency and an explicit dependency in App-ID? (Choose two.)

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

policy

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

Answer: AD

NEW QUESTION 8
Which statement best describes the use of Policy Optimizer?

A. Policy Optimizer can display which Security policies have not been used in the last 90 days
B. Policy Optimizer on a VM-50 firewall can display which Layer 7 App-ID Security policies have unused applications
C. Policy Optimizer can add or change a Log Forwarding profile for each Secunty policy selected
D. Policy Optimizer can be used on a schedule to automatically create a disabled Layer 7 App-ID Security policy for every Layer 4 policy that exists Admins can then manually enable policies they want to keep and delete ones they want to remove

Answer: B

NEW QUESTION 9
What is an advantage for using application tags?

A. They are helpful during the creation of new zones
B. They help with the design of IP address allocations in DHCP.

C. They help content updates automate policy updates
D. They help with the creation of interfaces

Answer: C

NEW QUESTION 10
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 10
How do you reset the hit count on a security policy rule?

A. First disable and then re-enable the rule.
B. Reboot the data-plane.
C. Select a Security policy rule, and then select Hit Count > Reset.
D. Type the CLI command reset hitcount <POLICY-NAME>.

Answer: C

NEW QUESTION 13
An administrator would like to use App-ID's deny action for an application and would like that action updated with dynamic updates as new content becomes available.
Which security policy action causes this?

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

Answer: C

Explanation:
Explanation/Reference: Reference:

https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/firewall- administration/manage- configuration backups/revert-firewall-configuration- changes.html

NEW QUESTION 15
Which data flow direction is protected in a zero trust firewall deployment that is not protected in a perimeter-only firewall deployment?

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

Answer: D

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

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

Answer: CD

NEW QUESTION 23
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 27
By default, which action is assigned to the interzone-default rule?

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

Answer: C

NEW QUESTION 29
Which file is used to save the running configuration with a Palo Alto Networks firewall?

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

Answer: A

NEW QUESTION 31
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 33
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 36
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 38
Which stage of the cyber-attack lifecycle makes it important to provide ongoing education to users on spear phishing links, unknown emails, and risky websites?

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

Answer: B

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

NEW QUESTION 42
Which interface type is used to monitor traffic and cannot be used to perform traffic shaping?

A. Mastered
B. Not Mastered

Answer: A

NEW QUESTION 46
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

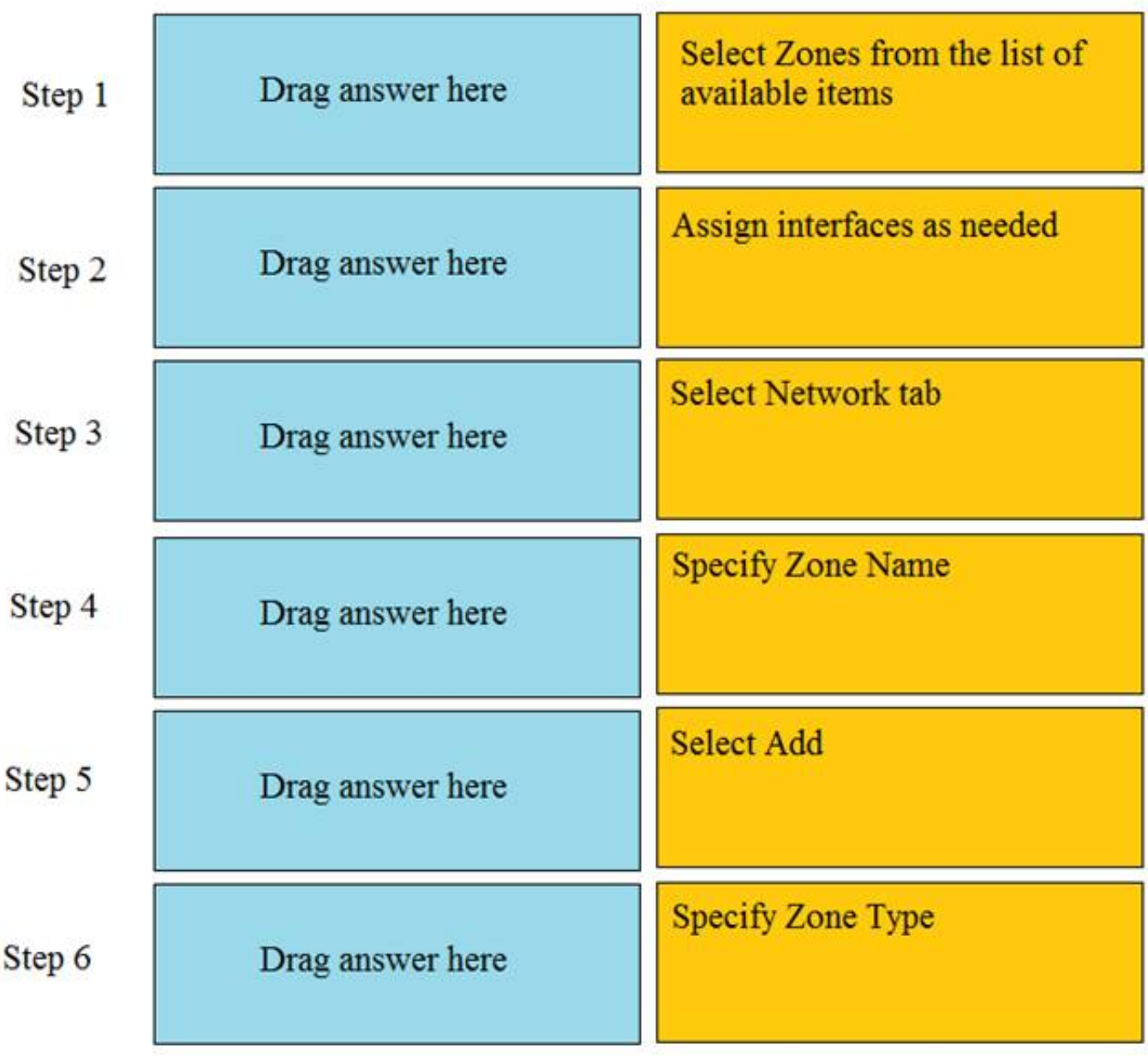
NEW QUESTION 48
Based on the security policy rules shown, ssh will be allowed on which port?

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

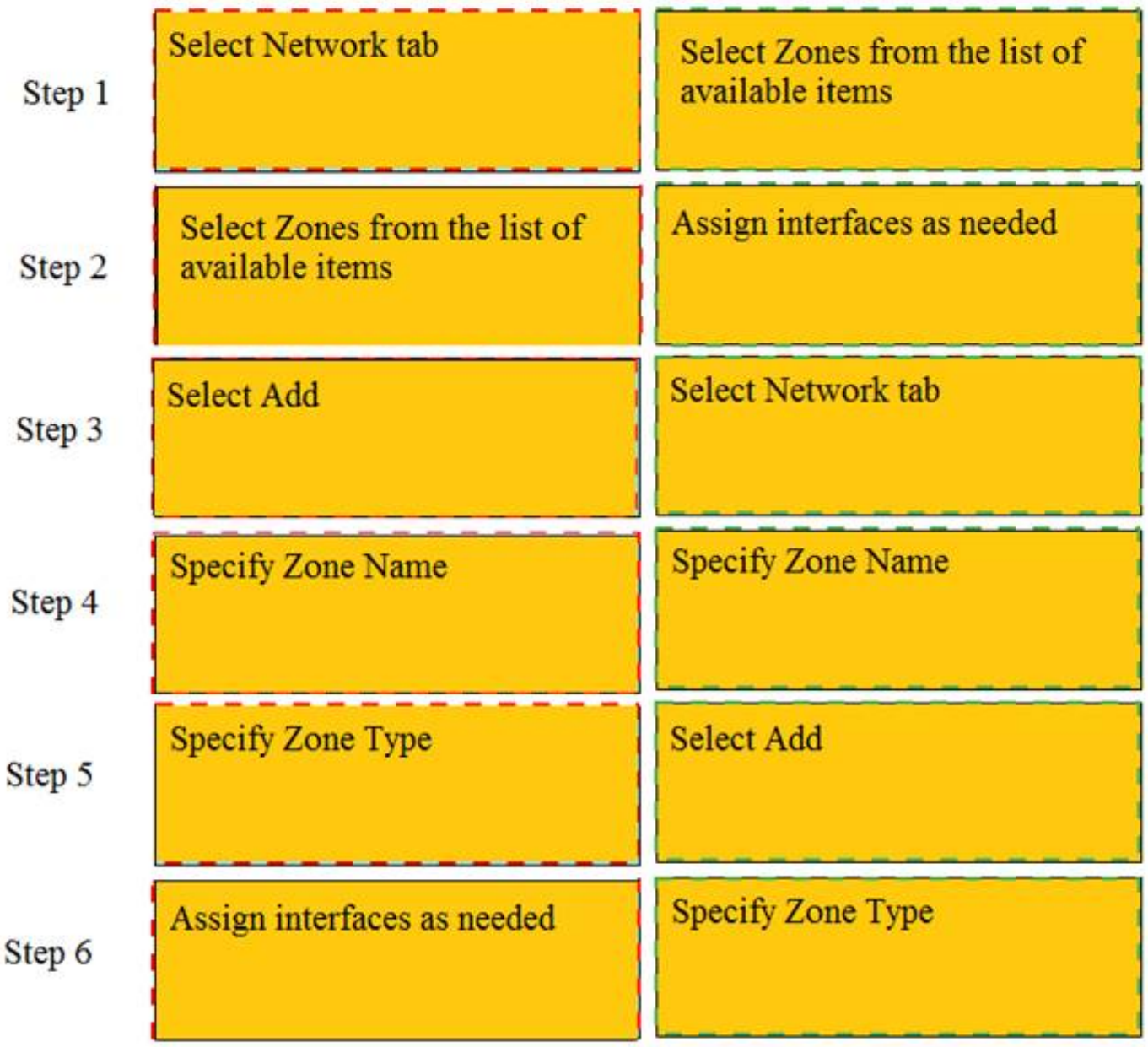
A. any port
B. same port as ssl and snmpv3
C. the default port
D. only ephemeral ports

Answer: C

NEW QUESTION 51
DRAG DROP
Order the steps needed to create a new security zone with a Palo Alto Networks firewall.



Answer:



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 56
Which DNS Query action is recommended for traffic that is allowed by Security policy and matches Palo Alto Networks Content DNS Signatures?

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

Answer: B

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

NEW QUESTION 58
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 62
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 64
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 66
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 69
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 72
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 73
You receive notification about new malware that infects hosts through malicious files transferred by FTP.
Which Security profile detects and protects your internal networks from this threat after you update your firewall's threat signature database?

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

Answer: C

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

NEW QUESTION 75
Which profile should be used to obtain a verdict regarding analyzed files?

A. WildFire analysis
B. Vulnerability profile
Content-ID
C. D: Advanced threat prevention

Answer: A

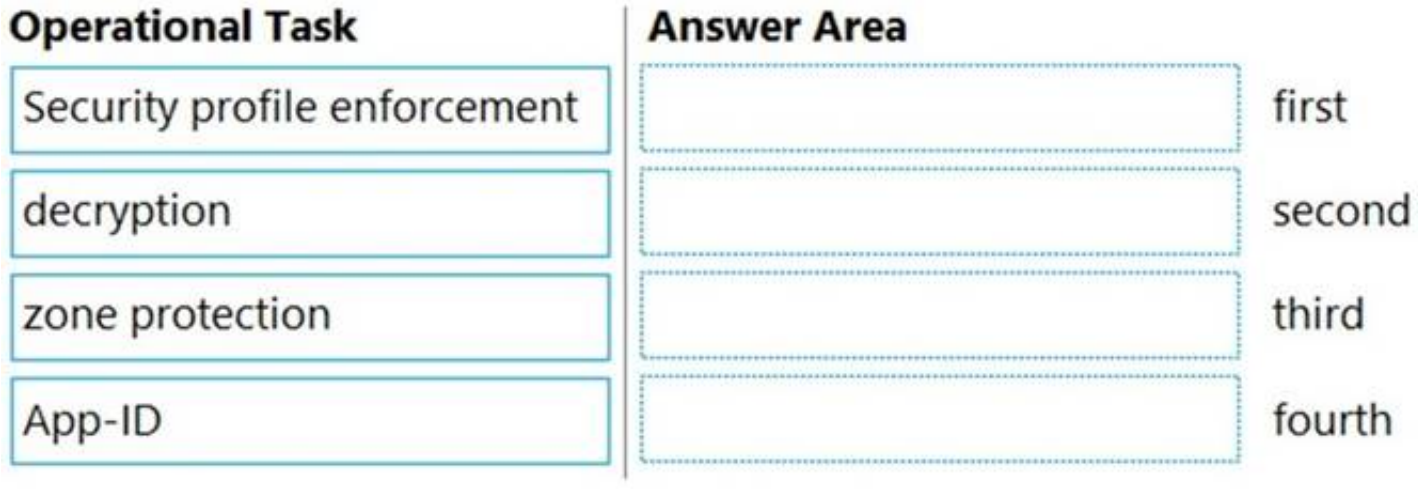
Explanation:
? A profile is a set of rules or settings that defines how the firewall performs a specific function, such as detecting and preventing threats, filtering URLs, or decrypting traffic1.
? There are different types of profiles that can be applied to different types of traffic or scenarios, such as Antivirus, Anti-Spyware, Vulnerability Protection, URL Filtering, File Blocking, Data Filtering, Decryption, or WildFire Analysis1.
? The WildFire Analysis profile is a profile that enables the firewall to submit unknown files or email links to the cloud-based WildFire service for analysis and verdict determination2. WildFire is the industry's most advanced analysis and prevention engine for highly evasive zero-day exploits and malware3. WildFire uses a variety of malware detection techniques, such as static analysis, dynamic analysis, machine learning, and intelligent run-time memory analysis, to identify and protect against unknown threats34.
? The Vulnerability Protection profile is a profile that protects the network from exploits that target known software vulnerabilities. It allows the administrator to configure the actions and log settings for each vulnerability severity level, such as critical, high, medium, low, or informational5.
? Content-ID is not a profile, but a feature of the firewall that performs multiple functions to identify and control applications, users, content, and threats on the network. Content-ID consists of four components: App-ID, User-ID, Content Inspection, and Threat Prevention.
? Advanced Threat Prevention is not a profile, but a term that refers to the comprehensive approach of Palo Alto Networks to prevent sophisticated and unknown threats. Advanced Threat Prevention includes WildFire, but also other products and services, such as DNS Security, Cortex XDR, Cortex XSOAR, and AutoFocus.
Therefore, the profile that should be used to obtain a verdict regarding analyzed files is the WildFire Analysis profile.
References:
1: Security Profiles - Palo Alto Networks 2: WildFire Analysis Profile - Palo Alto
Networks 3: WildFire - Palo Alto Networks 4: Advanced Wildfire as an ICAP Alternative | Palo Alto Networks 5: Vulnerability Protection Profile - Palo Alto Networks : [Content-ID - Palo Alto Networks] : [Advanced Threat Prevention - Palo Alto Networks]

NEW QUESTION 79
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 81
DRAG DROP
Place the steps in the correct packet-processing order of operations.



A. Mastered
B. Not Mastered

Answer: A

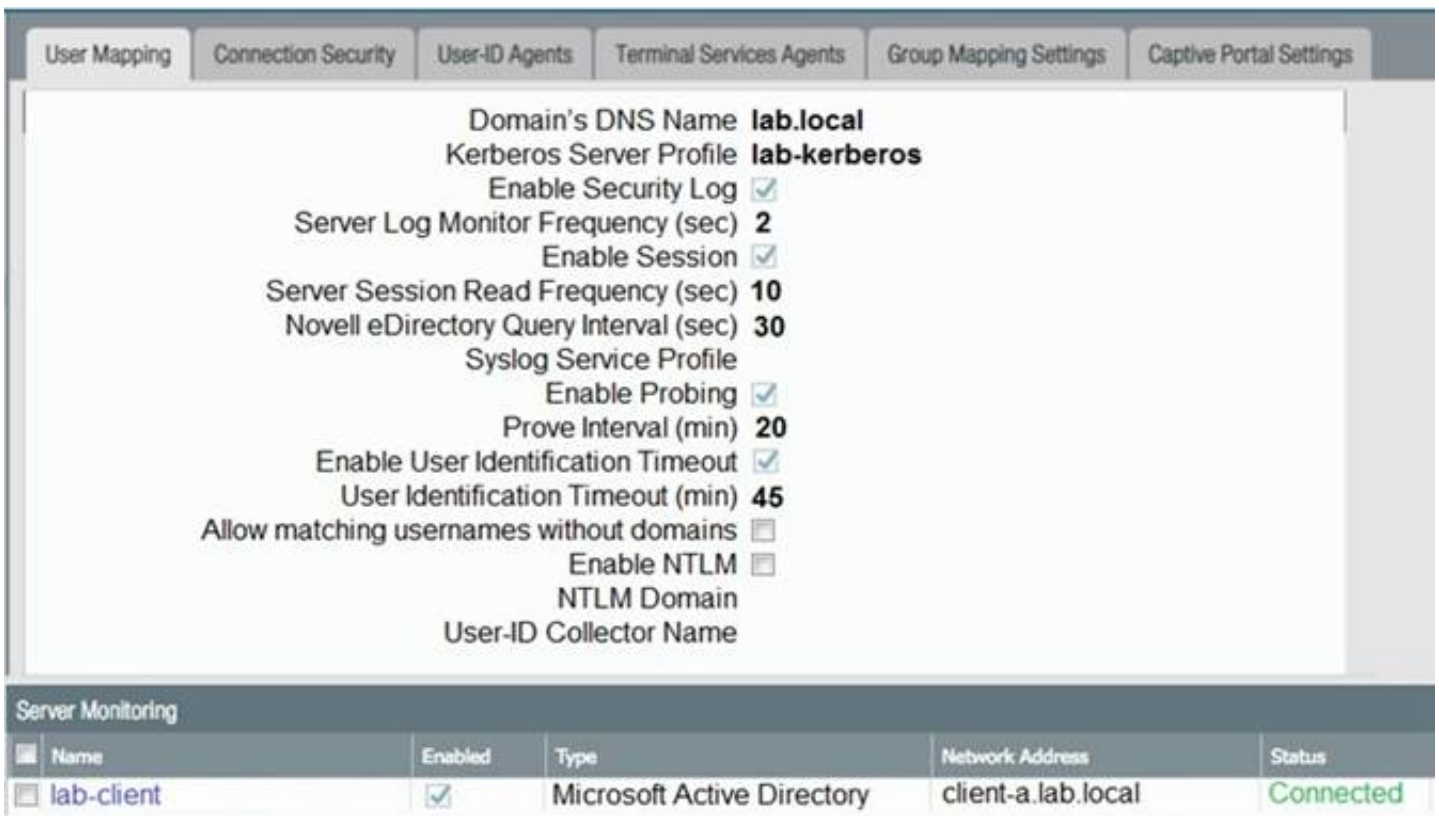
Explanation:

NEW QUESTION 84
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 89
Based on the graphic which statement accurately describes the output shown in the server monitoring panel?



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 94
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 96
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 100
What must be configured for the firewall to access multiple authentication profiles for external services to authenticate a non-local account?

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

Answer: A

NEW QUESTION 103
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 107
Which URL Filtering profile action would you set to allow users the option to access a site only if they provide a URL admin password?

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

Answer: B

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

NEW QUESTION 111
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 115
Complete the statement. A security profile can block or allow traffic

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

Answer: B

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

NEW QUESTION 120
Which two security profile types can be attached to a security policy? (Choose two.)

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

Answer: AD

NEW QUESTION 121
What is the maximum volume of concurrent administrative account sessions?

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

Answer: C

NEW QUESTION 124
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 125
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.

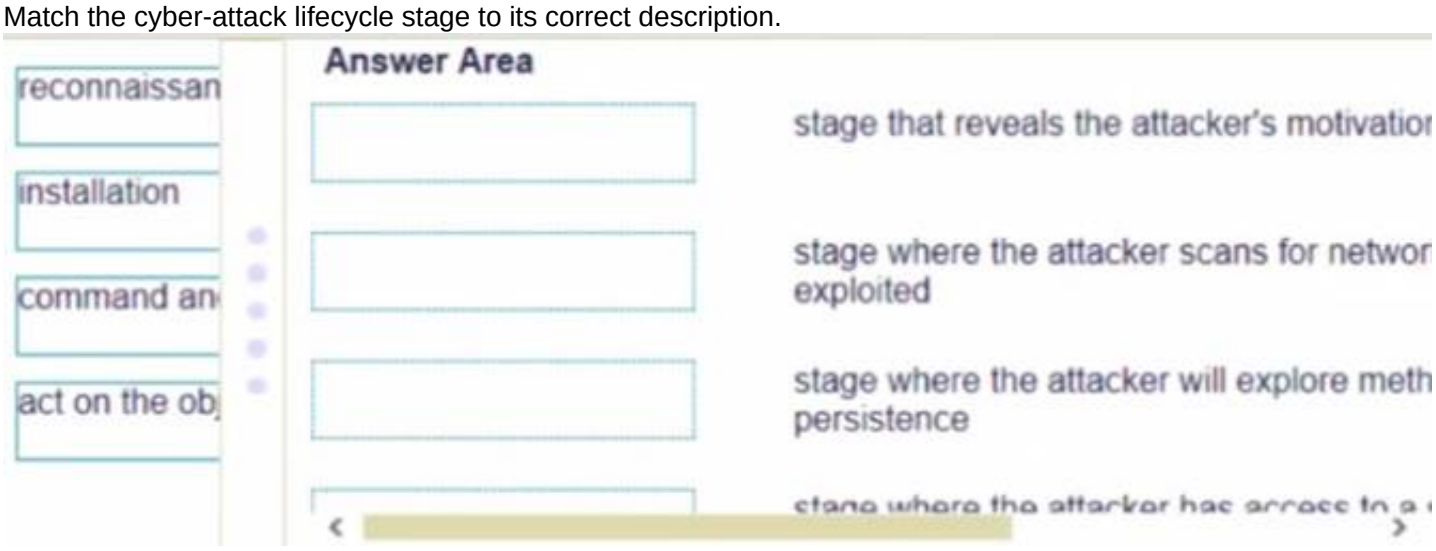
NEW QUESTION 127
Which link in the web interface enables a security administrator to view the security policy rules that match new application signatures?

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

Answer: D

Explanation:

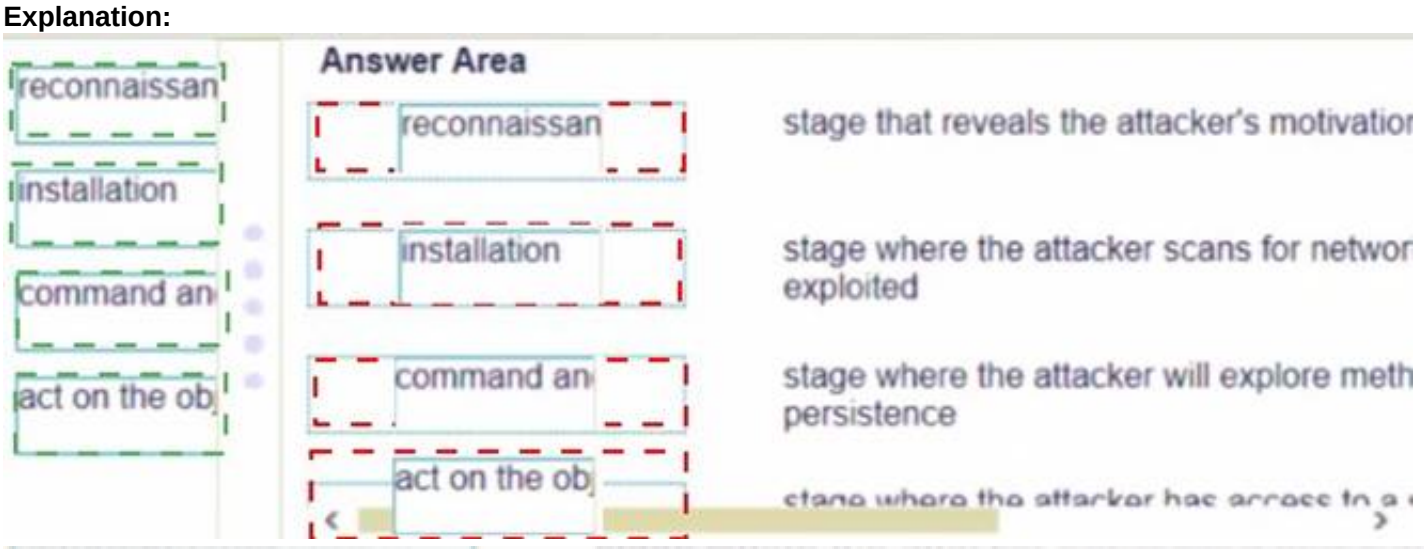
NEW QUESTION 131
DRAG DROP
Match the cyber-attack lifecycle stage to its correct description.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 133
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 138
An administrator would like to silently drop traffic from the internet to a ftp server. Which Security policy action should the administrator select?

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

Answer: D

NEW QUESTION 142
Which Palo Alto network security operating platform component provides consolidated policy creation and centralized management?

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

Answer: B

Explanation:

NEW QUESTION 147
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 151
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 152
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 155
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 156
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 160
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 162
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 166
An administrator is reviewing the Security policy rules shown in the screenshot below. Which statement is correct about the information displayed?

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

Answer: B

Explanation:

NEW QUESTION 169
Which administrative management services can be configured to access a management interface?

A. HTTP, CLI, SNMP, HTTPS
B. HTTPS, SSH telnet SNMP
C. SSH: telnet HTTP, HTTPS
D. HTTPS, HTT
E. CLI, API

Answer: D

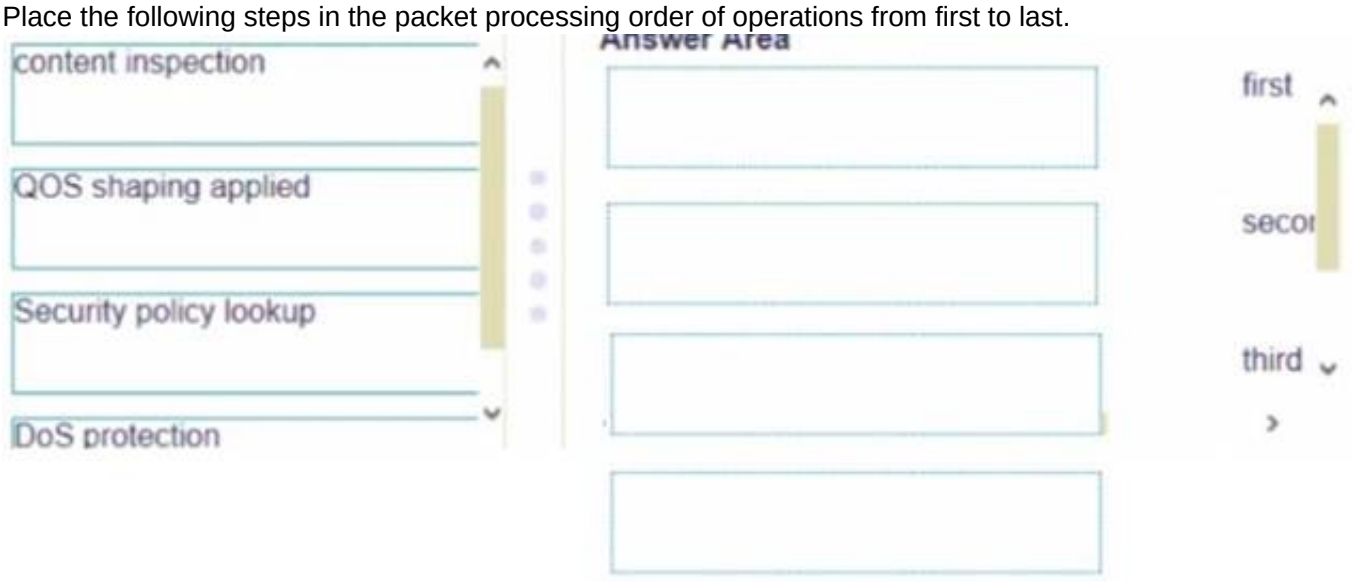
Explanation:
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/firewall-administration/management-interfaces
You can use the following user interfaces to manage the Palo Alto Networks firewall:
? Use the Web Interface to perform configuration and monitoring tasks with relative ease. This graphical interface allows you to access the firewall using HTTPS (recommended) or HTTP and it is the best way to perform administrative tasks.
? Use the Command Line Interface (CLI) to perform a series of tasks by entering
commands in rapid succession over SSH (recommended), Telnet, or the console port. The CLI is a no-frills interface that supports two command modes, operational and configure, each with a distinct hierarchy of commands and statements. When you become familiar with the nesting structure and syntax of the commands, the CLI provides quick response times and administrative efficiency.
? Use the XML API to streamline your operations and integrate with existing,
internally developed applications and repositories. The XML API is a web service implemented using HTTP/HTTPS requests and responses.
? Use Panorama to perform web-based management, reporting, and log collection
for multiple firewalls. The Panorama web interface resembles the firewall web interface but with additional functions for centralized management.

NEW QUESTION 171
What is a function of application tags?

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

Answer: C

NEW QUESTION 172
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 173
Which license is required to use the Palo Alto Networks built-in IP address EDLs?

A. DNS Security
B. Threat Prevention
C. WildFire
D. SD-Wan

Answer: B

Explanation:

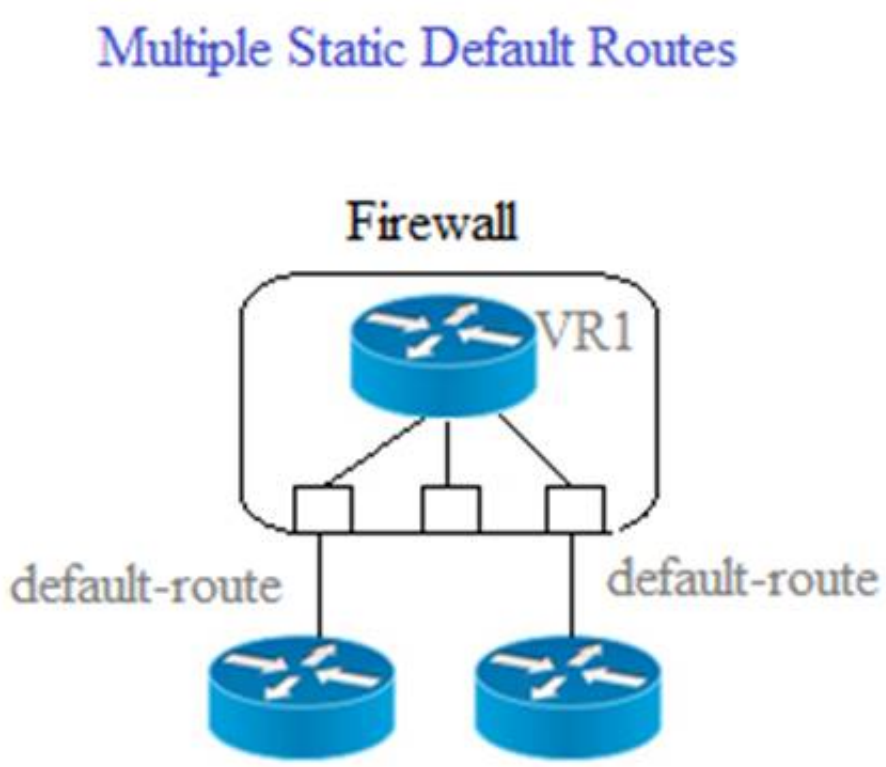
Reference:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/use-an-external- dynamic-list-in- policy/builtin-edls.html#:~:text=With%20an%

NEW QUESTION 176
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 178
Given the scenario, which two statements are correct regarding multiple static default routes? (Choose two.)



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

Answer: CD

NEW QUESTION 182
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 184
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 186
Which type of address object is "10 5 1 1/0 127 248 2"?

A. IP subnet

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

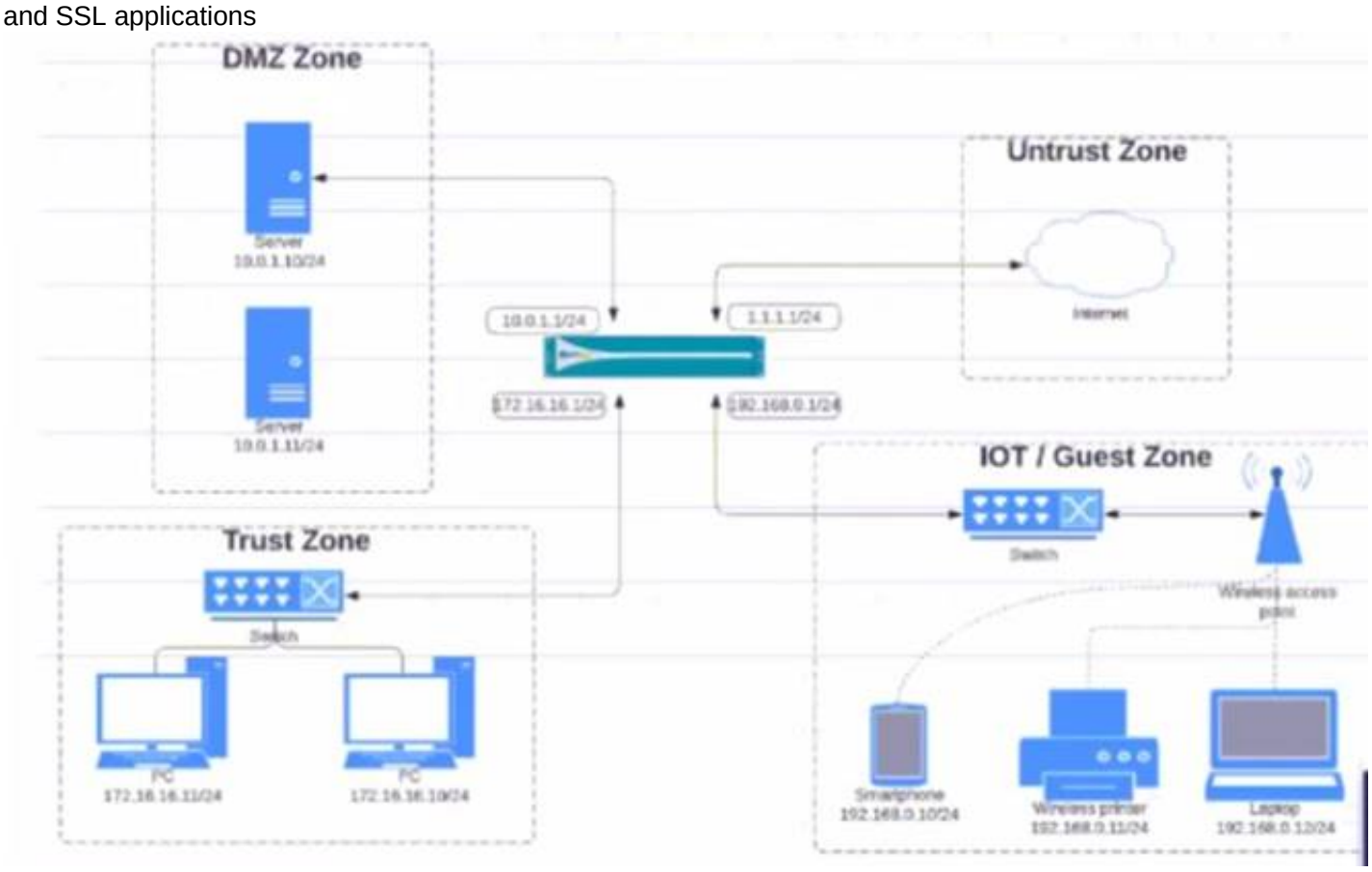
Answer: B

NEW QUESTION 189
Palo Alto Networks firewall architecture accelerates content map minimizing latency using which two components'? (Choose two)

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

Answer: B

NEW QUESTION 194
Given the network diagram, traffic should be permitted for both Trusted and Guest users to access general Internet and DMZ servers using SSH. web-browsing and SSL applications



Which policy achieves the desired results?
A)

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

B)

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

C)

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

D)

NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS
01-A	none	universal	IOT-Guest	10.0.1.0/24	any	any	DMZ	1.1.1.0/
			Trust	172.16.16.0/12			Untrust	192.168

A. Option

B. Option
C. Option
D. Option

Answer: C

NEW QUESTION 199
A Security Profile can block or allow traffic at which point?

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

Answer: A

NEW QUESTION 204
The PowerBall Lottery has reached a high payout amount and a company has decided to help employee morale by allowing employees to check the number, but doesn't want to unblock the gambling URL category.
Which two methods will allow the employees to get to the PowerBall Lottery site without the company unlocking the gambling URL category? (Choose two.)

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

Answer: CD

Explanation:

NEW QUESTION 208
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 209
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 211
Which object would an administrator create to block access to all high-risk applications?

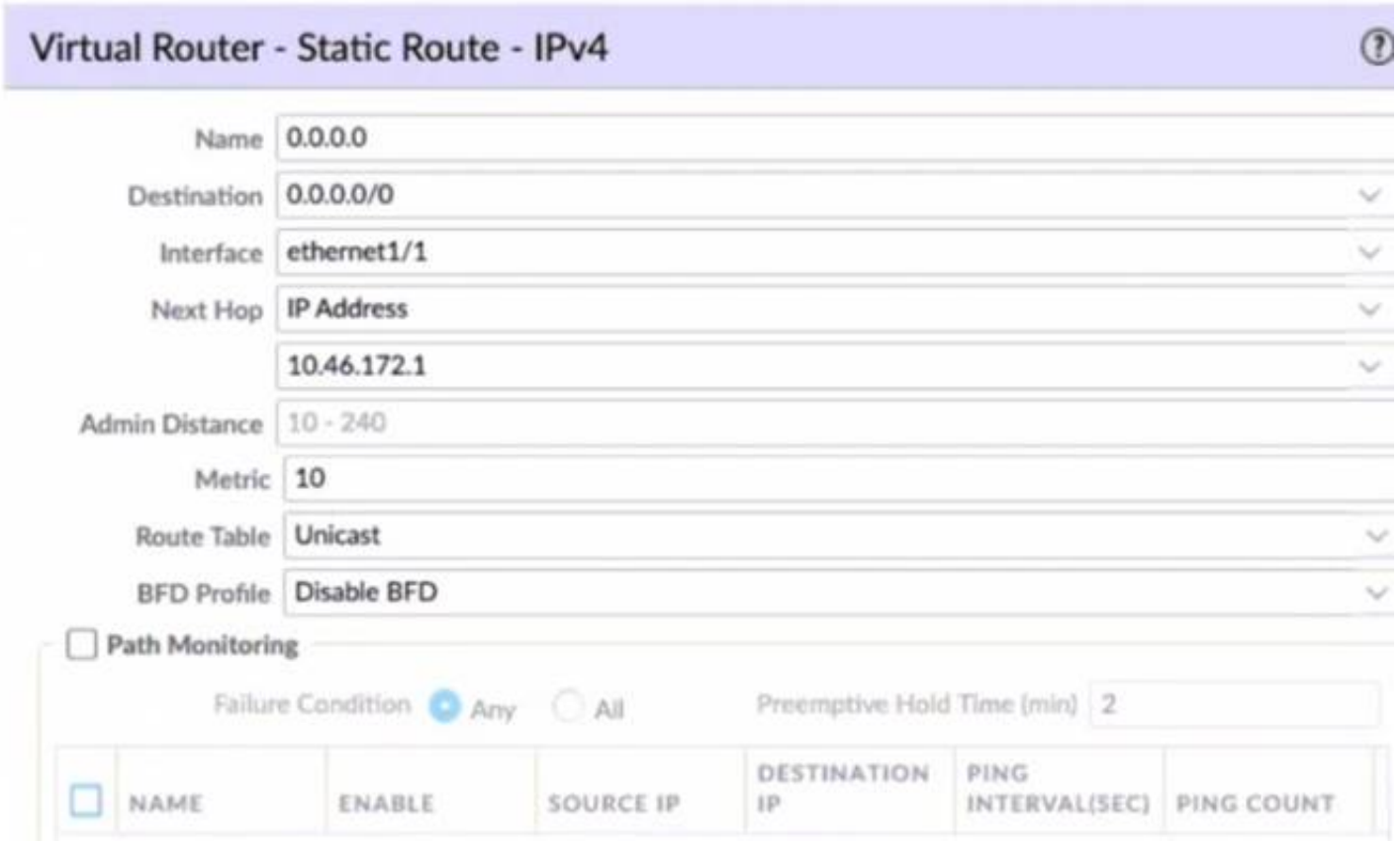
A. Mastered
B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 214
Given the screenshot what two types of route is the administrator configuring? (Choose two)



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

Answer: A

NEW QUESTION 216

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 217
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 221
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 222
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

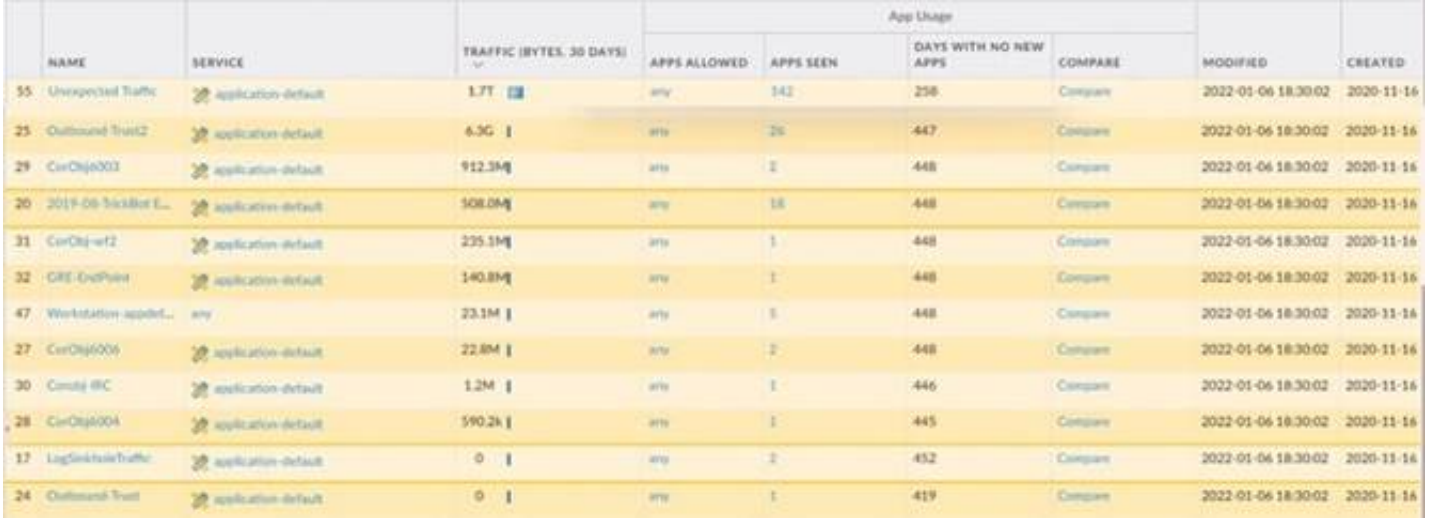
NEW QUESTION 223
Files are sent to the WildFire cloud service via the WildFire Analysis Profile. How are these files used?

A. WildFire signature updates

B. Malware analysis
C. Domain Generation Algorithm (DGA) learning
D. Spyware analysis

Answer: B

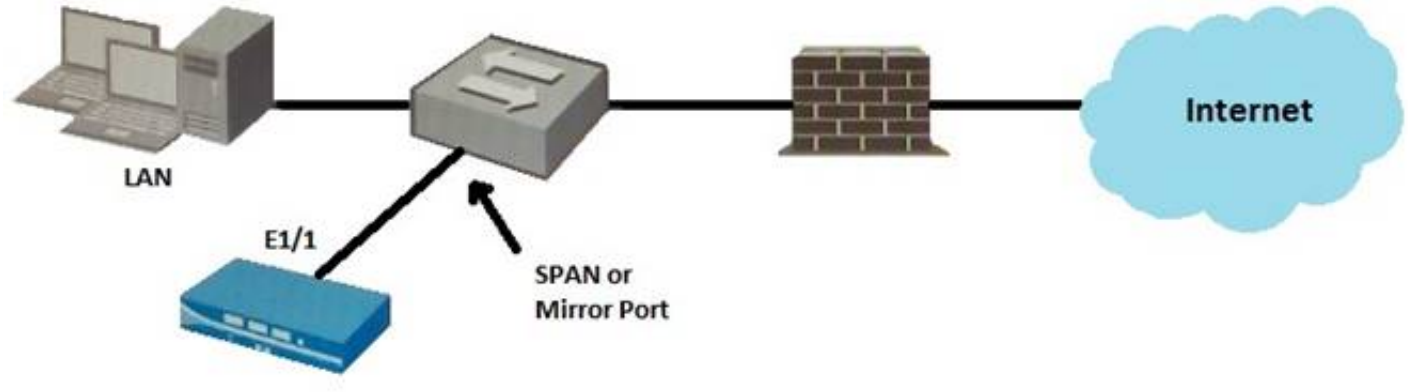
NEW QUESTION 228
An administrator is updating Security policy to align with best practices. Which Policy Optimizer feature is shown in the screenshot below?



A. Rules without App Controls
B. New App Viewer
C. Rule Usage
D. Unused Unused Apps

Answer: C

NEW QUESTION 231
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 233
Recently changes were made to the firewall to optimize the policies and the security team wants to see if those changes are helping.
What is the quickest way to reset the hit counter to zero in all the security policy rules?

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

Answer: D

NEW QUESTION 234
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your PCNSA Exam with Our Prep Materials Via below:

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