Paloalto-Networks

Exam Questions PCNSA

Palo Alto Networks Certified Network Security Administrator

NEW QUESTION 1
An administrator wants to create a No-NAT rule to exempt a flow from the default NAT rule. What is the best way to do this?

A. Create a Security policy rule to allow the traffic.
B. Create a new NAT rule with the correct parameters and leave the translation type as None
C. Create a static NAT rule with an application override.
D. Create a static NAT rule translating to the destination interface.

Answer: B

NEW QUESTION 2
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 3
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 4
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 5
Actions can be set for which two items in a URL filtering security profile? (Choose two.)

A. Block List
B. Custom URL Categories
C. PAN-DB URL Categories
D. Allow List

Answer: AD

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

NEW QUESTION 6
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 7
Which security profile will provide the best protection against ICMP floods, based on individual combinations of a packet`s source and destination IP address?

A. DoS protection
B. URL filtering
C. packet buffering
D. anti-spyware

Answer: A

NEW QUESTION 8
Based on the show security policy rule would match all FTP traffic from the inside zone to the outside zone?

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

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

Answer: B

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

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

Answer: AC

NEW QUESTION 14
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 18
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 23
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 27
What can be achieved by selecting a policy target prior to pushing policy rules from Panorama?

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

Answer: C

NEW QUESTION 28
You receive notification about a new malware that infects hosts An infection results in the infected host attempting to contact a command-and-control server Which Security Profile when applied to outbound Security policy rules detects and prevents this threat from establishing a command-and-control connection?

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

Answer: D

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

NEW QUESTION 33
What two authentication methods on the Palo Alto Networks firewalls support authentication and authorization for role-based access control? (Choose two.)

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

Answer: AB

Explanation:

Reference:https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/firewall-administration/manage-firewall-administrators/administrative-authentication.html
The administrative accounts are defined on an external SAML, TACACS+, or RADIUS server. The server performs both authentication and authorization. For authorization, you define Vendor-Specific Attributes (VSAs) on the TACACS+ or RADIUS server, or SAML attributes on the SAML server. PAN-OS maps the attributes to administrator roles, access domains, user groups, and virtual systems that you define on the firewall.

NEW QUESTION 34
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 37
Which built-in IP address EDL would be useful for preventing traffic from IP addresses that are verified as unsafe based on WildFire analysis Unit 42 research and data gathered from telemetry?

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

Answer: D

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

NEW QUESTION 38
Which Palo Alto networks security operating platform service protects cloud-based application such as Dropbox and salesforce by monitoring permissions and shared and scanning files for Sensitive information?

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

Answer: A

NEW QUESTION 41
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 45
You need to allow users to access the office–suite application of their choice. How should you configure the firewall to allow access to any office-suite application?

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

Answer: C

NEW QUESTION 48
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 51
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 56
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 61
Which dynamic update type includes updated anti-spyware signatures?

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

Answer: A

NEW QUESTION 65
Which three interface deployment methods can be used to block traffic flowing through the Palo Alto Networks firewall? (Choose three.)

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

Answer: BDE

NEW QUESTION 67
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 69
What are two valid selections within an Antivirus profile? (Choose two.)

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

Answer: BC

NEW QUESTION 73
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 75
At which point in the app-ID update process can you determine if an existing policy rule is affected by an app-ID update?

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

Answer: A

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

NEW QUESTION 80
Which option is part of the content inspection process?

A. IPsec tunnel encryption
B. Packet egress process
C. SSL Proxy re-encrypt
D. Packet forwarding process

Answer: C

NEW QUESTION 83
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 85
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 87
To use Active Directory to authenticate administrators, which server profile is required in the authentication profile?

A. Mastered
B. Not Mastered

Answer: A

NEW QUESTION 89
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 92
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 97
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 101
Which two components are utilized within the Single-Pass Parallel Processing architecture on a Palo Alto Networks Firewall? (Choose two.)

A. Layer-ID
B. User-ID
C. QoS-ID
D. App-ID

Answer: BD

Explanation:

NEW QUESTION 105
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

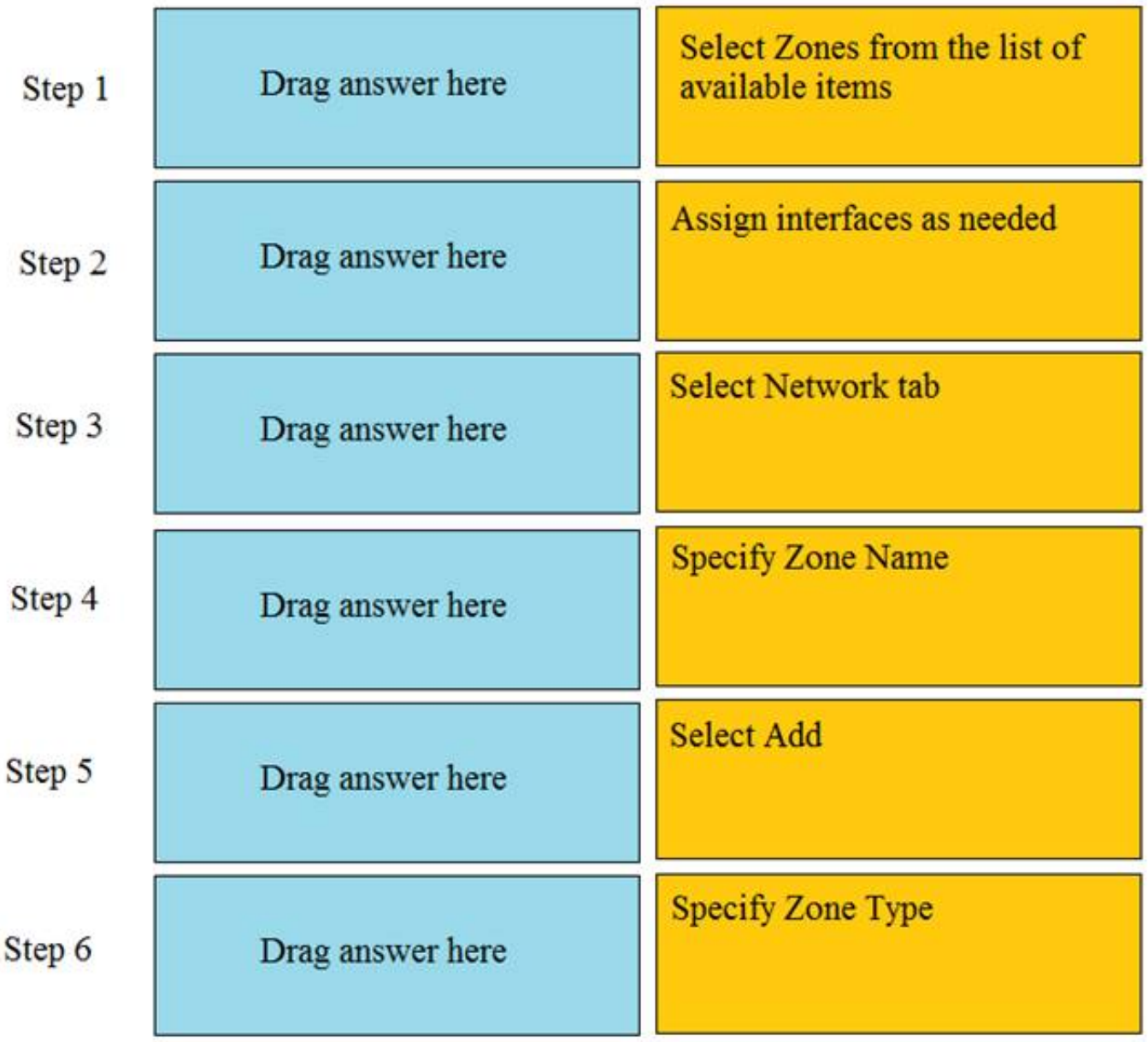
Explanation:
Weaponization and Delivery: Attackers will then determine which methods to use in order to deliver malicious payloads. Some of the methods they might utilize are automated tools, such as exploit kits, spear phishing attacks with malicious links, or attachments and malvertizing.
? Gain full 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 110
Which license must an administrator acquire prior to downloading Antivirus updates for use with the firewall?

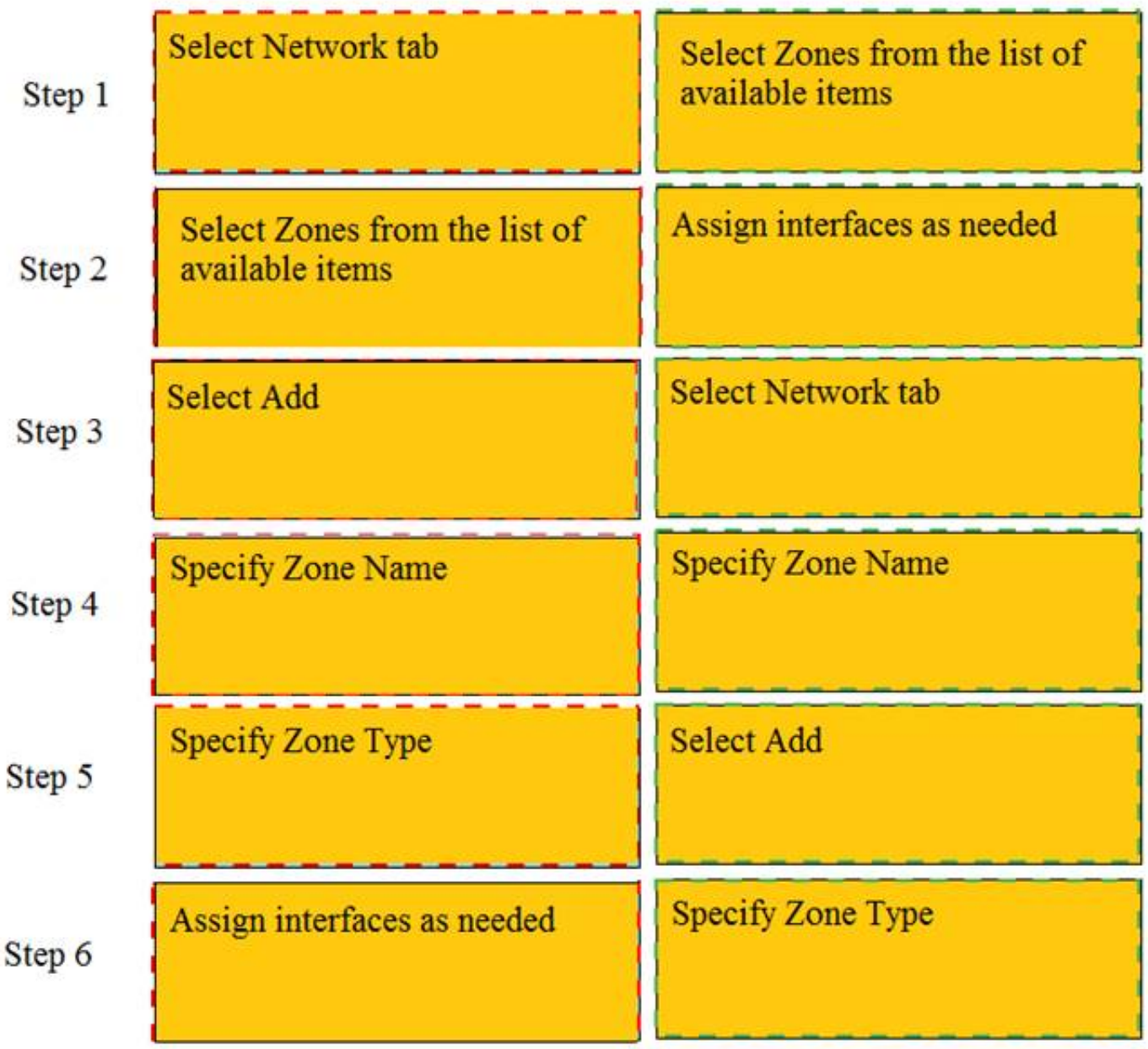
A. URL filtering
B. Antivirus
C. WildFire
D. Threat Prevention

Answer: D

NEW QUESTION 112
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 114
Which three statement describe the operation of Security Policy rules or Security Profiles? (Choose three)

Security policy rules inspect but do not block traffic.

A.
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 116
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 119
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 120
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 123
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 127
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 128
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 131
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 136
Which URL Filtering Profile action does not generate a log entry when a user attempts to access a URL?

A. override
B. allow
C. block
D. continue

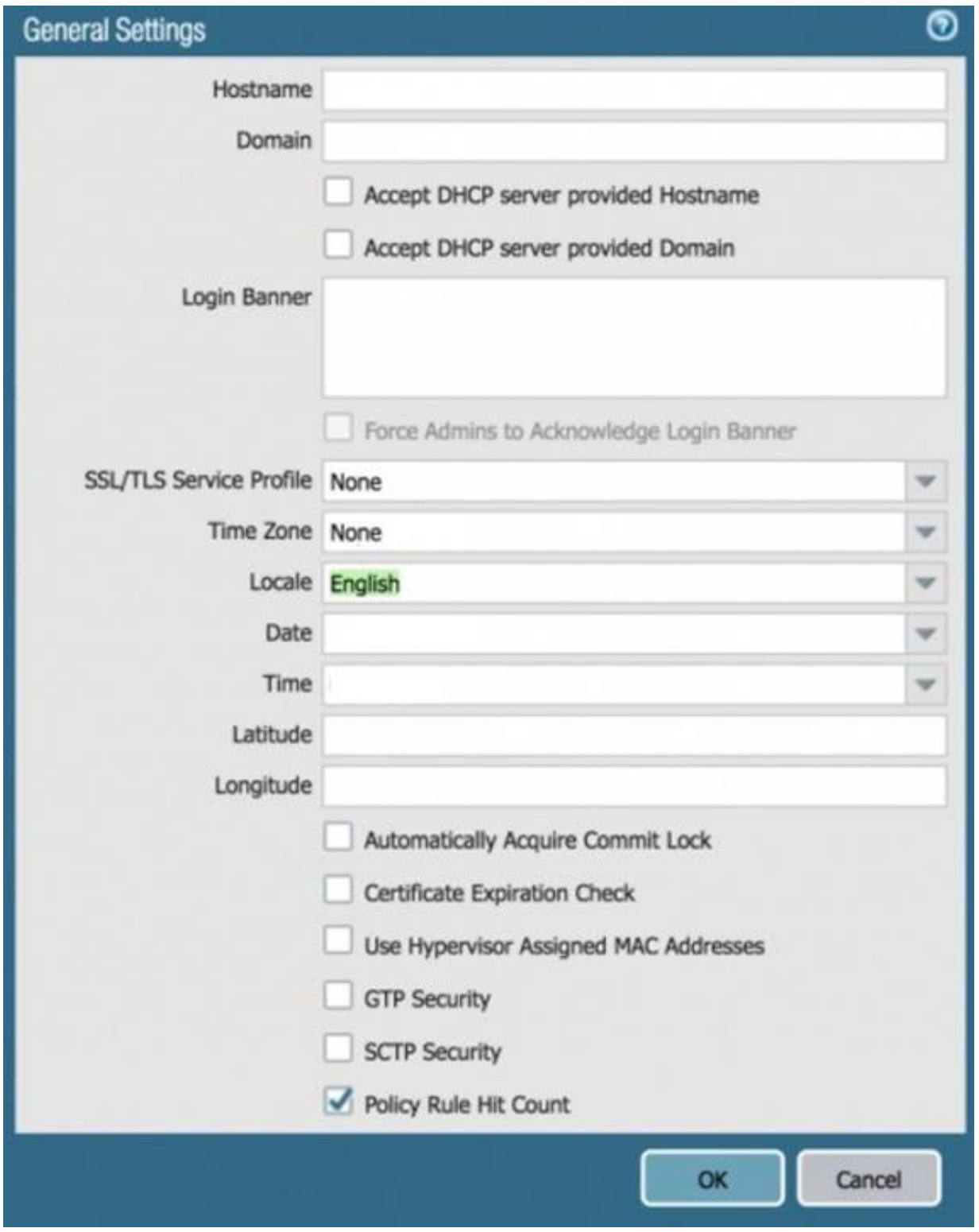
Answer: B

NEW QUESTION 139
Which interface type is part of a Layer 3 zone with a Palo Alto Networks firewall?

A. Management
B. High Availability
C. Aggregate
D. Aggregation

Answer: C

NEW QUESTION 143
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 148
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 150
If using group mapping with Active Directory Universal Groups, what must you do when configuring the User-ID?

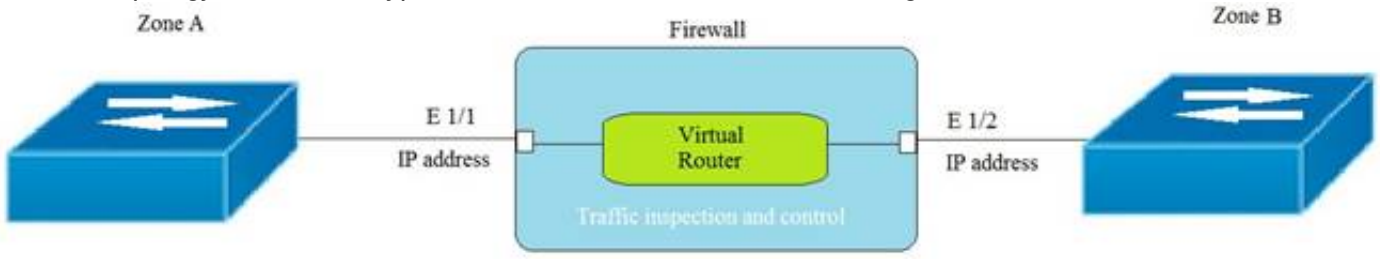
A. Create an LDAP Server profile to connect to the root domain of the Global Catalog server on port 3268 or 3269 for SSL
B. Configure a frequency schedule to clear group mapping cache
C. Configure a Primary Employee ID number for user-based Security policies
D. Create a RADIUS Server profile to connect to the domain controllers using LDAPS on port 636 or 389

Answer: B

Explanation:
? If you have Universal Groups, create an LDAP server profile to connect to the root domain of the Global Catalog server on port 3268 or 3269 for SSL, then create another LDAP server profile to connect to the root domain controllers on port 389. This helps ensure that users and group information is available for all domains and subdomains.

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

NEW QUESTION 152
Given the topology, which zone type should zone A and zone B to be configured with?



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

Answer: A

NEW QUESTION 156
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 161
An internal host wants to connect to servers of the internet through using source NAT. Which policy is required to enable source NAT on the firewall?

A. NAT policy with source zone and destination zone specified
B. post-NAT policy with external source and any destination address
C. NAT policy with no source of destination zone selected
D. pre-NAT policy with external source and any destination address

Answer: A

NEW QUESTION 163
DRAG DROP
Place the steps in the correct packet-processing order of operations.

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

A. Mastered
B. Not Mastered

Answer: A

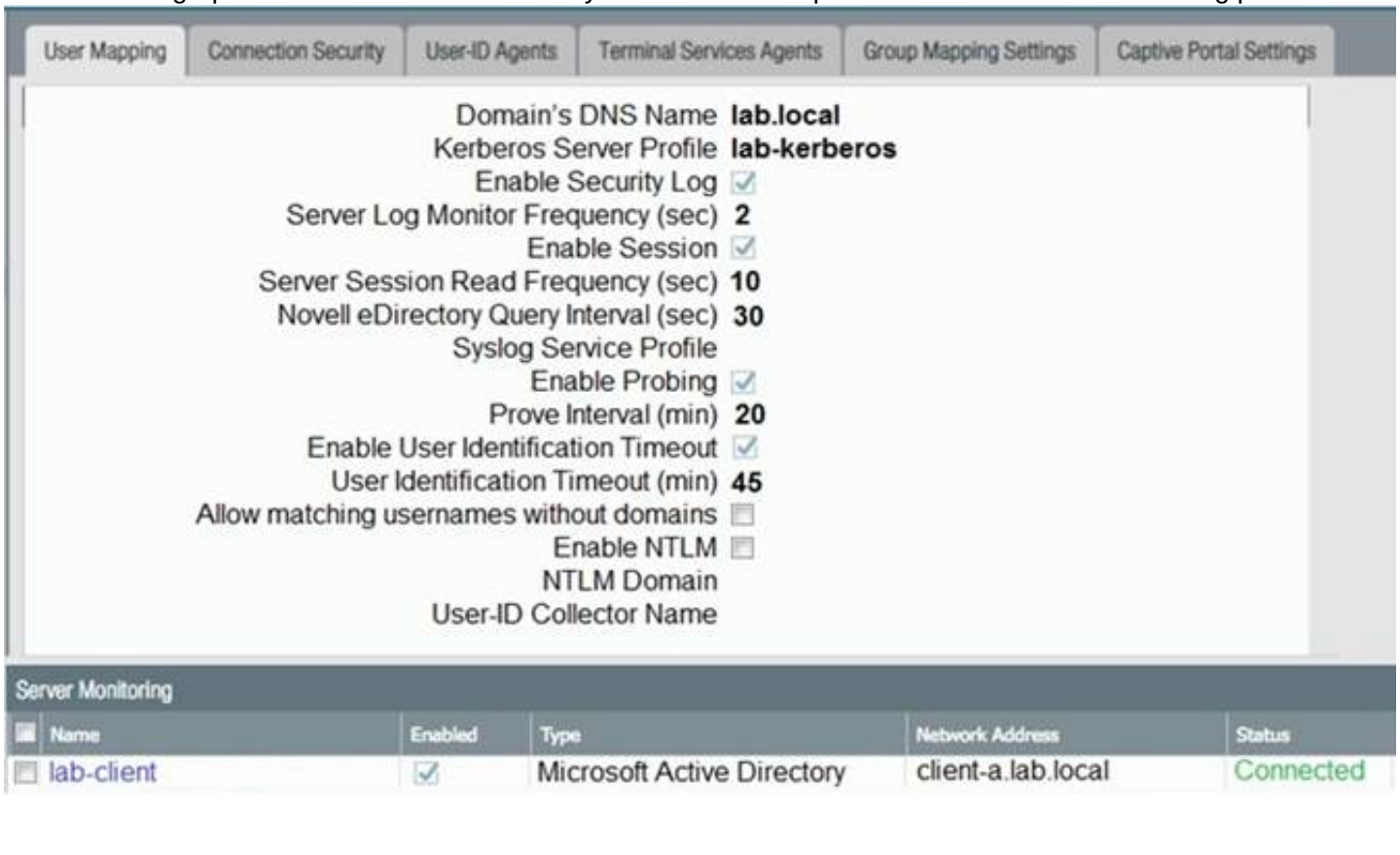
Explanation:

NEW QUESTION 168
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 173
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 178
Which statements is true regarding a Heatmap report?

A. When guided by authorized sales engineer, it helps determine te areas of greatest security risk.
B. It provides a percentage of adoption for each assessment area.
C. It runs only on firewall.
D. It provides a set of questionnaires that help uncover security risk prevention gaps across all areas of network and security architecture.

Answer: B

Explanation:
Reference:https://live.paloaltonetworks.com/t5/best-practice-assessment-blogs/the-best-practice-assessment-bpa-tool-for-ngfw-and-panorama/ba-p/248343

NEW QUESTION 182
During the packet flow process, which two processes are performed in application identification? (Choose two.)

A. pattern based application identification
B. application override policy match
C. session application identified
D. application changed from content inspection

Answer: AB

Explanation:
Reference:http://live.paloaltonetworks.com//t5/image/serverpage/image- id/12862i950F549C7D4E6309

NEW QUESTION 186
Which Security profile can you apply to protect against malware such as worms and Trojans?

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

Answer: B

Explanation:
Reference:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/security- profiles#:~:text=Antivirus%
20profiles%20protect%20against%20viruses,as%20well%20as%20spyware%20downloads

NEW QUESTION 187
The CFO found a USB drive in the parking lot and decide to plug it into their corporate laptop. The USB drive had malware on it that loaded onto their computer

and then contacted a known command and control (CnC) server, which ordered the infected machine to begin Exfiltrating data from the laptop.
Which security profile feature could have been used to prevent the communication with the CnC server?

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

Answer: A

Explanation:

NEW QUESTION 190
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

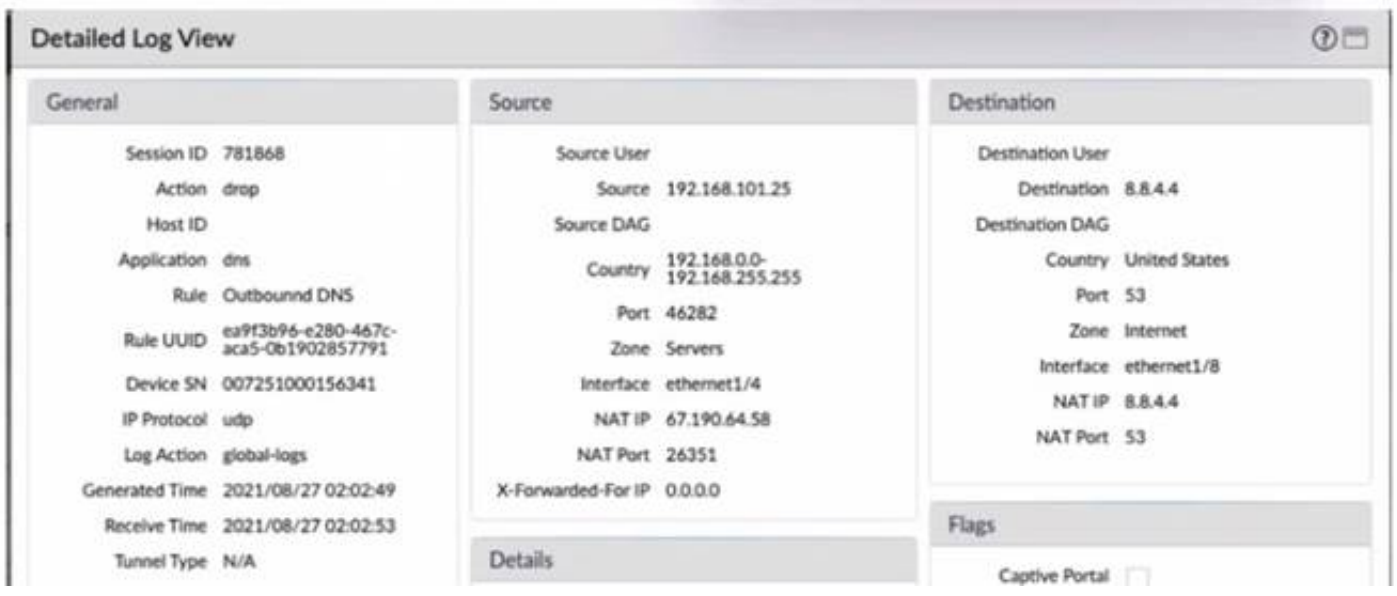
Answer: A

NEW QUESTION 191
Which interface type can use virtual routers and routing protocols?

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

Answer: B

NEW QUESTION 192
Given the detailed log information above, what was the result of the firewall traffic inspection?



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

Answer: B

NEW QUESTION 197
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 198
Which type of security rule will match traffic between the Inside zone and Outside zone, within the Inside zone, and within the Outside zone?

A. global

B. intrazone
C. interzone
D. universal

Answer: D

Explanation:

00ClomCAC

References:https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g0000

NEW QUESTION 201
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 206
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 209
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 210
An administrator needs to create a Security policy rule that matches DNS traffic within the LAN zone, and also needs to match DNS traffic within the DMZ zone
The administrator does not want to allow traffic between the DMZ and LAN zones.
Which Security policy rule type should they use?

default
A
B: universal
C. intrazone
D. interzone

Answer: C

NEW QUESTION 212
Which three configuration settings are required on a Palo Alto networks firewall management interface?

A. default gateway
B. netmask
C. IP address
D. hostname
E. auto-negotiation

Answer: ABC

Explanation:

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

NEW QUESTION 213
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 217
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 222
Which tab would an administrator click to create an address object?

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

Answer: D

NEW QUESTION 226
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 229
Which Security profile would you apply to identify infected hosts on the protected network uwall user database?

A. Anti-spyware
B. Vulnerability protection
C. URL filtering
D. Antivirus

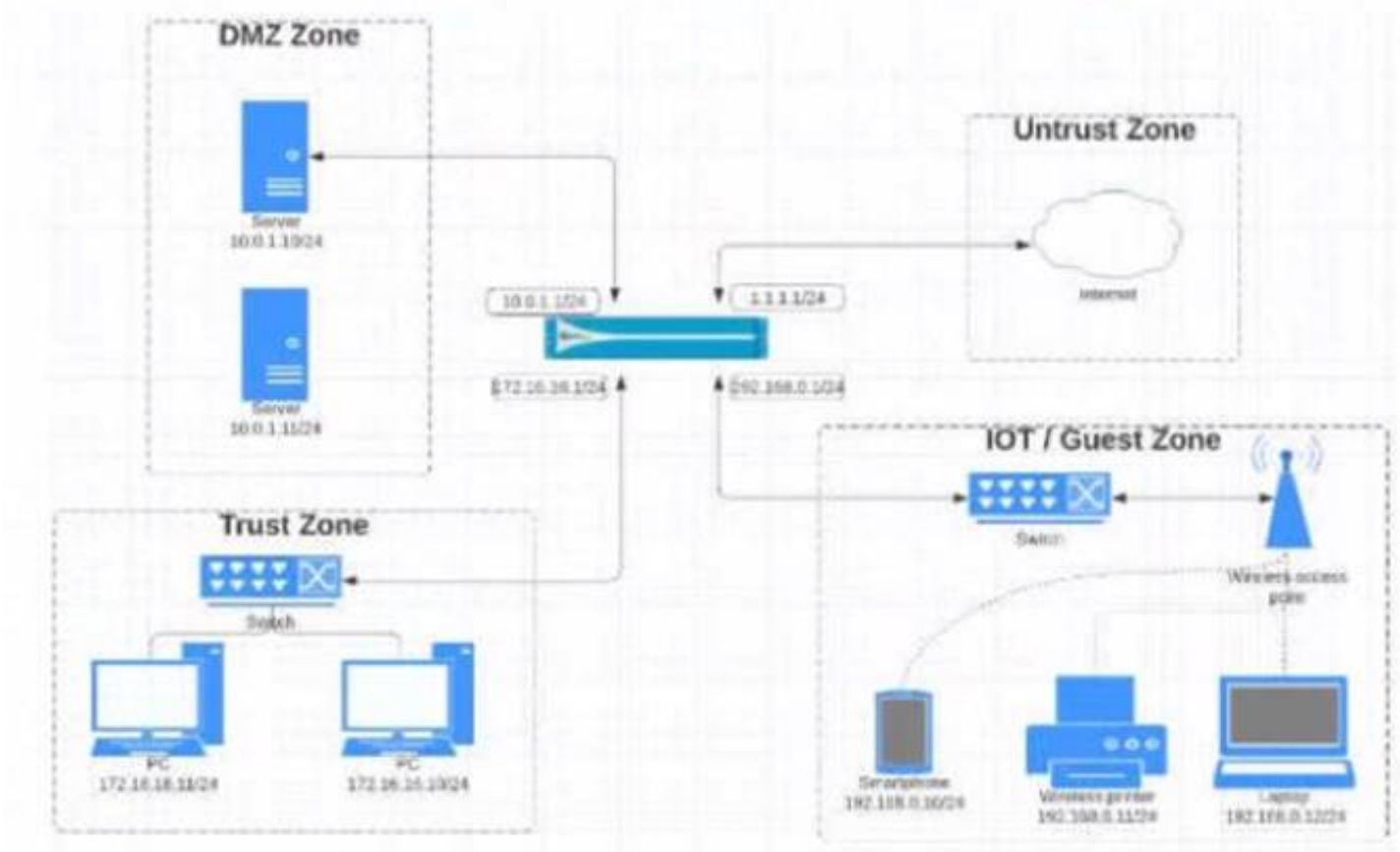
Answer: A

NEW QUESTION 231
Which service protects cloud-based applications such as Dropbox and Salesforce by administering permissions and scanning files for sensitive information?

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

Answer: C

NEW QUESTION 235
View the diagram.



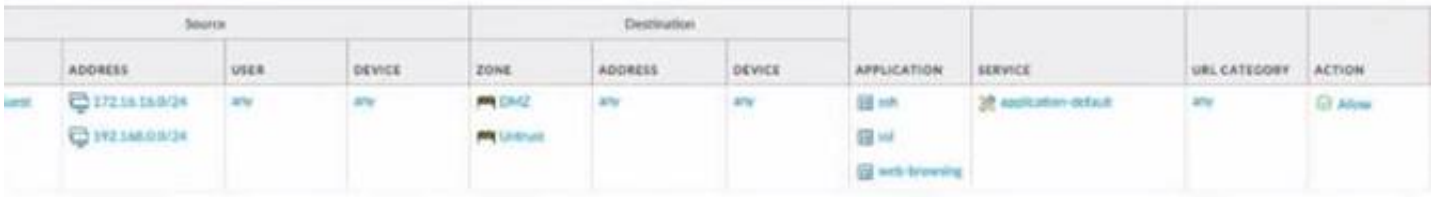
What is the most restrictive yet fully functional rule to allow general Internet and SSH traffic into both the DMZ and Untrust/Internet zones from each of the lOT/Guest and Trust Zones?

A)

B)

C)

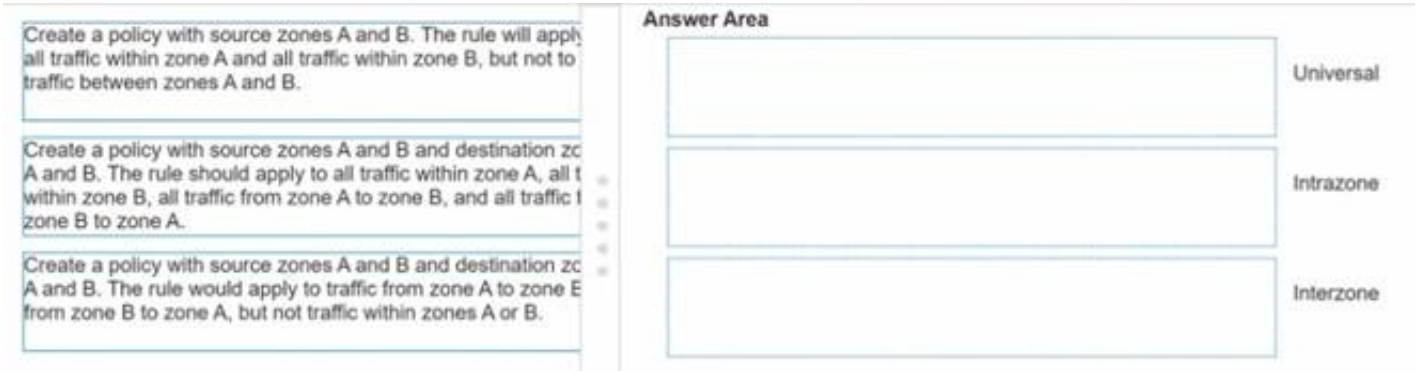
D)



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

Answer: C

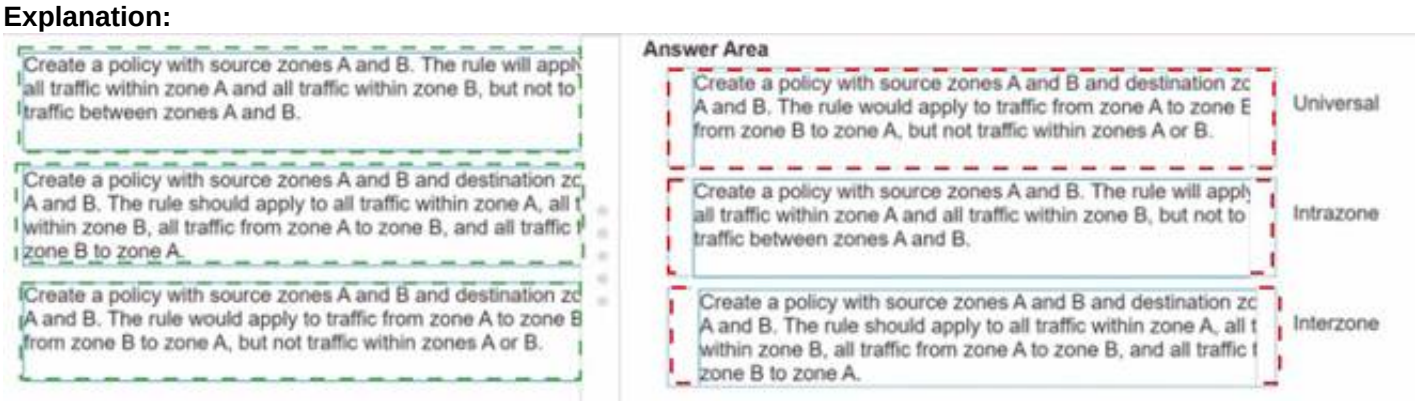
NEW QUESTION 237
DRAG DROP
Match each rule type with its example



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 241
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 244
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 245
An administrator needs to allow users to use their own office applications. How should the administrator configure the firewall to allow multiple applications in a dynamic environment?

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 246
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 247
In a File Blocking profile, which two actions should be taken to allow file types that support critical apps? (Choose two.)

A. Clone and edit the Strict profile.
B. Use URL filtering to limit categories in which users can transfer files.
C. Set the action to Continue.
D. Edit the Strict profile.

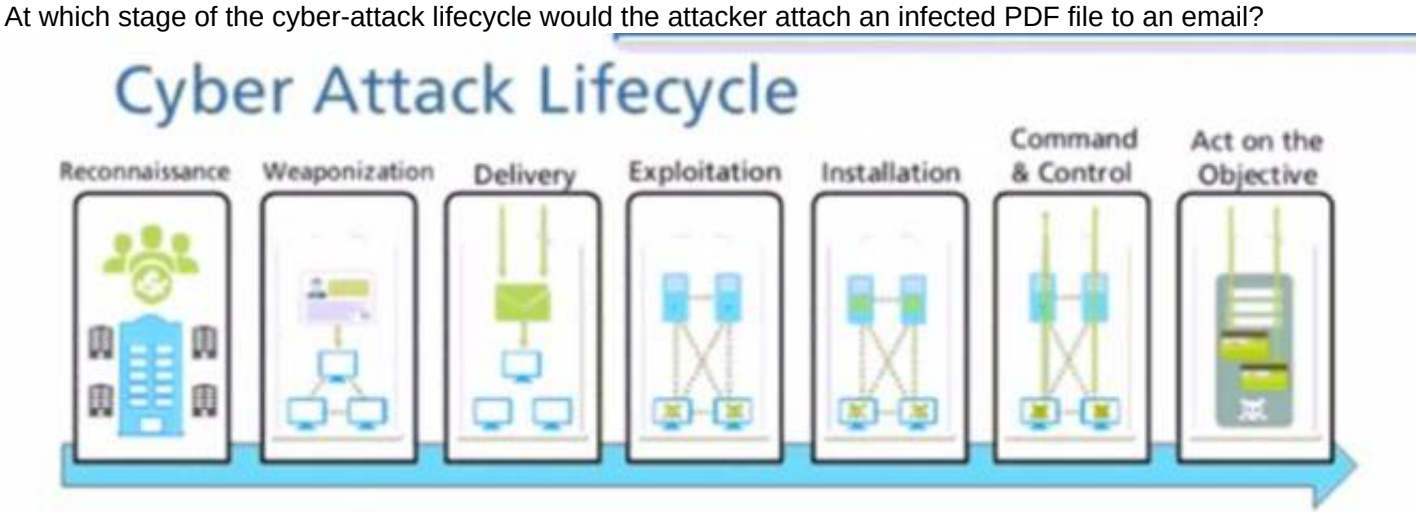
Answer: AD

NEW QUESTION 252
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 253
At which stage of the cyber-attack lifecycle would the attacker attach an infected PDF file to an email?



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

Answer: A

NEW QUESTION 258
Which objects would be useful for combining several services that are often defined together?

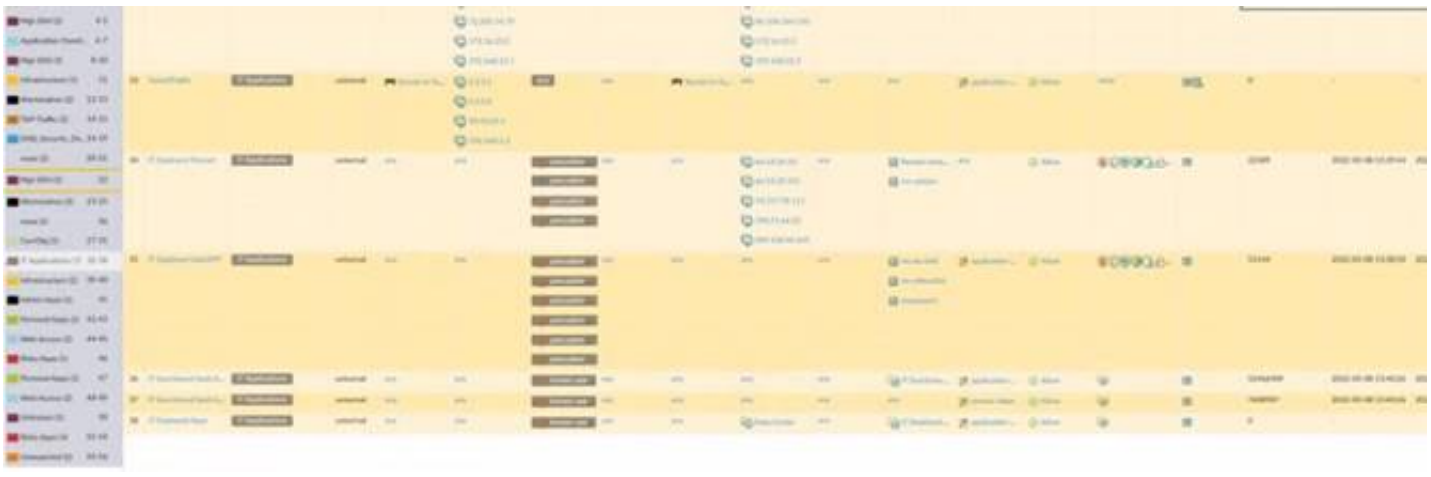
A. shared service objects
B. service groups
C. application groups
D. application filters

Answer: B

Explanation:

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

NEW QUESTION 262
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 264
To what must an interface be assigned before it can process traffic?

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

Answer: A

NEW QUESTION 269
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 271
An administrator would like to apply a more restrictive Security profile to traffic for file sharing applications. The administrator does not want to update the Security policy or object when new applications are released.
Which object should the administrator use as a match condition in the Security policy?

A. the Content Delivery Networks URL category
B. the Online Storage and Backup URL category
C. an application group containing all of the file-sharing App-IDs reported in the traffic logs
D. an application filter for applications whose subcategory is file-sharing

Answer: D

NEW QUESTION 276
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 281
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 286
Which action can be set in a URL Filtering Security profile to provide users temporary access to all websites in a given category using a provided password?

A. Mastered
B. Not Mastered

Answer: A

Explanation:
The user will see a response page indicating that a password is required to allow access to websites in the given category. With this option, the security administrator or help-desk person would provide a password granting temporary access to all websites in the given category. A log entry is generated in the URL Filtering log. The Override webpage doesn't display properly on client systems configured to use a proxy server.

NEW QUESTION 288
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 293
Choose the option that correctly completes this statement. A Security Profile can block or allow traffic .

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

Answer: B

Explanation:

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

NEW QUESTION 295
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 296
Users from the internal zone need to be allowed to Telnet into a server in the DMZ zone. Complete the security policy to ensure only Telnet is allowed. Security Policy: Source Zone: Internal to DMZ Zone services “Application defaults”, and action = Allow

A. Destination IP: 192.168.1.123/24
B. Application = ‘Telnet’
C. Log Forwarding
D. USER-ID = ‘Allow users in Trusted’

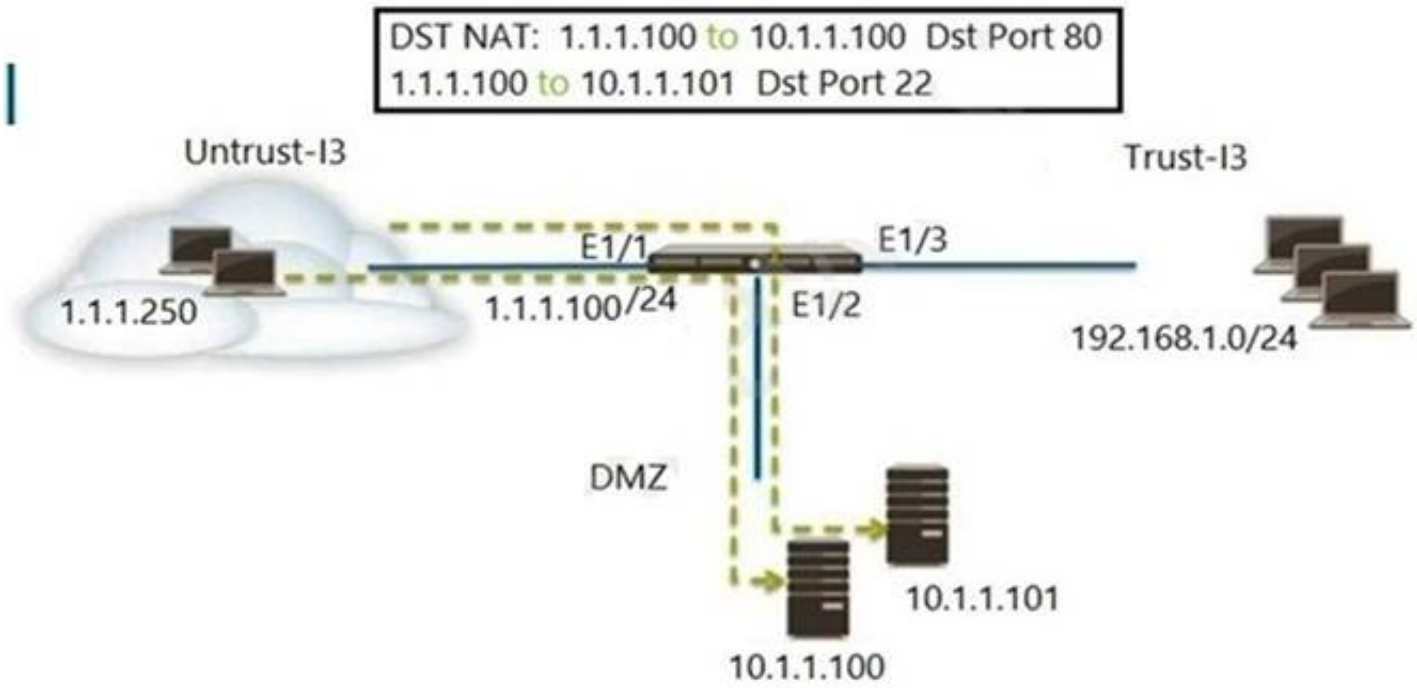
Answer: B

NEW QUESTION 299
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 304
FILL IN THE BLANK
Refer to the exhibit. An administrator is using DNAT to map two servers to a single public IP address. Traffic will be steered to the specific server based on the application, where Host A (10.1.1.100) receives HTTP traffic and Host B (10.1.1.101) receives SSH traffic.



Which two Security policy rules will accomplish this configuration? (Choose two.) A- Untrust (Any) to DMZ (1.1.1.100), ssh - Allow

A. Untrust (Any) to Untrust (10.1.1.1), web-browsing -Allow
B. Untrust (Any) to Untrust (10.1.1.1), ssh -Allow
C. Untrust (Any)to DMZ (10.1.1.100. 10.1.1.101), ssh, web-browsing-Allow
D. Untrust (Any) to DMZ (1.1.1.100), web-browsing - Allow

Answer: AE

NEW QUESTION 306
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 310

Which type of administrative role must you assign to a firewall administrator account, if the account must include a custom set of firewall permissions?

A. SAML
B. Multi-Factor Authentication
C. Role-based
D. Dynamic

Answer: C

Explanation:

Reference:https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/firewall-administration/manage-firewall-administrators/administrative-role-types.html

NEW QUESTION 311
An administrator would like to override the default deny action for a given application and instead would like to block the traffic and send the ICMP code "communication with the destination is administratively prohibited"
Which security policy action causes this?

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

Answer: B

NEW QUESTION 316
Which two features can be used to tag a user name so that it is included in a dynamic user group? (Choose two)

A. XML API
B. log forwarding auto-tagging
C. GlobalProtect agent
D. User-ID Windows-based agent

Answer: AD

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

NEW QUESTION 319
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 321
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 325
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.)

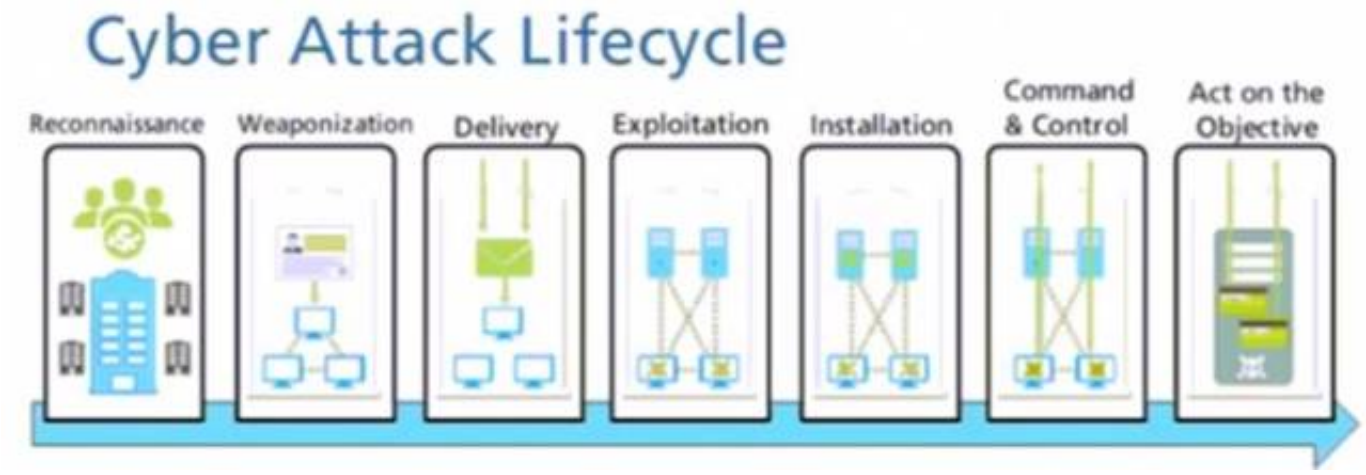
A. Add all the URLs from the gambling category except powerball.com to the block list and then set the action for the gambling category to allow.
B. Manually remove powerball.com from the gambling URL category.
C. Add *.powerball.com to the allow list
D. Create a custom URL category called PowerBall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

Answer: CD

Explanation:

NEW QUESTION 329

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



Exploitation

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

Answer: A

NEW QUESTION 331
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 333
An administrator is configuring a NAT rule
At a minimum, which three forms of information are required? (Choose three.)

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

Answer: BDE

NEW QUESTION 336
Which two firewall components enable you to configure SYN flood protection thresholds? (Choose two.)

A. QoS profile
B. DoS Protection profile
C. Zone Protection profile
D. DoS Protection policy

Answer: BC

Explanation:

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

NEW QUESTION 338
Which statement is true regarding a Prevention Posture Assessment?

A. The Security Policy Adoption Heatmap component filters the information by device groups, serial numbers, zones, areas of architecture, and other categories
B. It provides a set of questionnaires that help uncover security risk prevention gaps across all areas of network and security architecture
C. It provides a percentage of adoption for each assessment area
D. It performs over 200 security checks on Panorama/firewall for the assessment

Answer: B

NEW QUESTION 339
Access to which feature requires PAN-OS Filtering licens?

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

D. DNS Security

Answer: A

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

NEW QUESTION 341
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 343
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 345
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 350
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 353
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 358
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 359
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 360
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 363
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 366
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 370
Which administrator type utilizes predefined roles for a local administrator account?

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

Answer: C

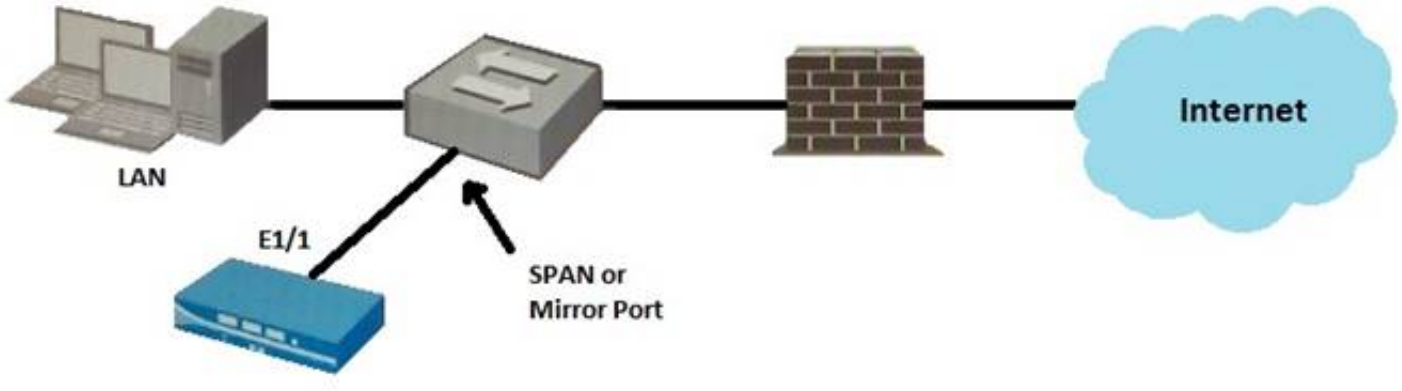
NEW QUESTION 372
An administrator is troubleshooting traffic that should match the interzone-default rule. However, the administrator doesn't see this traffic in the traffic logs on the firewall. The interzone-default was never changed from its default configuration.
Why doesn't the administrator see the traffic?

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

Answer: A

NEW QUESTION 374

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 377

Based on the screenshot what is the purpose of the group in User labelled "it"?

	Name	Type	Source Zone	Source Address	Source User	Destination Zone	Destination Address	Application
1	allow-it	universal	inside	any	it	dmz	any	it-tools

A. Allows users to access IT applications on all ports
B. Allows users in group "DMZ" lo access IT applications
C. Allows "any" users to access servers in the DMZ zone
D. Allows users in group "it" to access IT applications

Answer: D

NEW QUESTION 378

.....

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