

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 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 3

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 4

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 5

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 6

Which Palo Alto Networks security operating platform service protects cloud-based applications 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 7

Which rule type is appropriate for matching traffic both within and between the source and destination zones?

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

Answer: A

NEW QUESTION 8

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 9

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

Device SN 007251000154341	Interface ethernet1/4	NAT IP 8.8.8.4
IP Protocol udp	NAT IP 67.190.64.58	NAT Port 53
Log Action global-logs	NAT Port 24351	
Generated Time 2021/08/27 02:02:49	X-Forwarded-For IP 0.0.0.0	
Receive Time 2021/08/27 02:02:53		
Tunnel Type Null		
	Details	Flags
	Threat Type spyware	Captive Portal <input type="checkbox"/>
	Threat ID/Name Phishing:151.116.74.in-addr.arpa	Proxy Transaction <input type="checkbox"/>
	ID 109010001 (View in Threat Vault)	Decrypted <input type="checkbox"/>
	Category dns-phishing	Packet Capture <input type="checkbox"/>
	Content Version AppThreat-0-0	Client to Server <input checked="" type="checkbox"/>
	Severity low	Server to Client <input type="checkbox"/>
	Repeat Count 2	Tunnel Inspected <input type="checkbox"/>
	File Name	
	URL 151.116.74.in-addr.arpa	DeviceID
	Partial Hash 0	Source Device Category Virtual Machine
	Prap ID 0	Source Device Profile VMware
	Source UUID	Source Device Model
	Destination UUID	Source Device Vendor VMware, Inc.
	Dynamic User Group	Source Device OS Family
	Network Slice ID SST 0	Source Device OS Version
	Network Slice ID SD	Source Device Host ubuntu-server
	App Category networking	Source Device MAC 00:50:56:a2:19:a3
	App Subcategory infrastructure	Destination Device Category
	App Technology network-protocol	Destination Device Profile
	App Characteristic used by malware/hack-known-vulnerability/pervasive use	Destination Device Model
	App Container	
	App Risk 3	

- 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 10

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 10

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

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

Answer: A

Explanation:

To block hosts that use bulletproof hosts to provide malicious, illegal, and/or unethical content, use the bulletproof IP address list in policy.

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-new-features/content-inspection-features/edl-for-bulletproof-isps#:~:text=A%20new%20built%2Din%20external,%2C%20illegal%2C%20and%20unethical%20content.>

NEW QUESTION 12

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

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

Answer: D

NEW QUESTION 17

How is the hit count reset on a rule?

- A. select a security policy rule, right click Hit Count > Reset
- B. with a dataplane reboot
- C. Device > Setup > Logging and Reporting Settings > Reset Hit Count
- D. in the CLI, type command reset hitcount <POLICY-NAME>

Answer: A

NEW QUESTION 18

DRAG DROP

Order the steps needed to create a new security zone with a Palo Alto Networks firewall.

Step 1	Drag answer here	Select Zones from the list of available items
Step 2	Drag answer here	Assign interfaces as needed
Step 3	Drag answer here	Select Network tab
Step 4	Drag answer here	Specify Zone Name
Step 5	Drag answer here	Select Add
Step 6	Drag answer here	Specify Zone Type

Answer:

Step 1	Select Network tab	Select Zones from the list of available items
Step 2	Select Zones from the list of available items	Assign interfaces as needed
Step 3	Select Add	Select Network tab
Step 4	Specify Zone Name	Specify Zone Name
Step 5	Specify Zone Type	Select Add
Step 6	Assign interfaces as needed	Specify Zone Type

- 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 23

If users from the Trusted zone need to allow traffic to an SFTP server in the DMZ zone, how should a Security policy with App-ID be configured?

A)

Source Zone: Trusted
 Destination Zone: DMZ
 Services: Application-Default
 Applications: SSH
 Action: Deny

B)

Source Zone: Trusted
 Destination Zone: DMZ
 Services: SSH
 Applications: Any
 Action: Allow

C)

Source Zone: Trusted
Destination Zone: DMZ
Services: SSH
Applications: Any
Action: Deny

D)

Source Zone: Trusted
Destination Zone: DMZ
Services: Application-Default
Applications: SSH
Action: Allow

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

Answer: D

NEW QUESTION 27

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 32

What is the main function of the Test Policy Match function?

- A. verify that policy rules from Expedition are valid
- B. confirm that rules meet or exceed the Best Practice Assessment recommendations
- C. confirm that policy rules in the configuration are allowing/denying the correct traffic
- D. ensure that policy rules are not shadowing other policy rules

Answer: D

NEW QUESTION 33

What does an administrator use to validate whether a session is matching an expected NAT policy?

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

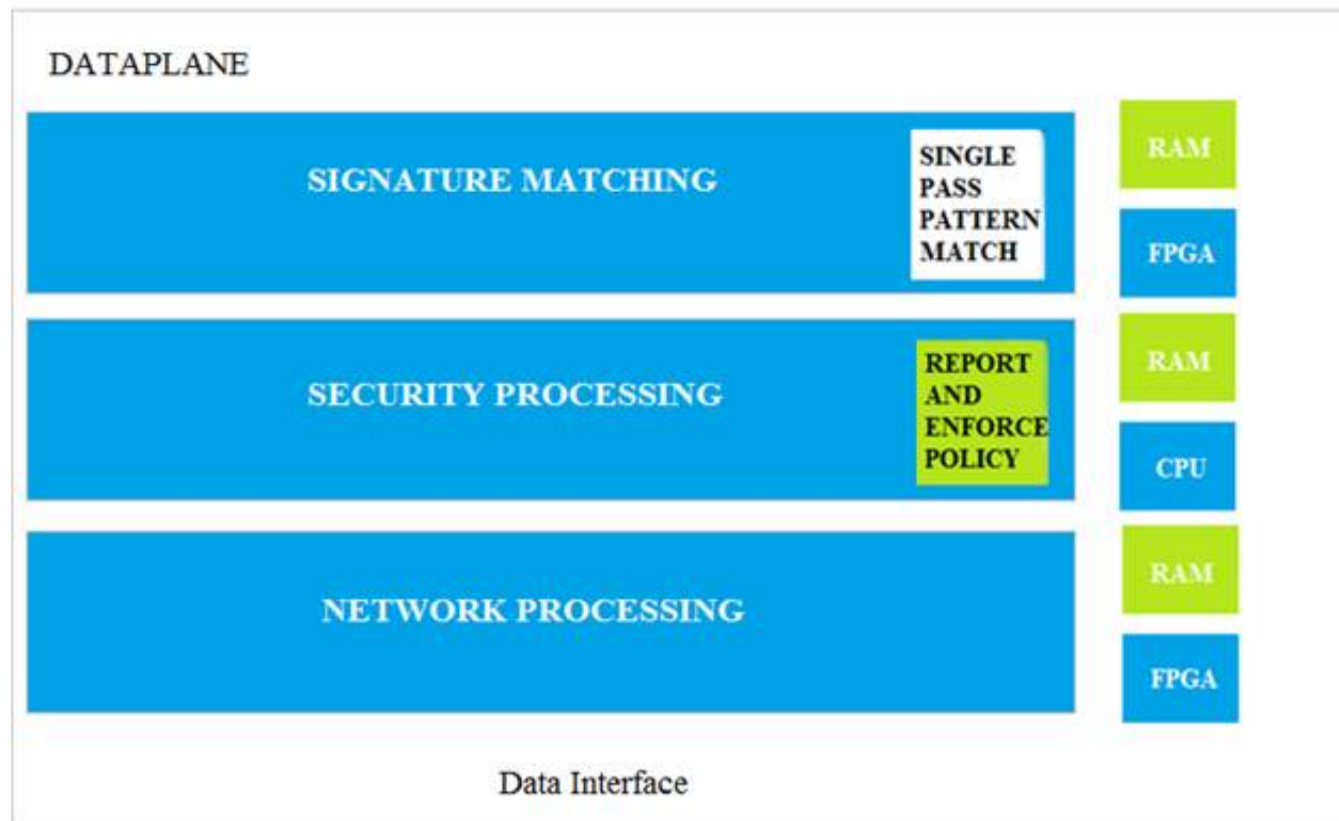
Answer: B

Explanation:

Reference: <https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g00000 0CIQSCA0>

NEW QUESTION 35

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

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 42

A server-admin in the USERS-zone requires SSH-access to all possible servers in all current and future Public Cloud environments. All other required connections have already been enabled between the USERS- and the OUTSIDE-zone. What configuration-changes should the Firewall-admin make?

- A. Create a custom-service-object called SERVICE-SSH for destination-port-TCP-22. Create a security-rule between zone USERS and OUTSIDE to allow traffic from any source IP-address to any destination IP-address for SERVICE-SSH
- B. Create a security-rule that allows traffic from zone USERS to OUTSIDE to allow traffic from any source IP-address to any destination IP-address for application SSH
- C. In addition to option a, a custom-service-object called SERVICE-SSH-RETURN that contains source-port-TCP-22 should be create
- D. A second security-rule is required that allows traffic from zone OUTSIDE to USERS for SERVICE-SSH-RETURN for any source- IP-address to any destination- Ip-address
- E. In addition to option c, an additional rule from zone OUTSIDE to USERS for application SSH from any source-IP-address to any destination-IP-address is required to allow the return-traffic from the SSH-servers to reach the server-admin

Answer: B

NEW QUESTION 46

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 48

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 51

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 architecture.

all areas of network and security

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 53

Based on the screenshot what is the purpose of the included groups?

	Name	Type	Source			Destination		Application	Service	Action
			Zone	Address	User	Zone	Address			
1	allow-it	universal	inside	any	it	dmz	any	it-tools	application-default	Allow

- A. They are only groups visible based on the firewall's credentials.
- B. They are used to map usernames to group names.
- C. They contain only the users you allow to manage the firewall.
- D. They are groups that are imported from RADIUS authentication servers.

Answer: B

Explanation:

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

NEW QUESTION 56

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 60

Which definition describes the guiding principle of the zero-trust architecture?

- A. never trust, never connect
- B. always connect and verify
- C. never trust, always verify
- D. trust, but verify

Answer: C

Explanation:

Reference:
<https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture>

NEW QUESTION 63

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 67

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

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

Answer: D

Explanation:

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

NEW QUESTION 72

During the App-ID update process, what should you click on to confirm whether an existing policy rule is affected by an App-ID update?

- A. check now
- B. review policies
- C. test policy match
- D. download

Answer: B

Explanation:

Reference:<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/app-id/manage-new-app-ids-introduced-in-content-releases/review-new-app-id-impact-on-existing-policy-rules>

NEW QUESTION 74

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 78

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

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

Answer: AD

NEW QUESTION 80

An administrator would like to create a URL Filtering log entry when users browse to any gambling website. What combination of Security policy and Security profile actions is correct?

Security policy = drop, Gambling category in URL profile = allow

- ~~A~~: Security policy = den
- C. Gambling category in URL profile = block
- D. Security policy = allow, Gambling category in URL profile = alert
- E. Security policy = allo
- F. Gambling category in URL profile = allow

Answer: C

NEW QUESTION 83

Which protocol used to map username to user groups when user-ID is configured?

- A. SAML
- B. RADIUS
- C. TACACS+
- D. LDAP

Answer: D

NEW QUESTION 86

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 90

DRAG DROP

Match each rule type with its example

Create a policy with source zones A and B. The rule will apply to all traffic within zone A and all traffic within zone B, but not to traffic between zones A and B.

Create a policy with source zones A and B and destination zone A and B. The rule should apply to all traffic within zone A, all traffic within zone B, all traffic from zone A to zone B, and all traffic from zone B to zone A.

Create a policy with source zones A and B and destination zone A and B. The rule would apply to traffic from zone A to zone B, from zone B to zone A, but not traffic within zones A or B.

Answer Area

Universal

Intrazone

Interzone

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Create a policy with source zones A and B. The rule will apply to all traffic within zone A and all traffic within zone B, but not to traffic between zones A and B.

Create a policy with source zones A and B and destination zone A and B. The rule should apply to all traffic within zone A, all traffic within zone B, all traffic from zone A to zone B, and all traffic from zone B to zone A.

Create a policy with source zones A and B and destination zone A and B. The rule would apply to traffic from zone A to zone B, from zone B to zone A, but not traffic within zones A or B.

Answer Area

Create a policy with source zones A and B and destination zone A and B. The rule would apply to traffic from zone A to zone B, from zone B to zone A, but not traffic within zones A or B.

Create a policy with source zones A and B. The rule will apply to all traffic within zone A and all traffic within zone B, but not to traffic between zones A and B.

Create a policy with source zones A and B and destination zone A and B. The rule should apply to all traffic within zone A, all traffic within zone B, all traffic from zone A to zone B, and all traffic from zone B to zone A.

Universal

Intrazone

Interzone

NEW QUESTION 94

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

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

Answer: D

NEW QUESTION 97

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 100

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 102

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

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

Answer: A

Explanation:

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

NEW QUESTION 107

In the example security policy shown, which two websites fcked? (Choose two.)

	Name	Tags	Zone	Address	Zone	Address	Application	Service	URL Category	Action	Profile
1	Block-Sites	outbound	inside	Any	Outside	Any	Any	any	Social-networking	Deny	None

- A. LinkedIn
- B. Facebook
- C. YouTube
- D. Amazon

Answer: AB

NEW QUESTION 109

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 114

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 115

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

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

Answer: BD

NEW QUESTION 120

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 123

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 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 127

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

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

Answer: B

Explanation:

Reference:

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

NEW QUESTION 128

Which statement best describes a common use of Policy Optimizer?

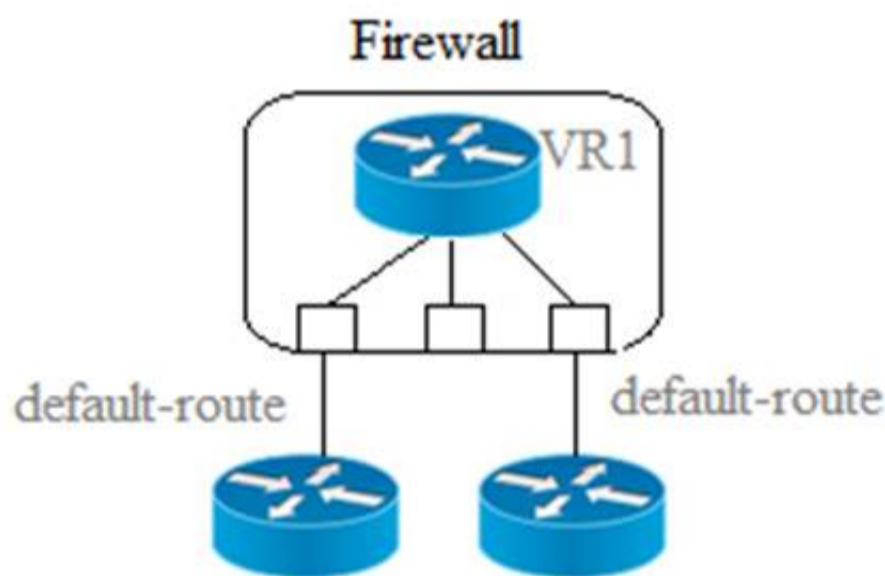
- A. Policy Optimizer on a VM-50 firewall can display which Layer 7 App-ID Security policies have unused applications.
- B. Policy Optimizer can add or change a Log Forwarding profile for each Security policy selected.
- C. Policy Optimizer can display which Security policies have not been used in the 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 132

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

Multiple Static Default Routes



Path monitoring does not determine if route is useable

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

Answer: CD

NEW QUESTION 134

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 138

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

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

Answer: BD

NEW QUESTION 139

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 144

Why does a company need an Antivirus profile?

- A. Mastered
- B. Not Mastered

Answer: A

NEW QUESTION 149

A website is unexpectedly allowed due to miscategorization.

What are two ways to resolve this issue for a proper response? (Choose two.)

- A. Identify the URL category being assigned to the website.Edit the active URL Filtering profile and update that category's site access settings to block.
- B. Create a URL category and assign the affected URL.Update the active URL Filtering profile site access setting for the custom URL category to block.
- C. Review the categorization of the website on <https://urlfiltering.paloaltonetworks.co>
- D. Submit for "request change", identifying the appropriate categorization, and wait for confirmation before testing again.
- E. Create a URL category and assign the affected URL.Add a Security policy with a URL category qualifier of the custom URL category below the original polic
- F. Set the policy action to Deny.

Answer: CD

NEW QUESTION 153

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 155

When is the content inspection performed in the packet flow process?

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

Answer: A

Explanation:

Reference:<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g0000000CIVHCA0>

NEW QUESTION 157

Which component is a building block in a Security policy rule?

- A. decryption profile
- B. destination interface
- C. timeout (min)
- D. application

Answer: D

Explanation:

Reference:

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/policies/policies-security/buildingblocks-in-a-security-policy-rule.html>

NEW QUESTION 158

Which firewall feature do you need to configure to query Palo Alto Networks service updates over a data-plane interface instead of the management interface?

- A. Data redistribution
- B. Dynamic updates
- C. SNMP setup
- D. Service route

Answer: D

NEW QUESTION 163

How frequently can wildfire updates be made available to firewalls?

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

Answer: D

NEW QUESTION 167

What must be considered with regards to content updates deployed from Panorama?

- A. Content update schedulers need to be configured separately per device group.
- B. Panorama can only install up to five content versions of the same type for potential rollback scenarios.
- C. A PAN-OS upgrade resets all scheduler configurations for content updates.
- D. Panorama can only download one content update at a time for content updates of the same type.

Answer: D

Explanation:

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

NEW QUESTION 170

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 171

In which stage of the Cyber-Attack Lifecycle would the attacker inject a PDF file within an email?

- A. Weaponization
- B. Reconnaissance
- C. Installation
- D. Command and Control
- E. Exploitation

Answer: A

NEW QUESTION 176

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

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

Allows users to access IT applications on all ports

- A: Allows users in group "DMZ" to 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 179

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions 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

100% Actual & Verified — Instant Download, Please Click
[Order The PCNSA Practice Test Here](#)