Exam Questions PCNSA

Palo Alto Networks Certified Network Security Administrator

https://www.2passeasy.com/dumps/PCNSA/

NEW QUESTION 1
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 2
Which operations are allowed when working with App-ID application tags?

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

Answer: B

NEW QUESTION 3
Which Security profile would you apply to identify infected hosts on the protected network using DNS traffic?

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

Answer: C

Explanation:

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

Answer Area

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

Answer:

Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 6
Which action related to App-ID updates will enable a security administrator to view the existing security policy rule that matches new application signatures?

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

Answer: A

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

NEW QUESTION 7

Which two configuration settings shown are not the default? (Choose two.)

Palo Alto Networks User-ID Agent Setup

Enable Security Log ✓
Server Log Monitor Frequency (sec) **15**
Enable Session ✓
Server Session Read Frequency (sec) **10**
Novell eDirectory Query Interval (sec) **30**
Syslog Service Profile
Enable Probing
Probe Interval (min) **20**
Enable User Identification Timeout ✓
User Identification Timeout (min) **45**
Allow matching usernames without domains
Enable NTLM
NTLM Domain
User-ID Collector Name

A. Enable Security Log
B. Server Log Monitor Frequency (sec)
C. Enable Session
D. Enable Probing

Answer: BC

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

A. Policy Optimizer can display which Security policies have not been used in the last 90 days
B. Policy Optimizer on a VM-50 firewall can display which Layer 7 App-ID Security policies have unused applications

C. Policy Optimizer can add or change a Log Forwarding profile for each Security policy selected
D. Policy Optimizer can be used on a schedule to automatically create a disabled Layer 7 App-ID Security policy for every Layer 4 policy that exists Admins can then manually enable policies they want to keep and delete ones they want to remove

Answer: B

NEW QUESTION 9
What 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 10
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 10
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 14
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 19

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 20

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 25

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

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

Answer: B

NEW QUESTION 28

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 33

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 36

Which data-plane processor layer of the graphic shown provides uniform matching for spyware and vulnerability exploits on a Palo Alto Networks Firewall?
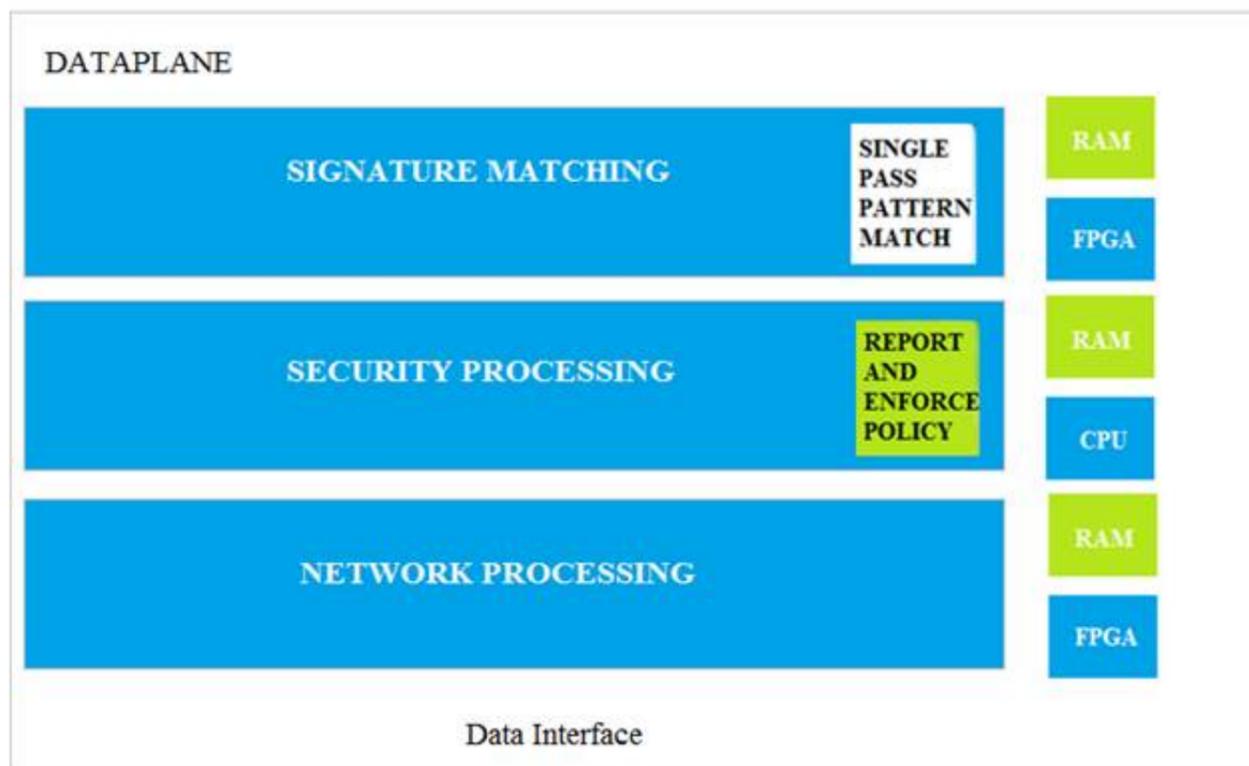
A. Signature Matching
B. Network Processing
C. Security Processing
D. Security Matching

Answer: A

NEW QUESTION 38
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 40
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 44
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 47
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 48
Based on the graphic which statement accurately describes the output shown in the server monitoring panel?

User Mapping	Connection Security	User-ID Agents	Terminal Services Agents	Group Mapping Settings	Captive Portal Settings

Domain's DNS Name	**lab.local**
Kerberos Server Profile	**lab-kerberos**
Enable Security Log	☑
Server Log Monitor Frequency (sec)	**2**
Enable Session	☑
Server Session Read Frequency (sec)	**10**
Novell eDirectory Query Interval (sec)	**30**
Syslog Service Profile	
Enable Probing	☑
Prove Interval (min)	**20**
Enable User Identification Timeout	☑
User Identification Timeout (min)	**45**
Allow matching usernames without domains	☐
Enable NTLM	☐
NTLM Domain	
User-ID Collector Name	

Server Monitoring

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

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

Answer: A

NEW QUESTION 49
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 53
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 55
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 58
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 60
The Palo Alto Networks NGFW was configured with a single virtual router named VR-1 What changes are required on VR-1 to route traffic between two interfaces on the NGFW?

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

Answer: D

Explanation:

NEW QUESTION 61
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 62
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:

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

00ClomCAC

NEW QUESTION 67
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 70
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 74
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 75
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 80
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 84
What is a recommended consideration when deploying content updates to the firewall from Panorama?

A. Before deploying content updates, always check content release version compatibility.
B. Content updates for firewall A/P HA pairs can only be pushed to the active firewall.
C. Content updates for firewall A/A HA pairs need a defined master device.
D. After deploying content updates, perform a commit and push to Panorama.

Answer: D

Explanation:
Reference:https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/manage-licenses-and-updates/deploy-updates-to-firewalls-log-collectors-and-wildfire-appliances-using-panorama/schedule-a-content-update-using-panorama.html

NEW QUESTION 86
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 90
Which link in the web interface enables a security administrator to view the security policy rules that match new application signatures?

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

Answer: D

Explanation:

NEW QUESTION 93
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 96
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 100
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 104
In which section of the PAN-OS GUI does an administrator configure URL Filtering profiles?

A̶: Policies
B̶: Network
C. Objects
D. Device

Answer: C

Explanation:
An administrator can configure URL Filtering profiles in the Objects section of the PAN-OS GUI. A URL Filtering profile is a collection of URL filtering controls that you can apply to individual Security policy rules that allow access to the internet1. You can set site access for URL categories, allow or disallow user credential submissions, enable safe search enforcement, and various other settings1.
To create a URL Filtering profile, go to Objects > Security Profiles > URL Filtering and click Add. You can then specify the profile name, description, and settings for each URL category and action2. Youcan also configure other options such as User Credential Detection, HTTP Header Insertion, and URL Filtering Inline ML2. After creating the profile, you can attach it to a Security policy rule that allows web traffic2.

NEW QUESTION 105
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 110
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 112
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 117
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 119
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 120
DRAG DROP
Place the following steps in the packet processing order of operations from first to last.
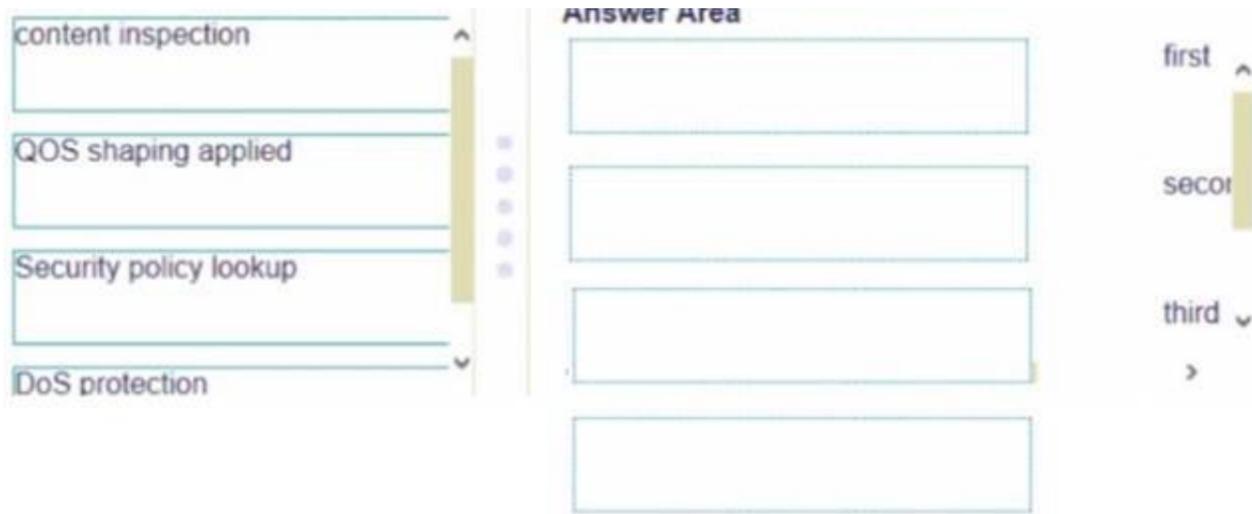
A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 124

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 125

An administrator has an IP address range in the external dynamic list and wants to create an exception for one specific IP address in this address range.
Which steps should the administrator take?

A. Add the address range to the Manual Exceptions list and exclude the IP address by selecting the entry.
adding it to the Manual Exceptions list.
B. Add each IP address in the range as a list entry and then exclude the IP address by
C. Select the address range in the List Entries list
D. A column will open with the IP addresse
E. Select the entry to exclude.
F. Add the specific IP address from the address range to the Manual Exceptions list by using regular expressions to define the entry.

Answer: D

NEW QUESTION 128

An administrator would like to protect against inbound threats such as buffer overflows and illegal code execution.
Which Security profile should be used?

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

Answer: C

NEW QUESTION 132

The firewall sends employees an application block page when they try to access Youtube. Which Security policy rule is blocking the youtube application?

	Name	Type	Source		Destination		Application	Service	URL Category	Action	Profile
			Zone	Address	Zone	Address					
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 133
Selecting the option to revert firewall changes will replace what settings?

A. The running configuration with settings from the candidate configuration
B. The candidate configuration with settings from the running configuration
C. The device state with settings from another configuration
D. Dynamic update scheduler settings

Answer: A

NEW QUESTION 135
Why should a company have a File Blocking profile that is attached to a Security policy?

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

Answer: A

NEW QUESTION 138
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 139
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 144
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?
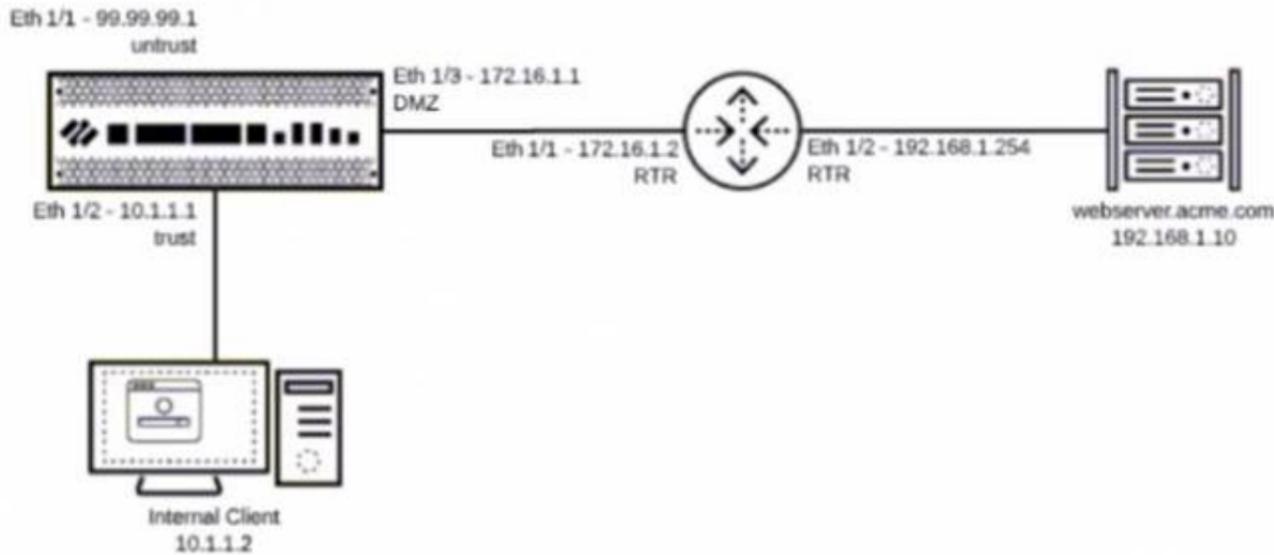
A. Add a route with the destination of 192 168 1 0/24 using interface Eth 1/3 with a next- hop of 192.168 1.10
B. Add a route with the destination of 192 168 1 0/24 using interface Eth 1/2 with a next- hop of 172.16.1.2
C. Add a route with the destination of 192 168 1 0/24 using interface Eth 1/3 with 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 148
Your company is highly concerned with their Intellectual property being accessed by unauthorized resources. There is a mature process to store and include metadata tags for all confidential documents.
Which Security profile can further ensure that these documents do not exit the corporate network?

A. File Blocking
B. Data Filtering
C. Anti-Spyware
D. URL Filtering

Answer: B

Explanation:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/objects/objects-security-profiles-data-filtering

NEW QUESTION 152
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 154
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 156
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	LOG SOURCE	ACTION	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 160

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 165
What are the two default behaviors for the intrazone-default policy? (Choose two.)

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

Answer: AB

NEW QUESTION 167
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 169
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 174
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 179
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 181
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 185

......

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual PCNSA Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the PCNSA Product From:

https://www.2passeasy.com/dumps/PCNSA/

Money Back Guarantee

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