Paloalto-Networks

Exam Questions PCNSA

Palo Alto Networks Certified Network Security Administrator

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
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 3
Which update option is not available to administrators?

A. New Spyware Notifications
B. New URLs
C. New Application Signatures
D. New Malicious Domains
E. New Antivirus Signatures

Answer: B

NEW QUESTION 4
Which object would an administrator create to enable access to all applications in the office-programs subcategory?

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

Answer: A

NEW QUESTION 5
Which Security policy match condition would an administrator use to block traffic from IP addresses on the Palo Alto Networks EDL of Known Malicious IP Addresses list?

A.

destination address
B. source address
C. destination zone
D. source zone

Answer: B

Explanation:
Reference:https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/use-an-external-dynamic-list-in-policy/external-dynamic-list.html

NEW QUESTION 6
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 7
What is a prerequisite before enabling an administrative account which relies on a local firewall user database?

A. Configure an authentication policy
B. Configure an authentication sequence
C. Configure an authentication profile
D. Isolate the management interface on a dedicated management VLAN

Answer: C

NEW QUESTION 8
Which information is included in device state other than the local configuration?

A.

uncommitted changes

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

Answer: D

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

NEW QUESTION 9
When creating a Panorama administrator type of Device Group and Template Admin, which two things must you create first? (Choose two.)

A. password profile
B.

access domain
C. admin rote
D. server profile

Answer: CD

NEW QUESTION 10
Which type of security policy rule will match traffic that flows between the Outside zone and inside zone, but would not match traffic that flows within the zones?

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

Answer: C

Explanation:
Reference:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/software-and-content- updates/dynamic-contentupdates.html#:~:text=WildFire%20signature%20updates%20are%20made,within% 20a%20minute%20of %20availability

NEW QUESTION 10
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 11
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 13
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 18
Which statement best describes the use of Policy Optimizer?

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

Answer: B

NEW QUESTION 20
What are three characteristics of the Palo Alto Networks DNS Security service? (Choose three.)

A. It uses techniques such as DGA.DNS tunneling detection and machine learning.
B. It requires a valid Threat Prevention license.
C. It enables users to access real-time protections using advanced predictive analytics.
D. It requires a valid URL Filtering license.
E. It requires an active subscription to a third-party DNS Security service.

Answer: ABC

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

NEW QUESTION 25
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 27
What are three factors that can be used in domain generation algorithms? (Choose three.)

A. cryptographic keys
B. time of day
C. other unique values
D. URL custom categories
E. IP address

Answer: ABC

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

NEW QUESTION 31
Which statement is true regarding NAT rules?

A. Static NAT rules have precedence over other forms of NAT.
B. Translation of the IP address and port occurs before security processing.
C. NAT rules are processed in order from top to bottom.
D. Firewall supports NAT on Layer 3 interfaces only.

Answer: C

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

NEW QUESTION 34
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

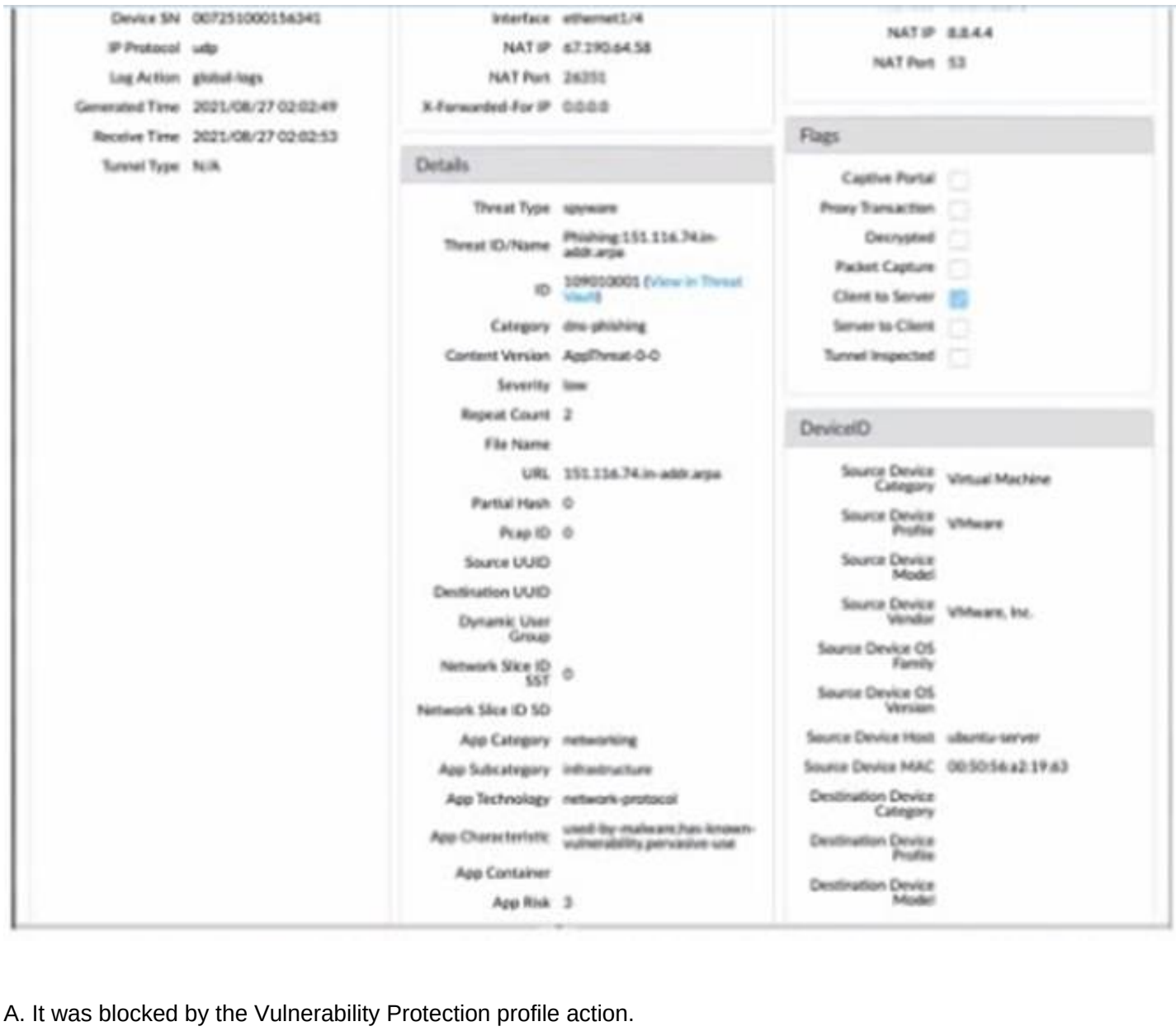
Answer: D

NEW QUESTION 39
Which two settings allow you to restrict access to the management interface? (Choose two)

A. Mastered
B. Not Mastered

Answer: A

NEW QUESTION 43
Given the detailed log information above, what was the result of the firewall traffic inspection?



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 47
What are two valid selections within an Antivirus profile? (Choose two.)

A. deny
B. drop
C. default
D. block-ip

Answer: BC

NEW QUESTION 49
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 54
A security administrator has configured App-ID updates to be automatically downloaded and installed. The company is currently using an application identified by App-ID as SuperApp_base.
On a content update notice, Palo Alto Networks is adding new app signatures labeled SuperApp_chat and SuperApp_download, which will be deployed in 30 days.
Based on the information, how is the SuperApp traffic affected after the 30 days have passed?

A. All traffic matching the SuperApp_chat, and SuperApp_download is denied because it no longer matches the SuperApp-base application
B. No impact because the apps were automatically downloaded and installed
C. No impact because the firewall automatically adds the rules to the App-ID interface
D. All traffic matching the SuperApp_base, SuperApp_chat, and SuperApp_download is denied until the security administrator approves the applications

Answer: A

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 58
An administrator is implementing an exception to an external dynamic list by adding an entry to the list manually. The administrator wants to save the changes, but the OK button is grayed out.
What are two possible reasons the OK button is grayed out? (Choose two.)

A. The entry contains wildcards.
B. The entry is duplicated.
C. The entry doesn't match a list entry.
D. The entry matches a list entry.

Answer: BC

NEW QUESTION 59
Which feature would be useful for preventing traffic from hosting providers that place few restrictions on content, whose services are frequently used by attackers to distribute illegal or unethical material?

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

Answer: A

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

NEW QUESTION 62

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

A. GlobalProtect agent
B. XML API
C.

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

Answer: BC

NEW QUESTION 69
Which type security policy rule would match traffic flowing between the inside zone and outside zone within the inside zone and within the outside zone?

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

Answer: B

NEW QUESTION 73
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 78
Prior to a maintenance-window activity, the administrator would like to make a backup of only the running configuration to an external location. What command in Device > Setup > Operations would provide the most operationally efficient way to achieve this outcome?

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Export Named Configuration Snapshot This option exports the current running configuration, a candidate configuration snapshot, or a previously imported configuration (candidate or running). The firewall exports the configuration as an XML file with the specified name. You can save the snapshot in any network

location. These exports often are used as backups. These XML files also can be used as templates for building other firewall configurations.

NEW QUESTION 80
A company moved its old port-based firewall to a new Palo Alto Networks NGFW 60 days ago. Which utility should the company use to identify out-of-date or unused rules on the firewall?

A. Rule Usage Filter > No App Specified
B. Rule Usage Filter >Hit Count > Unused in 30 days
C. Rule Usage Filter > Unused Apps
D. Rule Usage Filter > Hit Count > Unused in 90 days

Answer: D

NEW QUESTION 85
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 87
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 89
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 90
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 95
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 99
What does an administrator use to validate whether a session is matching an expected NAT policy?

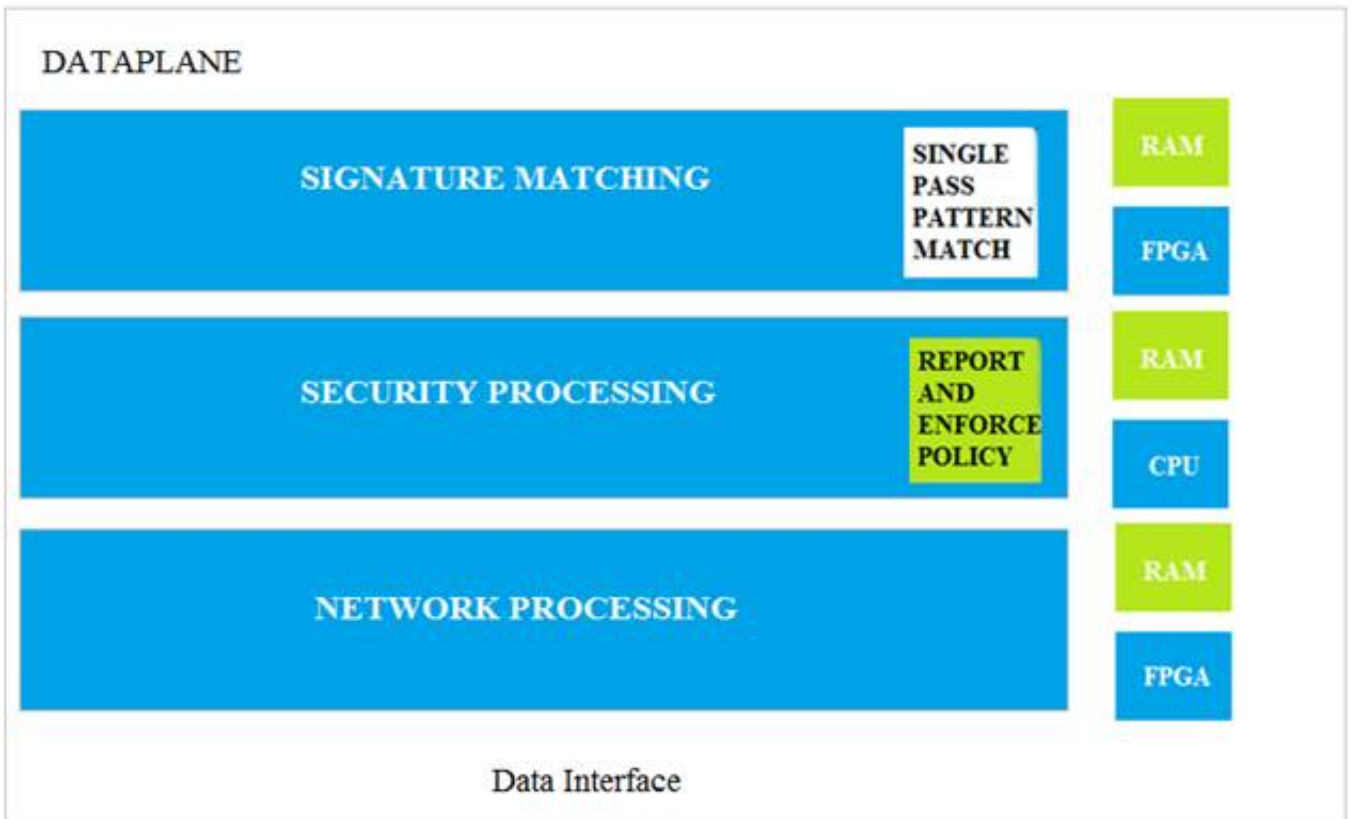
A. system log
B. test command
C. threat log
D. config audit

Answer: B

Explanation:

Reference:https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g00000 0ClQSCA0

NEW QUESTION 100
Which data-plane processor layer of the graphic shown provides uniform matching for spyware and vulnerability exploits on a Palo Alto Networks Firewall?



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

Answer: A

NEW QUESTION 104
Which three types of authentication services can be used to authenticate user traffic flowing through the firewalls data plane? (Choose three)

A. TACACS
B. SAML2
C. SAML10
D. Kerberos
E. TACACS+

Answer: ABD

NEW QUESTION 105
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 110
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 114
Identify the correct order to configure the PAN-OS integrated USER-ID agent.
* 3. add the service account to monitor the server(s)
* 2. define the address of the servers to be monitored on the firewall
* 4. commit the configuration, and verify agent connection status
* 1. create a service account on the Domain Controller with sufficient permissions to execute the User- ID agent

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

Answer: D

NEW QUESTION 118
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 123
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

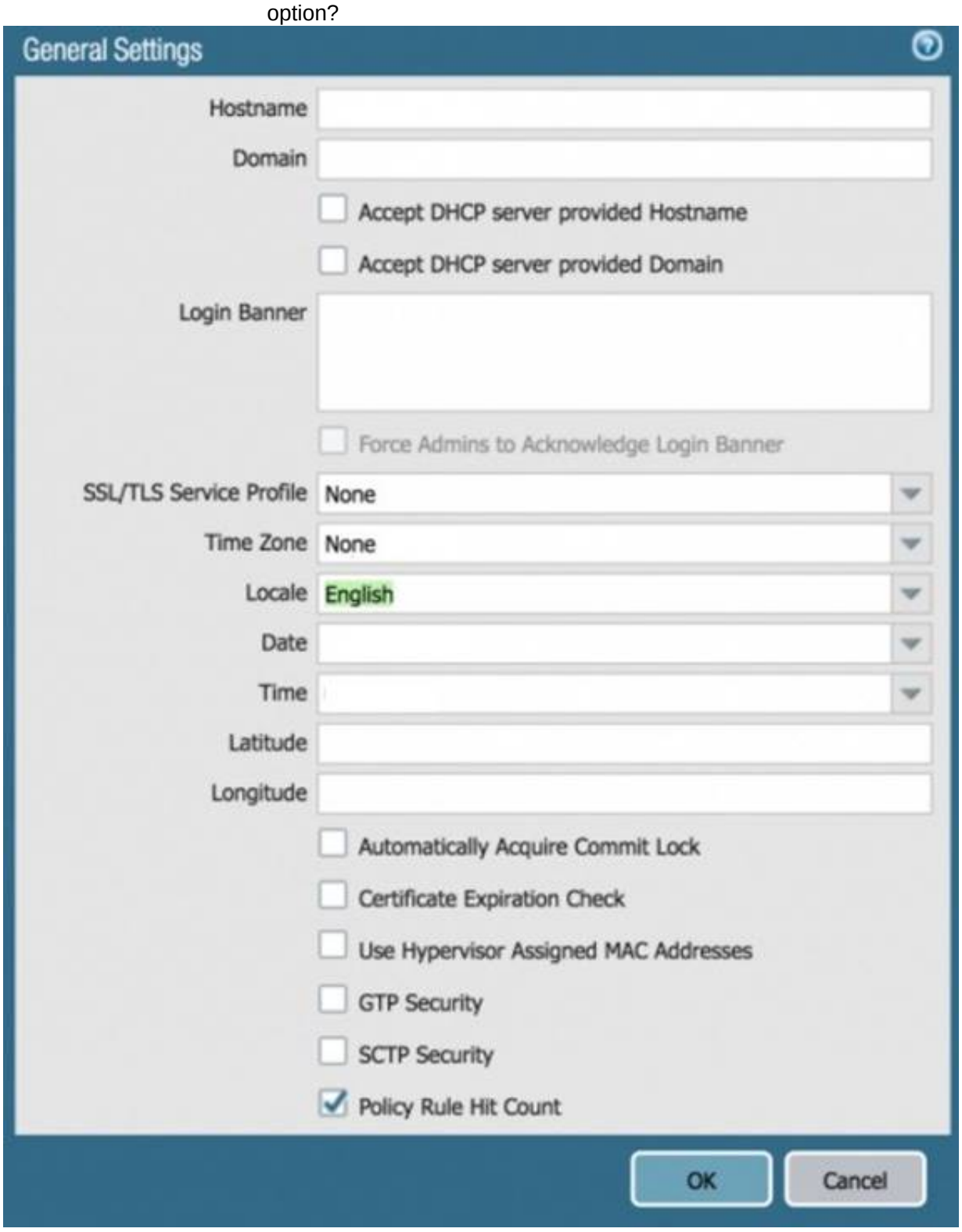
NEW QUESTION 126
Which profile should be used to obtain a verdict regarding analyzed files?

A. WildFire analysis
B. Vulnerability profile
C. Content-ID
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 127
Based on the graphic, what is the purpose of the SSL/TLS Service profile configuration option?



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 130
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 133
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

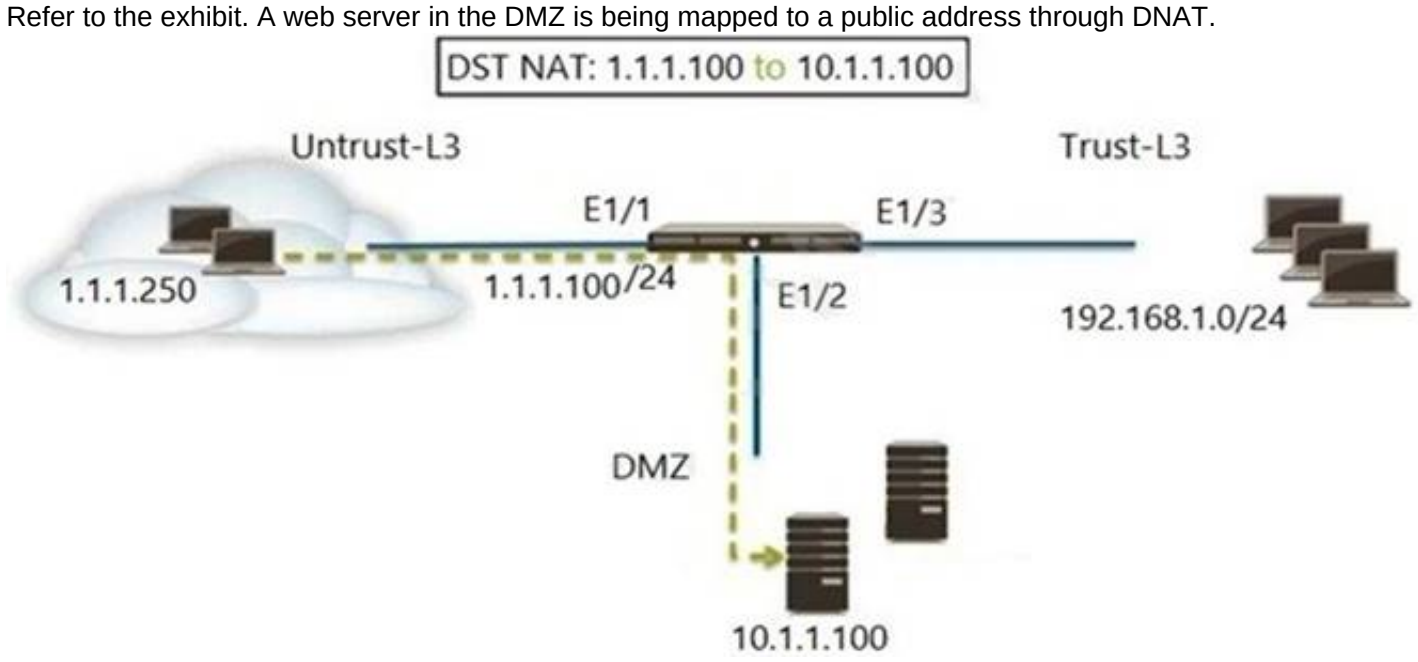
Answer: C

NEW QUESTION 134
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 139
Refer to the exhibit. A web server in the DMZ is being mapped to a public address through DNAT.



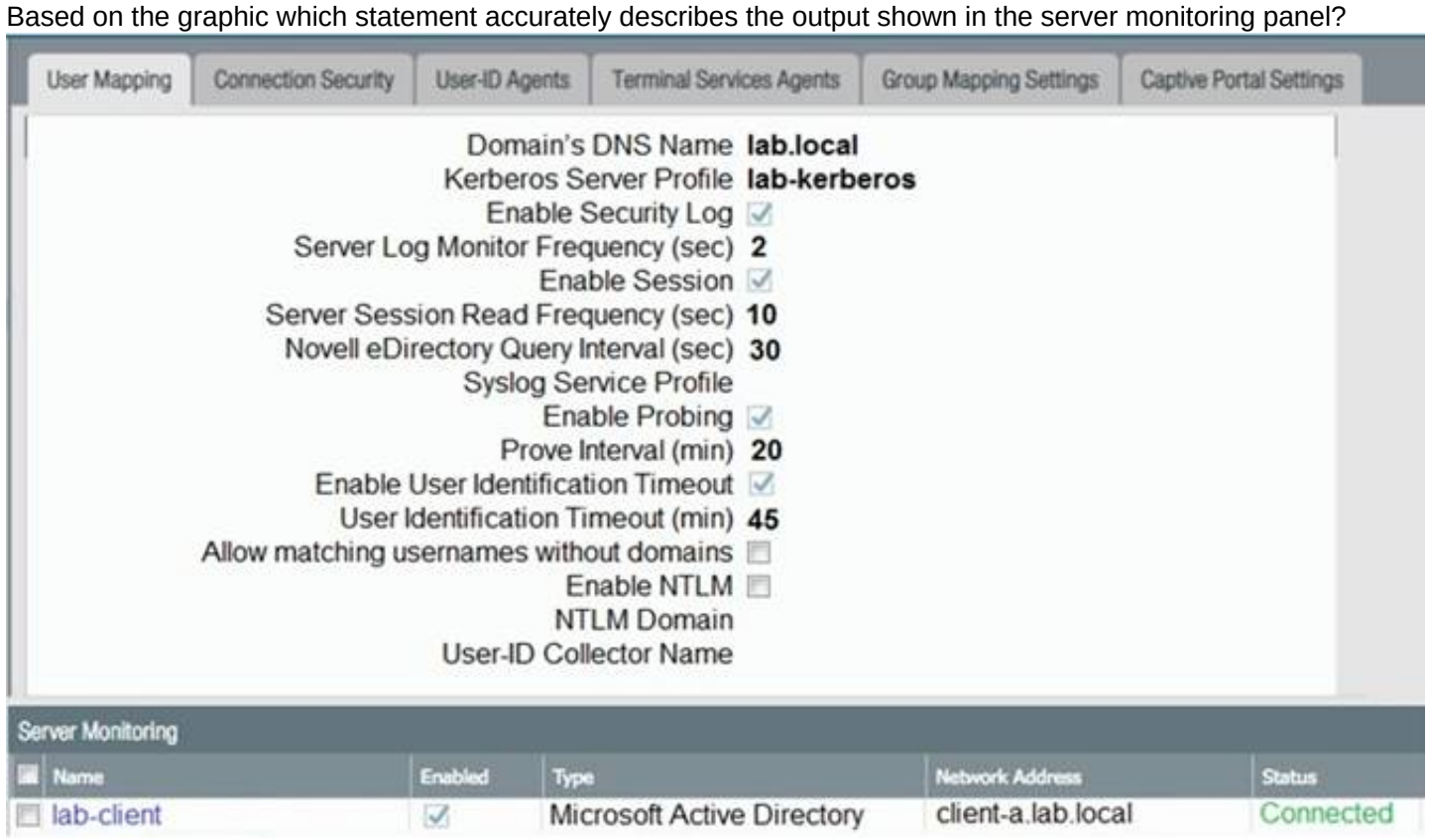
Which Security policy rule will allow traffic to flow to the web server?

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Reference:https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/networking/nat/nat-configuration-examples/destination-nat-exampleone-to-one-mapping

NEW QUESTION 143
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 146
Based on the screenshot what is the purpose of the included groups?

	Name	Type	Source Zone	Source Address	Source User	Destination Zone	Destination 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 150
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 152
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 157
What is the correct process tor creating a custom URL category?

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

Answer: D

Explanation:

NEW QUESTION 159
What must be configured before setting up Credential Phishing Prevention?

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

Answer: B

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

NEW QUESTION 162
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 164
Which license must an Administrator acquire prior to downloading Antivirus Updates for use with the firewall?

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

Answer: A

NEW QUESTION 168
When creating a custom URL category object, which is a valid type?

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

Answer: D

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

NEW QUESTION 173
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 174
What is the main function of Policy Optimizer?

A. reduce load on the management plane by highlighting combinable security rules
B. migrate other firewall vendors' security rules to Palo Alto Networks configuration
C. eliminate "Log at Session Start" security rules
D. convert port-based security rules to application-based security rules

Answer: D

Explanation:
Reference:https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-new-features/app-id- features/policy- optimizer.html

NEW QUESTION 177
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 178
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 180
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 183
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 186
An administrator needs to allow users to use only certain email applications.
How should the administrator configure the firewall to restrict users to specific email applications?

A. Create an application filter and filter it on the collaboration category, email subcategory.
B. Create an application group and add the email applications to it.
C. Create an application filter and filter it on the collaboration category.
D. Create an application group and add the email category to it.

Answer: B

NEW QUESTION 189
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 193
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 194
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 198
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 200
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 201
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 205
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.

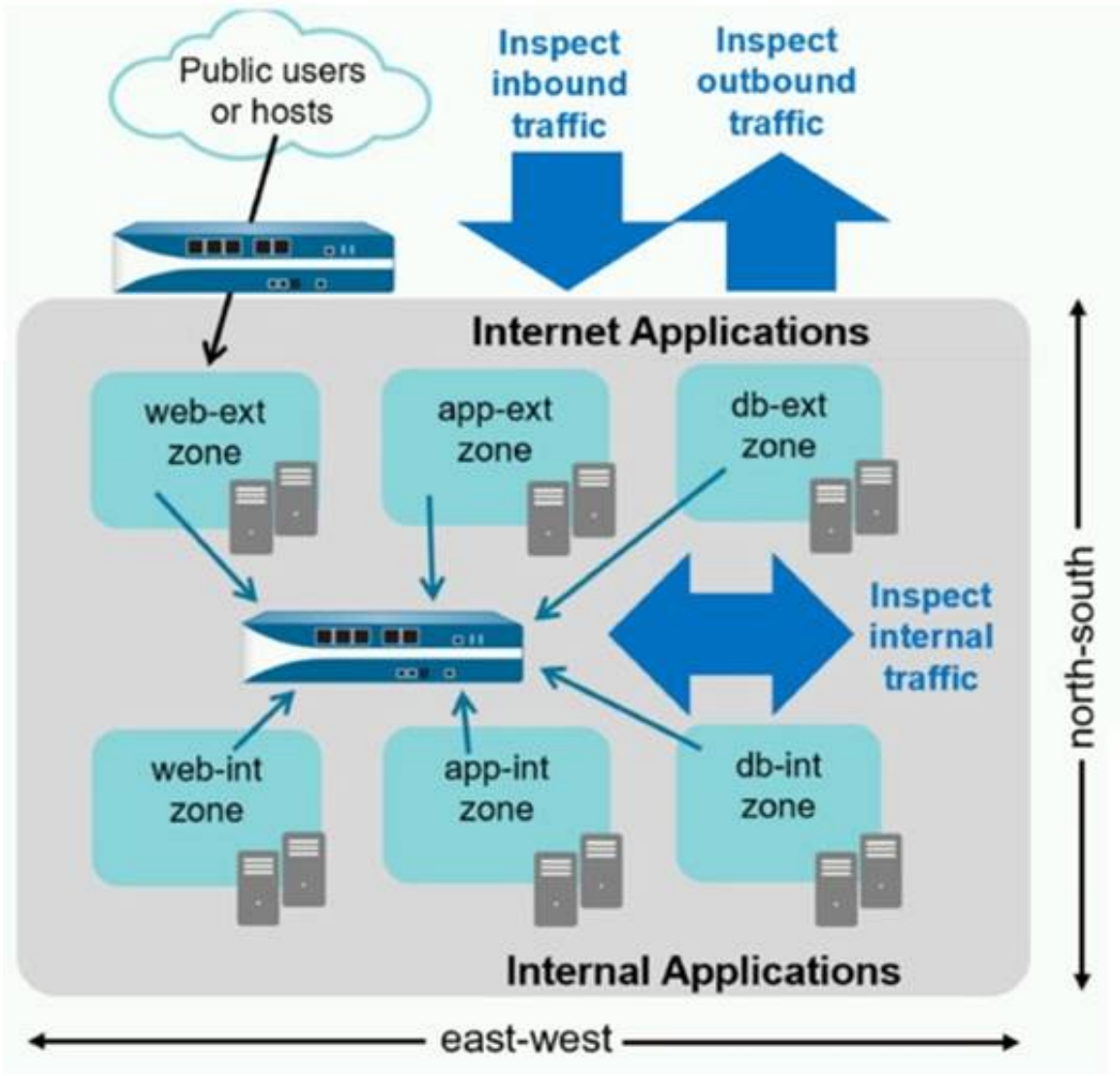
NEW QUESTION 207
By default, what is the maximum number of templates that can be added to a template stack?

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.

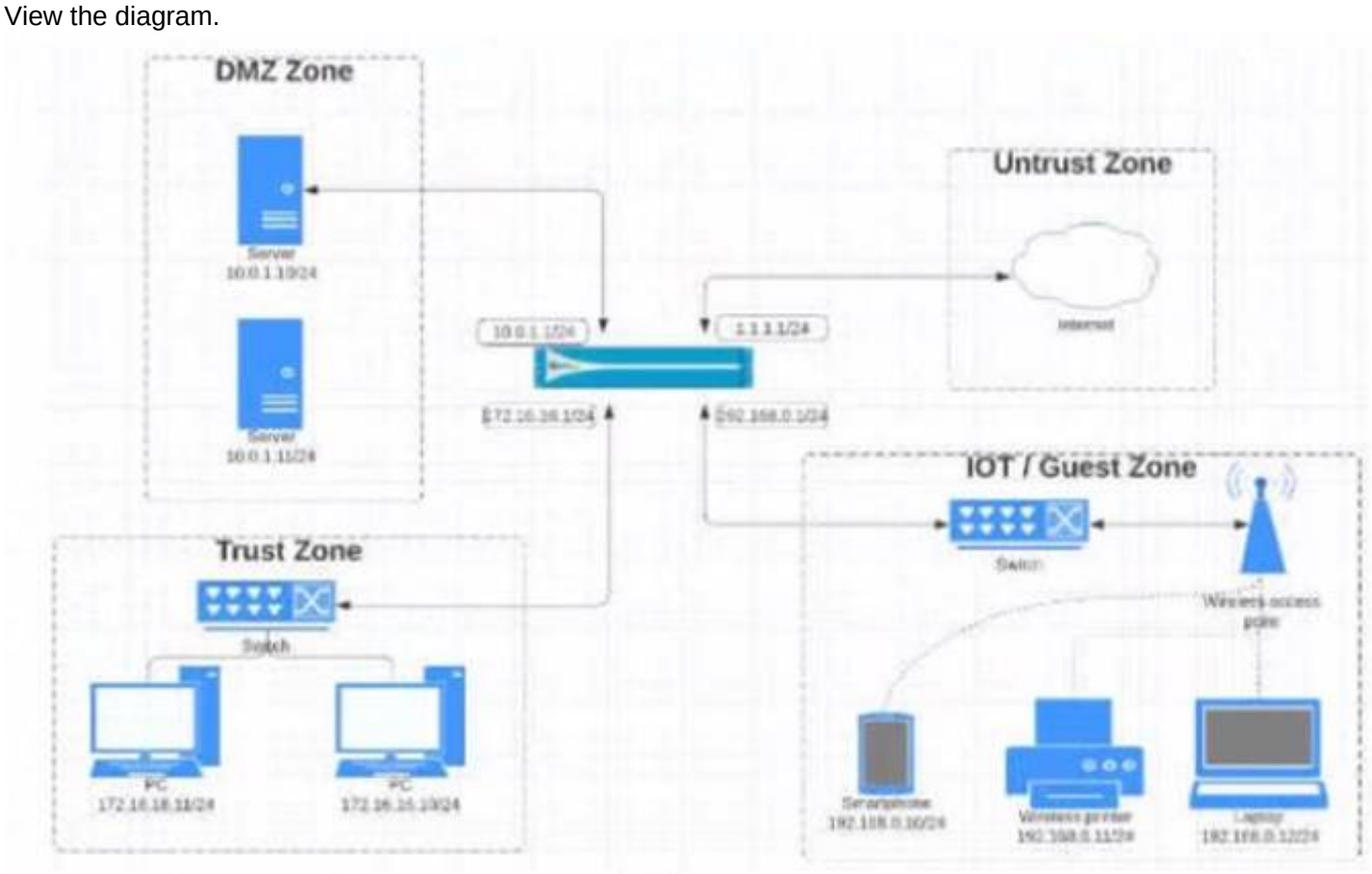
NEW QUESTION 210
An administrator notices that protection is needed for traffic within the network due to malicious lateral movement activity. Based on the image shown, which traffic would the administrator need to monitor and block to mitigate the malicious activity?



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

Answer: D

NEW QUESTION 215
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 lOT/Guest and Trust Zones?
A)

B)

C)

D)

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

Option D

D.

Answer: C

NEW QUESTION 220
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 225
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 226
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 227
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 229
What can be achieved by disabling the Share Unused Address and Service Objects with Devices setting on Panorama?

A. Increase the backup capacity for configuration backups per firewall
B. Increase the per-firewall capacity for address and service objects
C. Reduce the configuration and session synchronization time between HA pairs
D. Reduce the number of objects pushed to a firewall

Answer: D

NEW QUESTION 231
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 236
What in the minimum frequency for which you can configure the firewall too check for new wildfire antivirus signatures?

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

Answer: B

Explanation:

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

NEW QUESTION 237
Given the image, which two options are true about the Security policy rules. (Choose two.)

	Name	Tags	Type	Source Zone	Source Address	Source User	Source HIP Profile	Destination Zone	Destination Address	Rule Usage Hit Count	Rule Usage Last Hit	Rule Usage 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

A. The Allow Office Programs rule is using an Application Filter
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.

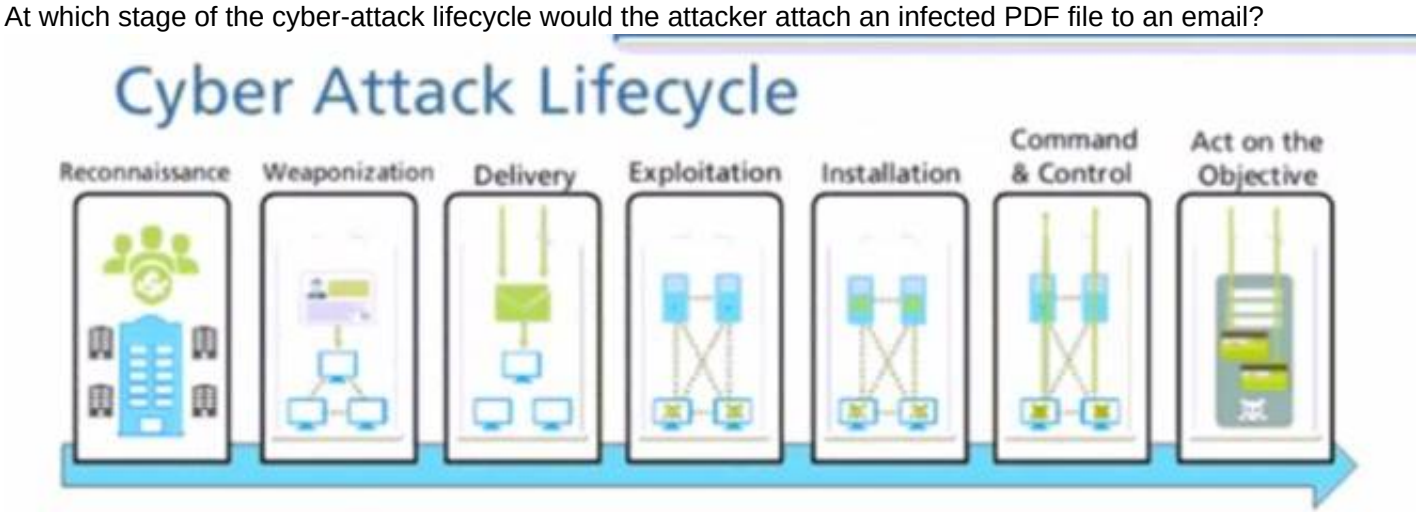
NEW QUESTION 239
Which type of address object is www.paloaltonetworks.com?

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

Answer: D

Explanation:

NEW QUESTION 242
At which stage of the cyber-attack lifecycle would the attacker attach an infected PDF file to an email?



A. delivery
B. command and control
C. explotation
D. reinsurance
E. installation

Answer: A

NEW QUESTION 245
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 250
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 254
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 257
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 260
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 261
Which administrator receives a global notification for a new malware that infects hosts. The infection will result in the infected host attempting to contact and command-and-control (C2) server.
Which security profile components will detect and prevent this threat after the firewall`s signature database has been updated?

A. antivirus profile applied to outbound security policies
B. data filtering profile applied to inbound security policies
C. data filtering profile applied to outbound security policies
D. vulnerability profile applied to inbound security policies

Answer: C

Explanation:

NEW QUESTION 264
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

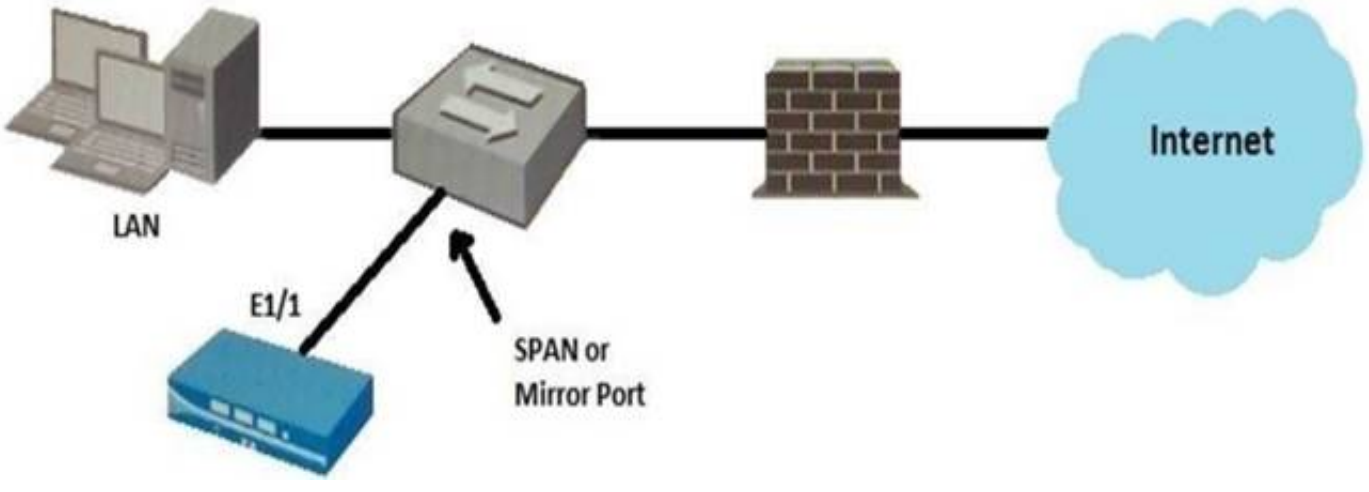
Explanation:
Reference:https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/threat-prevention/best-practices-for-content-and-threat-content-updates/best-practices-mission- critical.html

NEW QUESTION 267
Which the app-ID application will you need to allow in your security policy to use facebook- chat?

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

Answer: BD

NEW QUESTION 268
Given the topology, which zone type should you configure for firewall interface E1/1?



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

Answer: A

NEW QUESTION 273
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

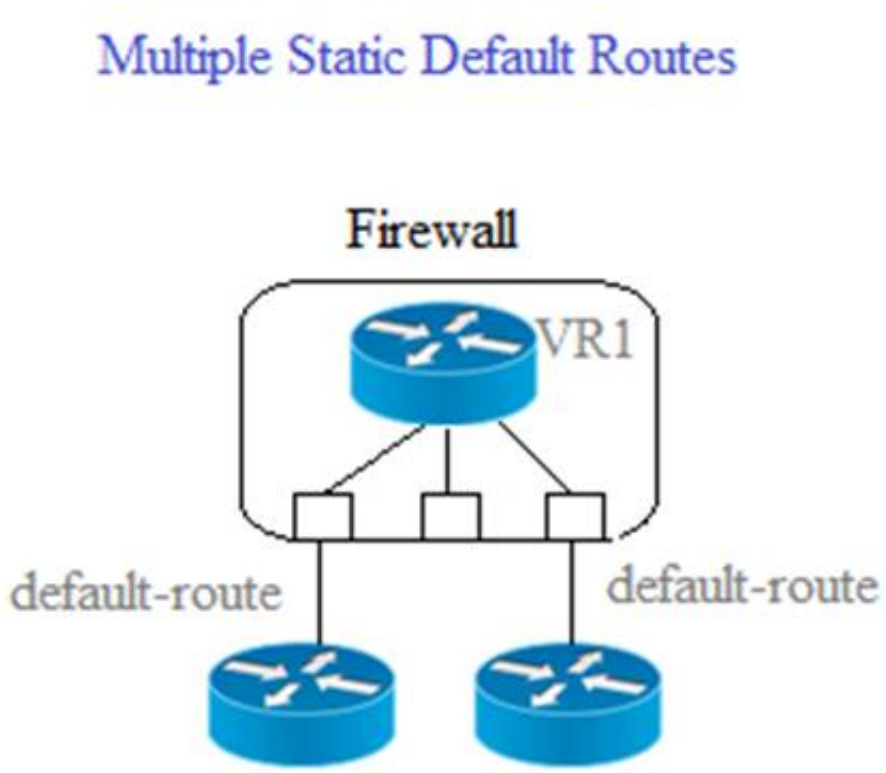
Answer: D

NEW QUESTION 275
Which statement is true regarding a Best Practice Assessment?

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

Answer: C

NEW QUESTION 280
Given the scenario, which two statements are correct regarding multiple static default routes? (Choose two.)



Path monitoring does not determine if route is useable

A
B: Route with highest metric is actively used
C. Path monitoring determines if route is useable
D. Route with lowest metric is actively used

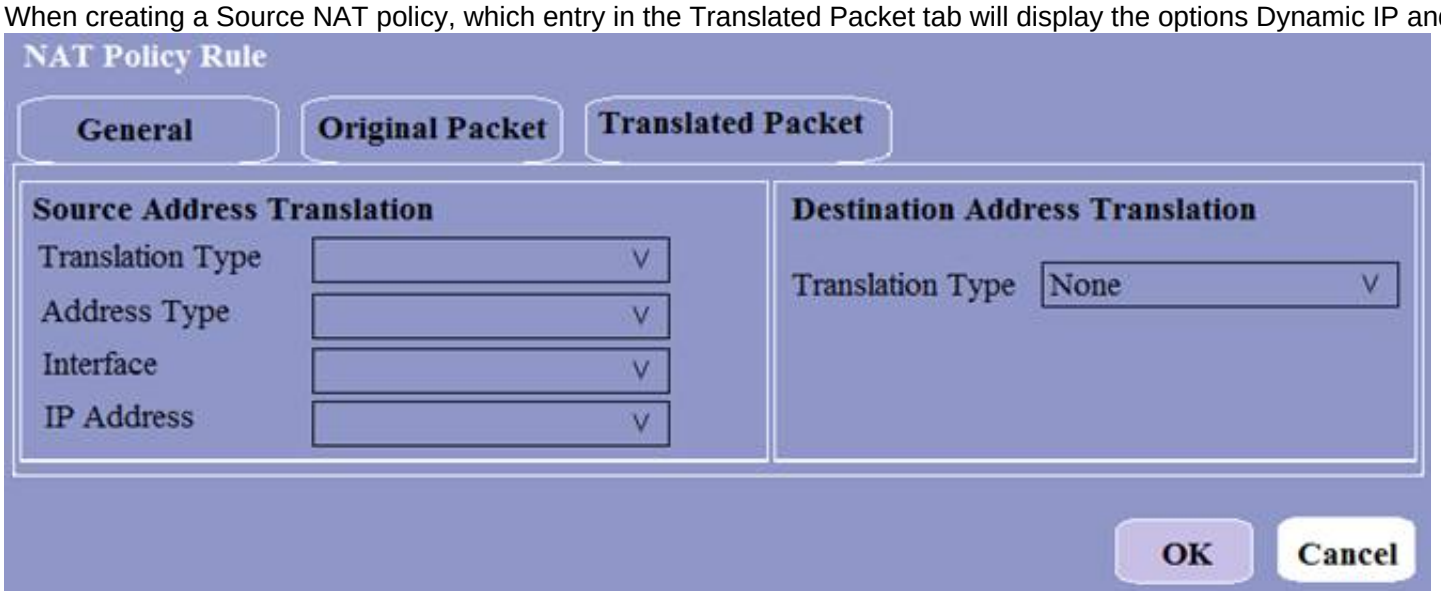
Answer: CD

NEW QUESTION 285
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 288
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 292
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 296
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 301
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 304
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 306
Why does a company need an Antivirus profile?

A. Mastered
B. Not Mastered

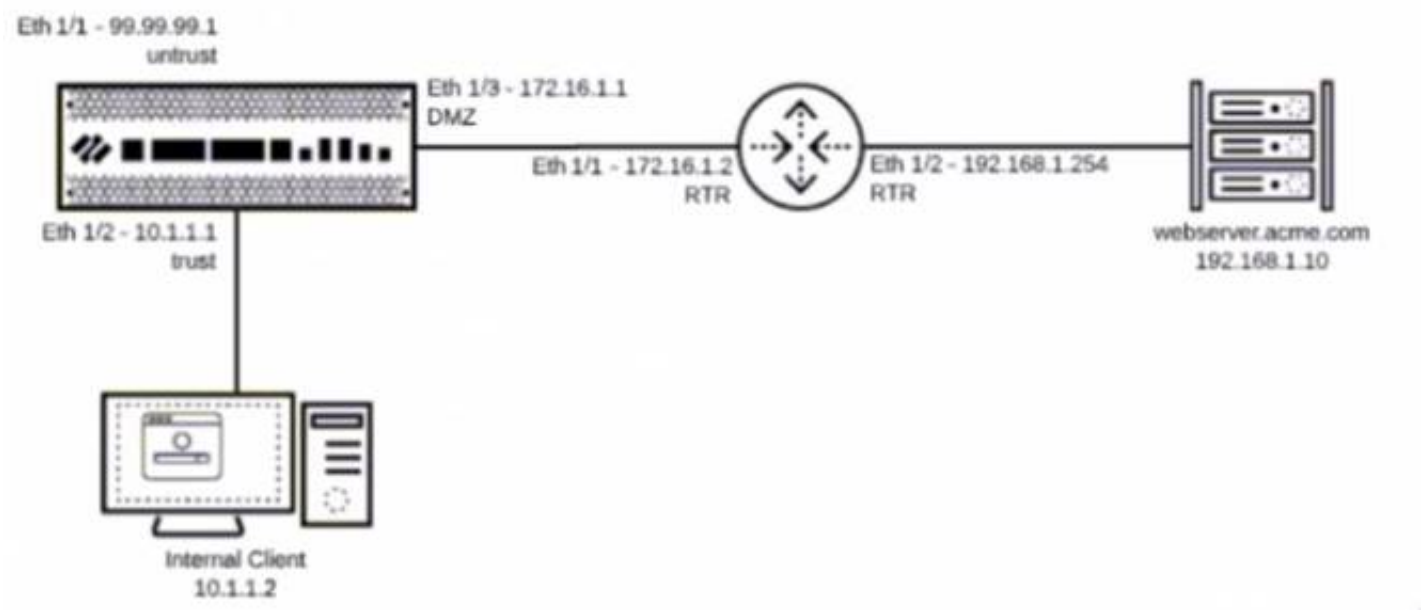
Answer: A

NEW QUESTION 309
An administrator wants to create a NAT policy to allow multiple source IP addresses to be translated to the same public IP address. What is the most appropriate NAT policy to achieve this?

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

Answer: A

NEW QUESTION 310
You have been tasked to configure access to a new web server located in the DMZ
Based on the diagram what configuration changes are required in the NGFW virtual router to route traffic from the 10 1 1 0/24 network to 192 168 1 0/24?



A. Add a route with the destination of 192 168 1 0/24 using interface Eth 1/3 with a next- hop of 192.168 1.10
B. Add a route with the destination of 192 168 1 0/24 using interface Eth 1/2 with a next- hop of 172.16.1.2
C. Add a route with the destination of 192 168 1 0/24 using interface Eth 1/3 with a next- hop of 172.16.1.2
D. Add a route with the destination of 192 168 1 0/24 using interface Eth 1/3 with a next- hop of 192.168.1.254

Answer: C

NEW QUESTION 313
Which type of profile must be applied to the Security policy rule to protect against buffer overflows illegal code execution and other attempts to exploit system flaws?

A. anti-spyware
B. URL filtering
C. vulnerability protection
D. file blocking

Answer: C

Explanation:

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

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

NEW QUESTION 315
An administrator needs to add capability to perform real-time signature lookups to block or sinkhole all known malware domains.
Which type of single unified engine will get this result?

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

Answer: A

NEW QUESTION 317
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 319
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 320
A network administrator created an intrazone Security policy rule on the firewall. The source zones were set to IT. Finance, and HR.
Which two types of traffic will the rule apply to? (Choose two)

A. Mastered
B. Not Mastered

Answer: A

NEW QUESTION 323
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 326
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 330
You receive notification about new malware that is being used to attack hosts The malware exploits a software bug in a common application
Which Security Profile detects and blocks access to this threat after you update the firewall's threat signature database?

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

Answer: B

NEW QUESTION 335
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 337
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 338
Given the screenshot, what are two correct statements about the logged traffic? (Choose two.)

TYPE	FROM ZONE	TO ZONE	INGRESS I/F	SOURCE	NAT APPLIED	EGRESS I/F	DESTINATION	TO PORT	APPLICATION	ACTION	SESSION END REASON	BYTES	ACTION SOURCE	LOG ACTION	BYTES SENT	BYTES RECEIVED	LOG TYPE
end	LAN	Internet	ethernet1/2	192.168.200.100	yes	ethernet1/5	198.54.12.97	443	web-browsing	allow	threat	3.3k	from-policy	default	2.7k	541	traffic

A. The web session was unsuccessfully decrypted.
B. The traffic was denied by security profile.
C. The traffic was denied by URL filtering.
D. The web session was decrypted.

Answer: D

NEW QUESTION 343
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 348
How frequently can wildfire updates be made available to firewalls?

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

Answer: D

NEW QUESTION 351
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 355
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 359
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 362
An administrator wants to prevent users from submitting corporate credentials in a phishing attack.
Which Security profile should be applied?

A. antivirus
B. anti-spyware
C. URL filtering
D. vulnerability protection

Answer: B

NEW QUESTION 367
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 370
Your company occupies one floor in a single building you have two active directory domain controllers on a single networks the firewall s management plane is only slightly utilized.
Which user-ID agent sufficient in your network?

A. PAN-OS integrated agent deployed on the firewall
B. Windows-based agent deployed on the internal network a domain member
C. Citrix terminal server agent deployed on the network
D. Windows-based agent deployed on each domain controller

Answer: D

Explanation:

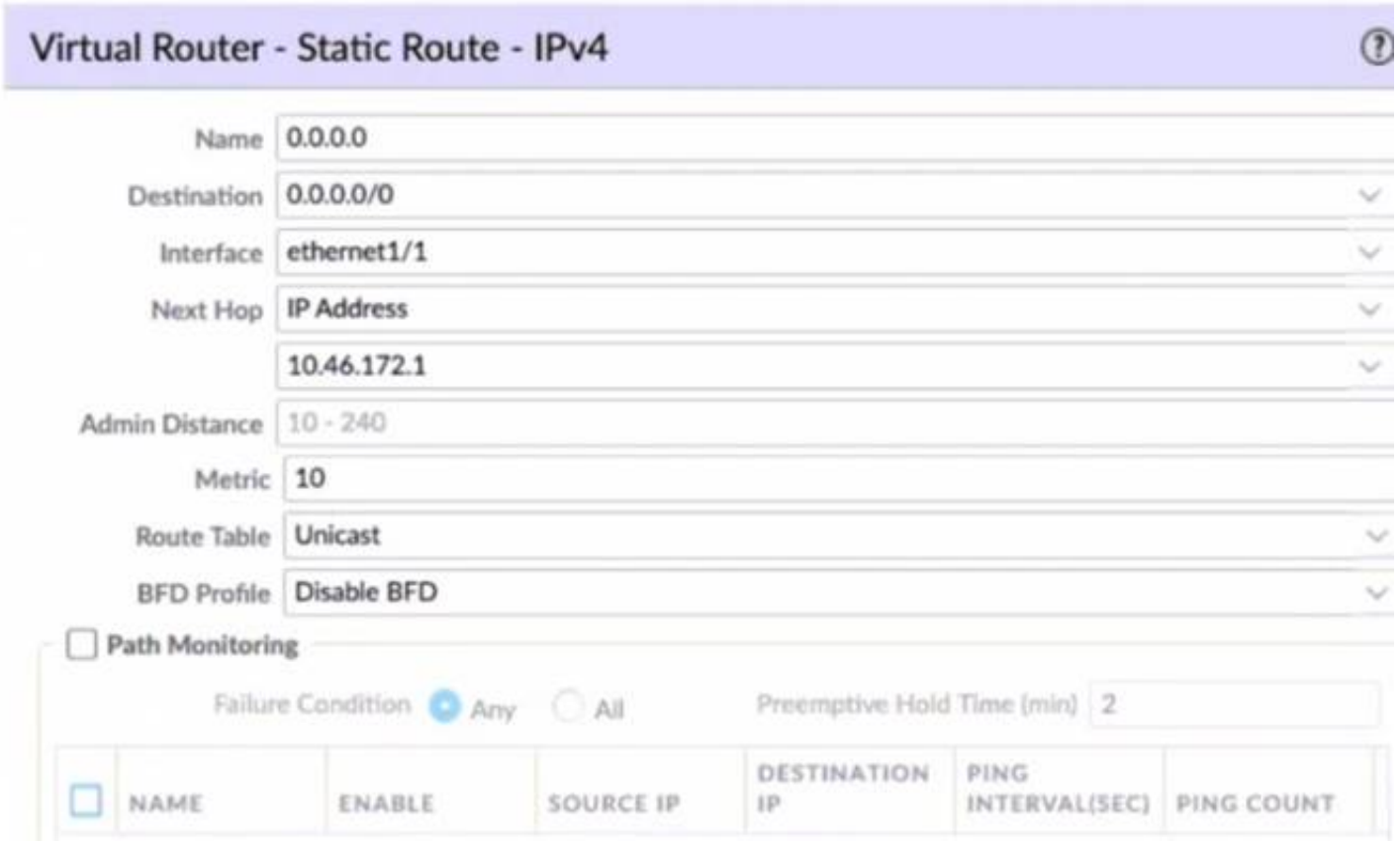
Reference:
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/user-id/map-ip-addresses-to-users/configureuser-mapping-using-the-windows-user-id-agent/configure-the-windows-based-user-id-agent-for-usermapping.html

NEW QUESTION 375
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 379
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 381
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 384
Starting with PAN_OS version 9.1 which new type of object is supported for use within the user field of a security policy rule?

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

Answer: B

NEW QUESTION 389
How can a complete overview of the logs be displayed to an administrator who has permission in the system to view them?

A. Select the unified log entry in the side menu.
B. Modify the number of columns visible on the page
C. Modify the number of logs visible on each page.
D. Select the system logs entry in the side menu.

Answer: A

Explanation:
The best way to view a complete overview of the logs is to select the unified log entry in the side menu. The unified log is a single view that displays all the logs generated by the firewall, such as traffic, threat, URL filtering, data filtering, and WildFire logs1. The unified log allows the administrator to filter, sort, and export the logs based on various criteria, such as time range, severity, source, destination, application, or action1.
Modifying the number of columns visible on the page or the number of logs visible on each page does not provide a complete overview of the logs, but only changes the display settings of the current log view. Selecting the system logs entry in the side menu does not show all the logs generated by the firewall, but only shows the logs related to system events, such as configuration changes, system alerts, or HA status2.
References:
1: View Logs - Palo Alto Networks 2: View and Manage Logs - Palo Alto Networks

NEW QUESTION 393
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 395
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 397
What can be used as match criteria for creating a dynamic address group?

A. Usernames
B. IP addresses
C. Tags
D. MAC addresses

Answer: C

NEW QUESTION 400
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

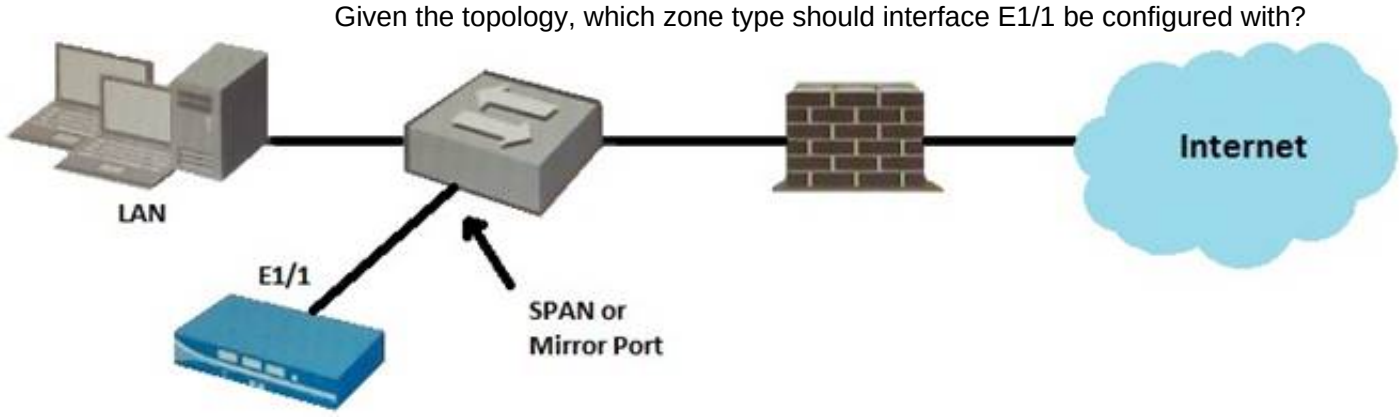
Answer: B

NEW QUESTION 402
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 403
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 408
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 413
.....

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