



Paloalto-Networks

Exam Questions PCNSA

Palo Alto Networks Certified Network Security Administrator

About ExamBible

Your Partner of IT Exam

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1

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 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 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 4

Which attribute can a dynamic address group use as a filtering condition to determine its membership?

- A. tag
- B. wildcard mask
- C. IP address
- D. subnet mask

Answer: A

Explanation:

Dynamic Address Groups: A dynamic address group populates its members dynamically using look ups for tags and tag-based filters. Dynamic address groups are very useful if you have an extensive virtual infrastructure where changes in virtual machine location/IP address are frequent. For example, you have a sophisticated failover setup or provision new virtual machines frequently and would like to apply policy to traffic from or to the new machine without modifying the configuration/rules on the firewall. <https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface-help/objects/objects-address-groups>

NEW QUESTION 5

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

Addresses list?

A.

destination address

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

Answer: B

Explanation:

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

NEW QUESTION 6

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

- A. Mastered
- B. Not Mastered

Answer: A

NEW QUESTION 7

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 8

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 9

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

No App Specified
 These are security policies that have no application specified and allow any application on the configured service which can present a security risk. Palo Alto Networks you convert these service only security policies to application based policies.

	Name	Service	Traffic (Bytes, 30 days)	App Usage			Compare	Modified
				Apps Allowed	Apps Seen	Days with No New Apps		
3	egress-outside	application-default	25.3G	any	8	8	Compare	2019-06-2...
1	inside-portal	any	372.6M	any	9	8	Compare	2019-06-2...

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

Answer: C

NEW QUESTION 10

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 10

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 11

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 15

An administrator would like to block access to a web server, while also preserving

resources and minimizing half-open sockets. What are two security policy actions the administrator can select? (Choose two.)

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

Answer: AC

NEW QUESTION 18

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 20

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 21

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 22

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 24

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 28

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 31

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 36

Four configuration choices are listed, and each could be used to block access to a specific URL. If you configured each choices to block the sameURL then which choice would be the last to block access to the URL?

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

The precedence is from the top down; First Match Wins: 1) Block list: Manually entered blocked URLs Objects - 2) Allow list: Manually entered allowed URLs Objects - 3) Custom URL Categories - 4) Cached Cached: URLs learned from External Dynamic Lists (EDLs) - 5) Pre-Defined Categories: PAN-DB or Brightcloud categories.

NEW QUESTION 37

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

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

Answer: C

NEW QUESTION 42

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 46

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 47

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

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

Answer: BC

NEW QUESTION 50

Which action would an administrator take to ensure that a service object will be available only to the selected device group?

- A. create the service object in the specific template
- B. uncheck the shared option
- C. ensure that disable override is selected
- D. ensure that disable override is cleared

Answer: D

Explanation:

<https://docs.paloaltonetworks.com/panorama/9-0/panorama-admin/manage-firewalls/manage-device-groups/create-objects-for-use-in-shared-or-device-group-policy>

NEW QUESTION 55

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 59

In a security policy what is the quickest way to reset 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 62

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 66

By default, which action is assigned to the interzone-default rule?

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

Answer: C

NEW QUESTION 70

Given the Cyber-Attack Lifecycle diagram, identify the stage in which the attacker can initiate malicious code against a targeted machine.



- A.

Exploitation

- B. Installation
- C. Reconnaissance
- D. Act on Objective

Answer: A

NEW QUESTION 73

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

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

Answer: B

NEW QUESTION 76

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 80

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 81

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 86

Which two statements are correct about App-ID content updates? (Choose two.)

- A. Updated application content may change how security policy rules are enforced
- B. After an application content update, new applications must be manually classified prior to use
- C. Existing security policy rules are not affected by application content updates
- D. After an application content update, new applications are automatically identified and classified

Answer: AD

NEW QUESTION 87

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 90

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 93

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Export Named Configuration Snapshot This option exports the current running configuration, a candidate configuration snapshot, or a previously imported configuration (candidate or running). The firewall exports the configuration as an XML file with the specified name. You can save the snapshot in any network location. These exports often are used as backups. These XML files also can be used as templates for building other firewall configurations.

NEW QUESTION 97

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

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

Answer: D

NEW QUESTION 101

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 malvertising.

? 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 106

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

- A. Mastered
- B. Not Mastered

Answer: A

NEW QUESTION 110

What allows a security administrator to preview the Security policy rules that match new application signatures?

- A. Review Release Notes
- B. Dynamic Updates-Review Policies
- C. Dynamic Updates-Review App
- D. Policy Optimizer-New App Viewer

Answer: B

Explanation:

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

NEW QUESTION 115

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

	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

any port

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

Answer: C

NEW QUESTION 118

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 121

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 122

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 123

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 128

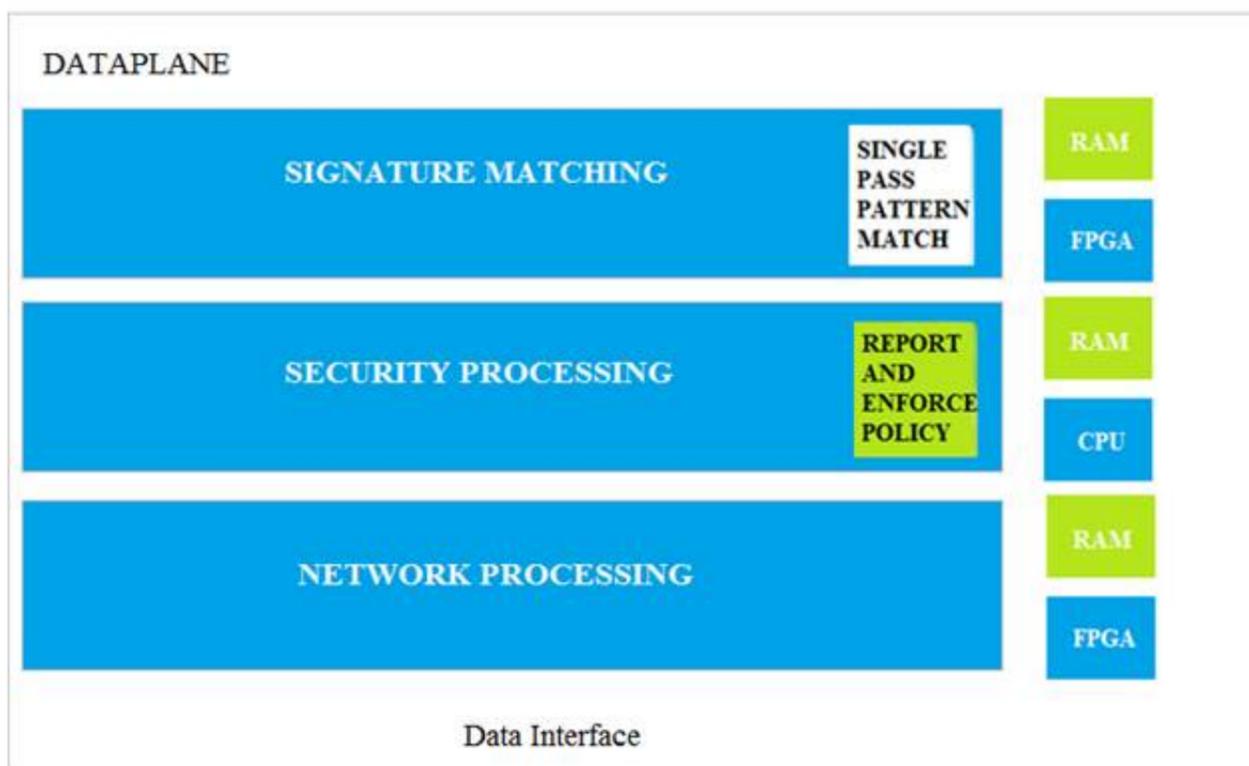
What is the minimum timeframe that can be set on the firewall to check for new WildFire signatures?

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

Answer: D

NEW QUESTION 130

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 131

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

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

Answer: ABD

NEW QUESTION 132

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 134

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 138

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 143

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 145

Which plane on a Palo alto networks firewall provides configuration logging and reporting functions on a separate processor?

- A. data
- B. network processing
- C. management

D. security processing

Answer: C

NEW QUESTION 146

The CFO found a malware infected USB drive in the parking lot, which when inserted infected their corporate laptop the malware contacted a known command-and-control server which exfiltrating corporate data.

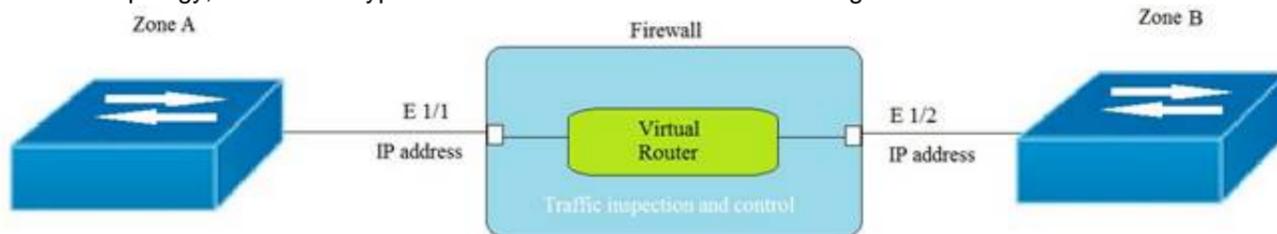
Which Security profile feature could have been used to prevent the communications with the command-and-control server?

- A. Create a Data Filtering Profile and enable its DNS sinkhole feature.
- B. Create an Antivirus Profile and enable its DNS sinkhole feature.
- C. Create an Anti-Spyware Profile and enable its DNS sinkhole feature.
- D. Create a URL Filtering Profile and block the DNS sinkhole URL category.

Answer: C

NEW QUESTION 148

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 149

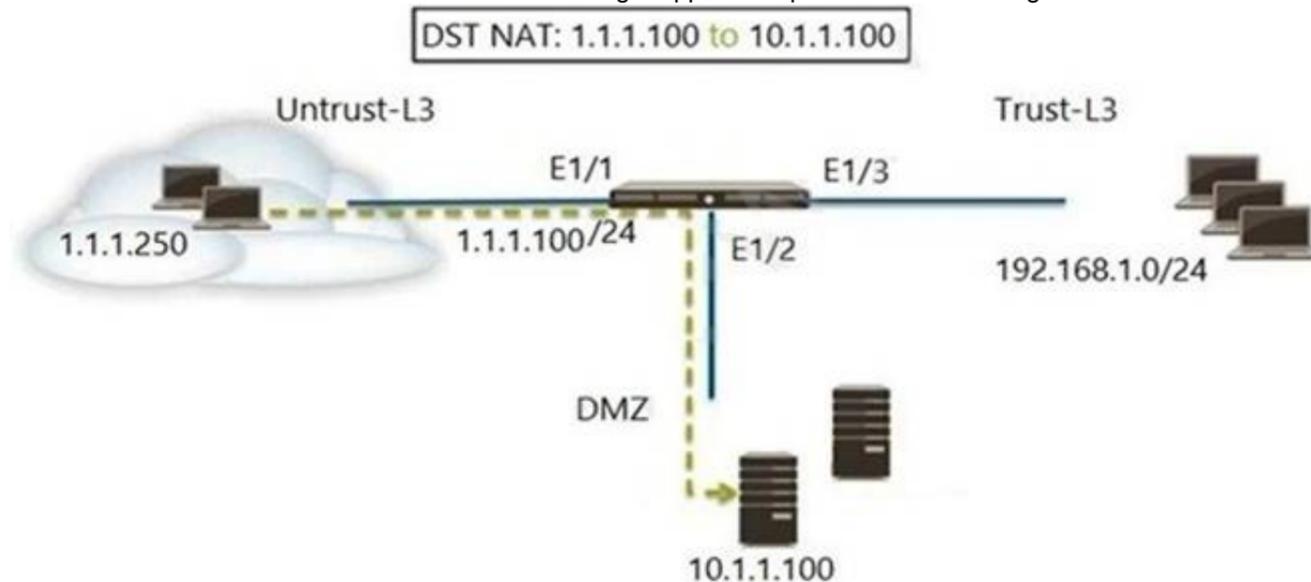
What are the requirements for using Palo Alto Networks EDL Hosting Service?

- 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 152

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



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

- A. Mastered
- B. Not Mastered

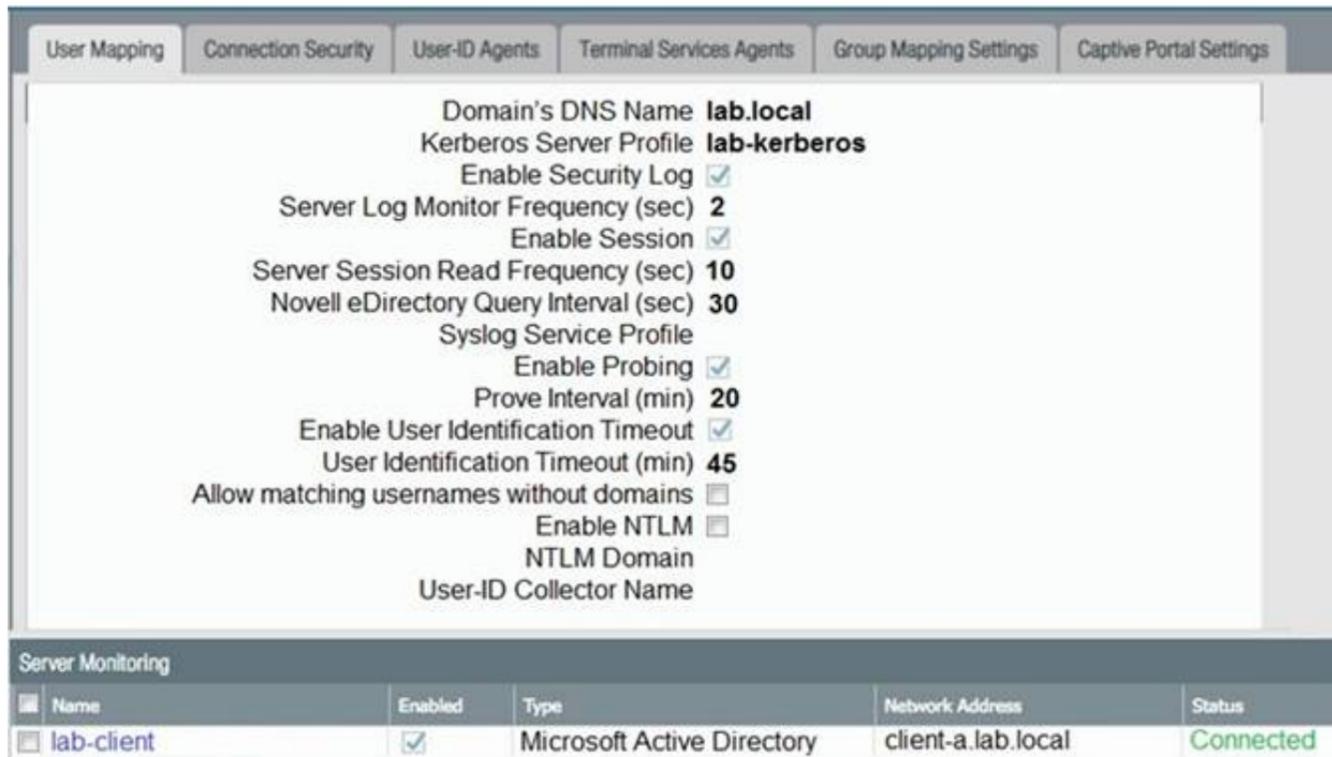
Answer: A

Explanation:

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

NEW QUESTION 157

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 160

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 165

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 166

Selecting the option to revert firewall changes will replace what settings?

- A. Mastered
- B. Not Mastered

Answer: A

NEW QUESTION 167

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 168

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

	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. 80
- B. 53
- C. 22
- D. 23

Answer: C

Explanation:

NEW QUESTION 172

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 176

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 181

What is the correct process for 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 184

Which User Credential Detection method should be applied within a URL Filtering Security profile to check for the submission of a valid corporate username and the associated password?

- A. Domain Credential
- B. IP User
- C. Group Mapping
- D. Valid Username Detected Log Severity

Answer: C

NEW QUESTION 186

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

General	Source	Destination
Session ID: 781868	Source User	Destination User
Action: drop	Source: 192.168.101.25	Destination: 8.8.4.4
Host ID	Source DAG	Destination DAG
Application: dns	Country: 192.168.0.0-192.168.255.255	Country: United States
Rule: Outbound DNS	Port: 46282	Port: 53
Rule UUID: ea9f3b96-e280-467c-aca5-0b1902857791	Zone: Servers	Zone: Internet
Device SN: 007251000156341	Interface: ethernet1/4	Interface: ethernet1/8
IP Protocol: udp	NAT IP: 67.190.64.58	NAT IP: 8.8.4.4
Log Action: global-logs	NAT Port: 26351	NAT Port: 53
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: N/A		

- 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 189

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 191

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 195

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 198

What is the main function of Policy Optimizer?

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

Answer: D

Explanation:

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

NEW QUESTION 201

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 206

What are three valid information sources that can be used when tagging users to dynamic user groups? (Choose three.)

- A. Biometric scanning results from iOS devices
- B. Firewall logs
- C. Custom API scripts
- D. Security Information and Event Management Systems (SIEMs), such as Splunk
- E. DNS Security service

Answer: BCE

NEW QUESTION 207

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 208

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?

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

Answer: C

NEW QUESTION 213

An administrator needs to allow users to use only certain email applications. How should the administrator configure the firewall to restrict users to specific email applications?

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

Answer: B

NEW QUESTION 214

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=kA10g000000CIN7CAK>

NEW QUESTION 219

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 220

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

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
- B. Gambling category in URL profile = block
- C. Security policy = allow, Gambling category in URL profile = alert
- D. Security policy = allow, Gambling category in URL profile = alert
- E. Security policy = allow
- F. Gambling category in URL profile = allow

Answer: C

NEW QUESTION 225

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 228

Which action results in the firewall blocking network traffic without notifying the sender?

Deny

- A. No notification
- B. Drop
- C. Drop
- D. Reset Client

Answer: C

NEW QUESTION 230

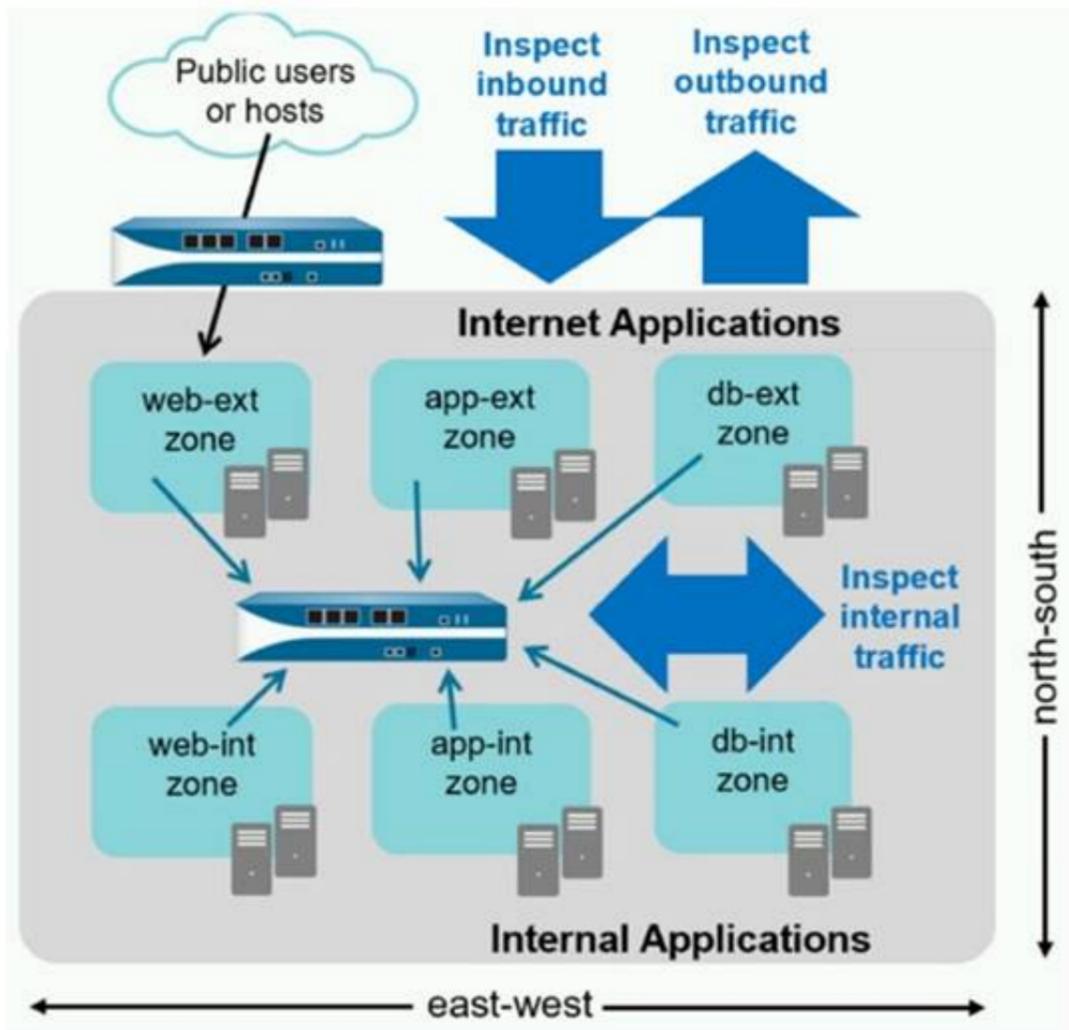
An administrator is troubleshooting traffic that should match the interzone-default rule. However, the administrator doesn't see this traffic in the traffic logs on the firewall. The interzone-default was never changed from its default configuration. Why doesn't the administrator see the traffic?

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

Answer: D

NEW QUESTION 232

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

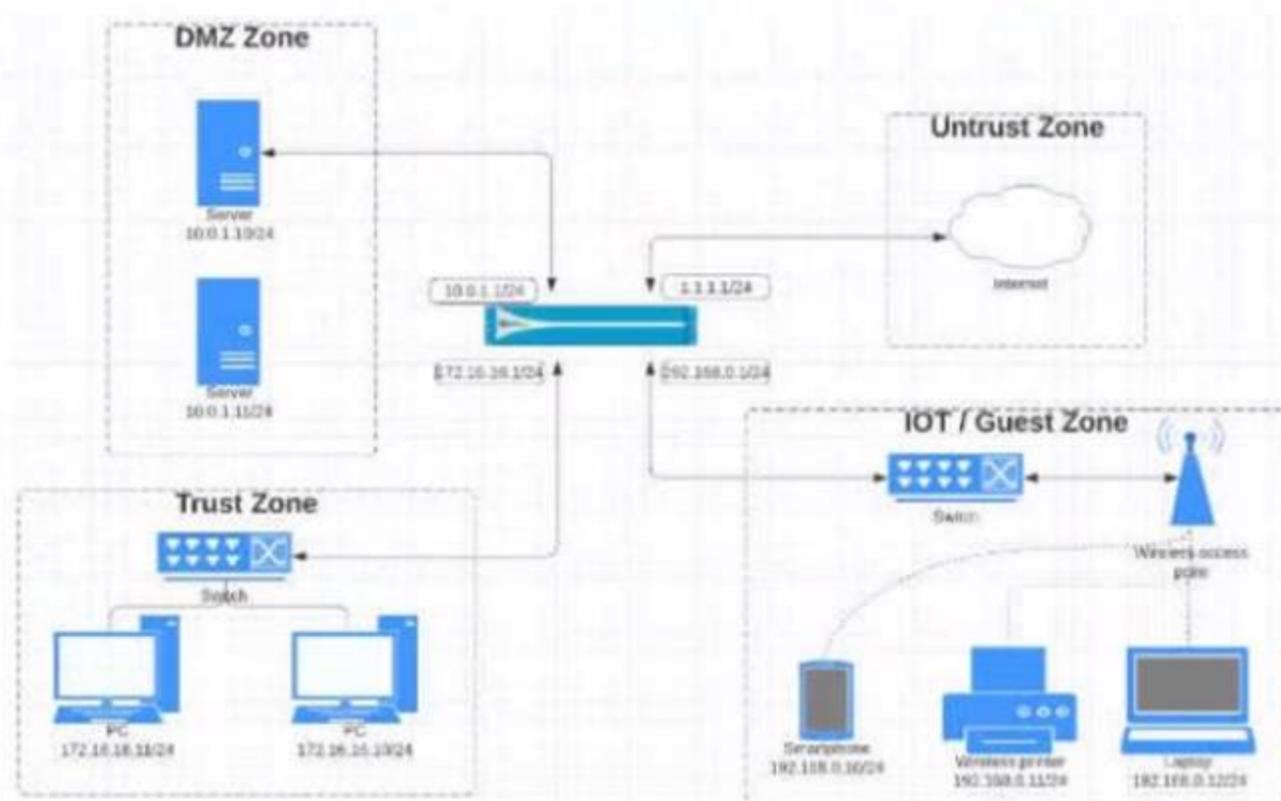


- A. branch office traffic
- B. north-south traffic
- C. perimeter traffic
- D. east-west traffic

Answer: D

NEW QUESTION 236

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 IOT/Guest and Trust Zones?

A)

	Source			Destination			APPLICATION	SERVICE	URL CATEGORY	ACTION
	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE				
Guest	172.16.16.0/24	any	any	DMZ	1.1.1.0/24	any	ssh	application-default	any	Allow
	192.168.0.0/24			Untrust	100.1.0/24		ssh			
							web-browsing			

B)

	Source			Destination			APPLICATION	SERVICE	URL CATEGORY	ACTION
	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE				
Guest	10.0.1.0/24	any	any	DMZ	1.1.1.0/24	any	ssh	application-default	any	Allow
	172.16.16.0/12			Untrust	192.168.0.0/24		ssh			
							web-browsing			

C)

	Source			Destination			APPLICATION	SERVICE	URL CATEGORY	ACTION
	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE				
Guest	172.16.16.0/24	any	any	DMZ	any	any	ssh	application-default	any	Allow
	192.168.0.0/24			Untrust			ssh			
							web-browsing			

D)

	Source			Destination			APPLICATION	SERVICE	URL CATEGORY	ACTION
	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE				
Guest	172.16.16.0/24	any	any	DMZ	any	any	ssh	application-default	any	Allow
	192.168.0.0/24			Untrust			ssh			
							web-browsing			

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

Option D

D.

Answer: C

NEW QUESTION 237

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/SMTSPS 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 240

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 241

DRAG DROP

Match each rule type with its example

Create a policy with source zones A and B. The rule will apply all traffic within zone A and all traffic within zone B, but not to traffic between zones A and B.	Answer Area <div style="border: 1px solid black; height: 30px; width: 100%;"></div> <div style="border: 1px solid black; height: 30px; width: 100%;"></div> <div style="border: 1px solid black; height: 30px; width: 100%;"></div>	Universal
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.		Intrazone
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 and from zone B to zone A, but not traffic within zones A or B.		Interzone

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Create a policy with source zones A and B. The rule will apply all traffic within zone A and all traffic within zone B, but not to traffic between zones A and B.	Answer Area <div style="border: 2px dashed red; padding: 5px;"> 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 and from zone B to zone A, but not traffic within zones A or B. </div> <div style="border: 2px dashed red; padding: 5px;"> Create a policy with source zones A and B. The rule will apply all traffic within zone A and all traffic within zone B, but not to traffic between zones A and B. </div> <div style="border: 2px dashed red; padding: 5px;"> 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. </div>	Universal
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.		Intrazone
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 and from zone B to zone A, but not traffic within zones A or B.		Interzone

NEW QUESTION 246

What are three differences between security policies and security profiles? (Choose three.)

- A. Security policies are attached to security profiles
- B. Security profiles are attached to security policies
- C. Security profiles should only be used on allowed traffic
- D. Security profiles are used to block traffic by themselves
- E. Security policies can block or allow traffic

Answer: BCE

NEW QUESTION 247

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 250

Which two Palo Alto Networks security management tools provide a consolidated creation of policies, centralized management and centralized threat intelligence. (Choose two.)

- A. GlobalProtect
- B. Panorama
- C. Aperture
- D. AutoFocus

Answer: BD

NEW QUESTION 254

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 256

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 258

What can be achieved by disabling the Share Unused Address and Service Objects with Devices setting on Panorama?

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

Answer: D

NEW QUESTION 262

What is the minimum frequency for which you can configure the firewall to 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 266

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 269

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 271

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.

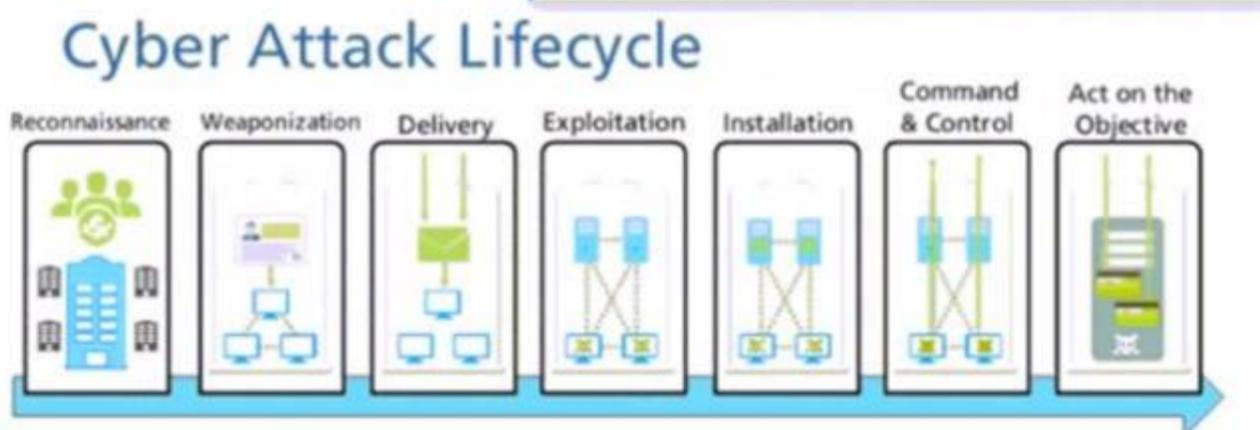
Which command in Device > Setup > Operations would provide the most operationally efficient way to accomplish this?

- 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 272

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



delivery

- A. command and control
- B. command and control
- C. exploitation
- D. reconnaissance
- E. installation

Answer: A

NEW QUESTION 273

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 276

Which user mapping method could be used to discover user IDs in an environment with multiple Windows domain controllers?

- A. Active Directory monitoring
- B. Windows session monitoring
- C. Windows client probing
- D. domain controller monitoring

Answer: A

NEW QUESTION 278

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?

the Content Delivery Networks URL category

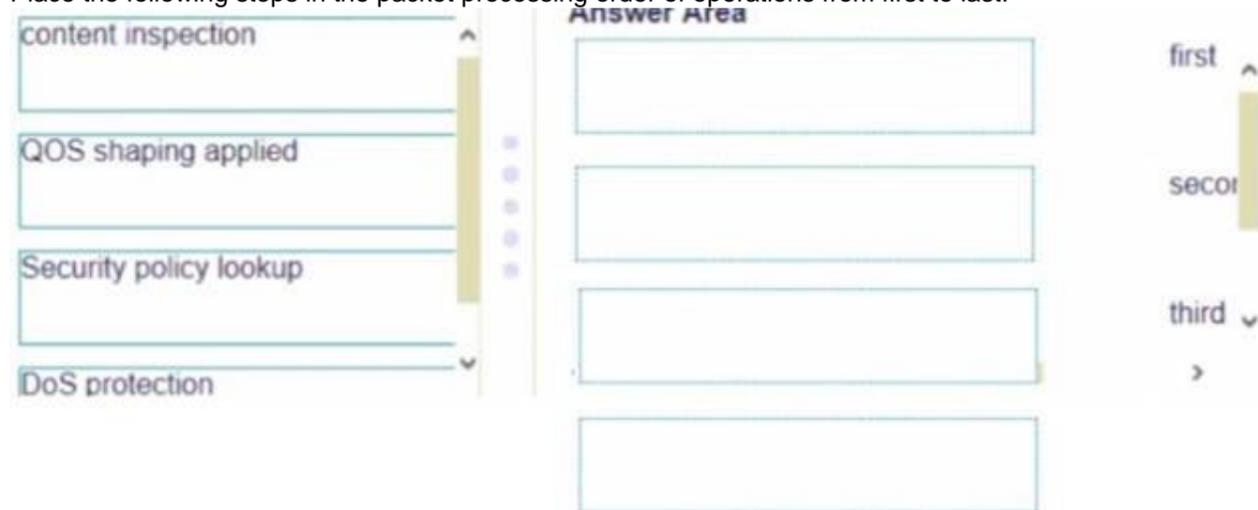
- A. the Online Storage and Backup URL category
- B. the Online Storage and Backup URL category
- C. an application group containing all of the file-sharing App-IDs reported in the traffic logs
- D. an application filter for applications whose subcategory is file-sharing

Answer: D

NEW QUESTION 281

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 282

Which administrator receives a global notification for a new malware that infects hosts. The infection will result in the infected host attempting to contact and command-and-control (C2) server.

Which security profile components will detect and prevent this threat after the firewall's signature database has been updated?

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

Answer: C

Explanation:

NEW QUESTION 284

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 285

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 287

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 290

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

- A. on either the data plane 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 292

What is a recommended consideration when deploying content updates to the firewall from Panorama?

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

Answer: C

NEW QUESTION 297

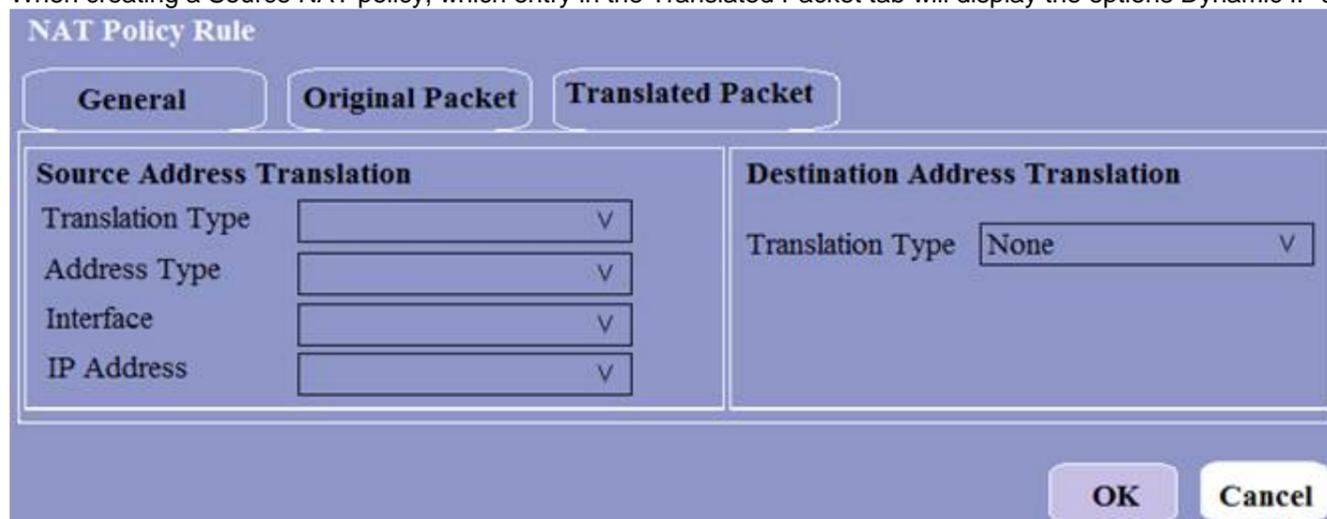
Users from the internal zone need to be allowed to Telnet into a server in the DMZ zone. Complete the security policy to ensure only Telnet is allowed. Security Policy: Source Zone: Internal to DMZ Zone services "Application defaults", and action = Allow

- 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 298

When creating a Source NAT policy, which entry in the Translated Packet tab will display the options Dynamic IP and Port, Dynamic, Static IP, and None?



The screenshot shows the 'Translated Packet' tab of a NAT Policy Rule configuration. It is divided into two sections: 'Source Address Translation' and 'Destination Address Translation'. In the 'Source Address Translation' section, the 'Translation Type' dropdown is currently set to 'None'. In the 'Destination Address Translation' section, the 'Translation Type' dropdown is also set to 'None'. Other fields like 'Address Type', 'Interface', and 'IP Address' are present but not filled. 'OK' and 'Cancel' buttons are at the bottom right.

- A. Translation Type
- B. Interface
- C. Address Type
- D. IP Address

Answer: A

NEW QUESTION 300

A network has 10 domain controllers, multiple WAN links, and a network infrastructure with bandwidth needed to support mission-critical applications. Given the scenario, which type of User-ID agent is considered a best practice by Palo Alto Networks?

Windows-based agent on a domain controller

- A. Captive Portal
- C. Citrix terminal server with adequate data-plane resources
- D. PAN-OS integrated agent

Answer: A

NEW QUESTION 301

Which type of address object is "10 5 1 1/0 127 248 2"?

- A. IP subnet
- B. IP wildcard mask
- C. IP netmask
- D. IP range

Answer: B

NEW QUESTION 302

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

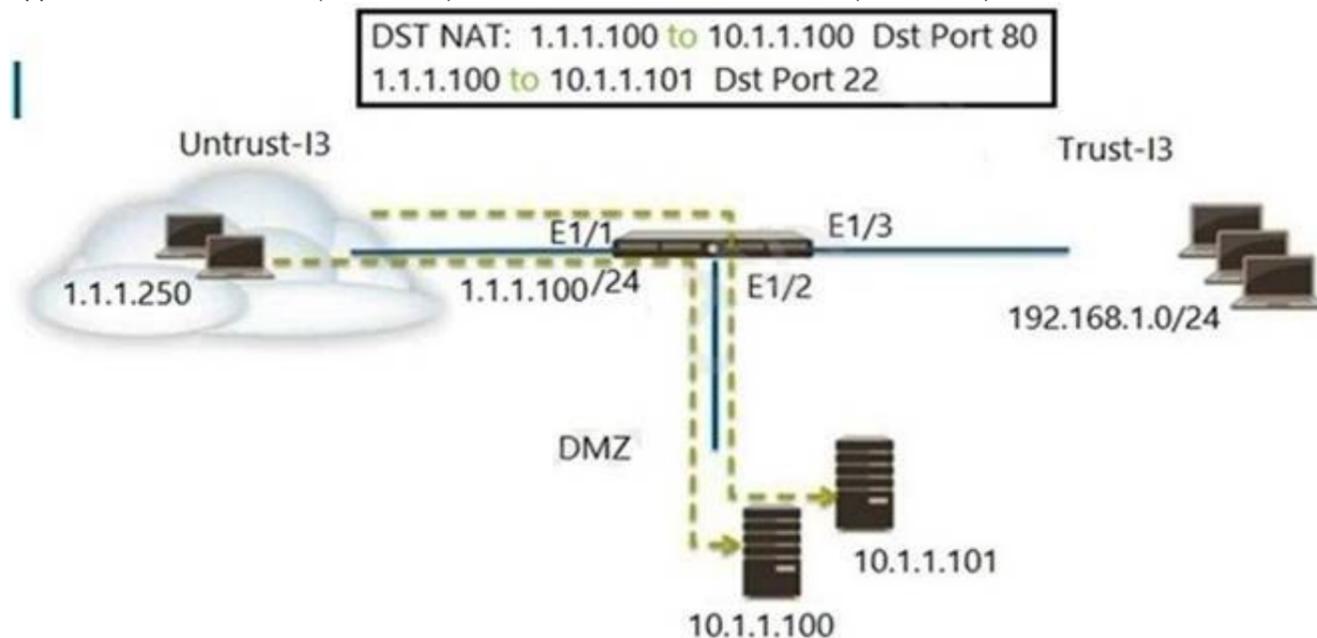
- A. Network Processing Engine
- Single Stream-based Engine
- B. Policy Engine
- D. Parallel Processing Hardware

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

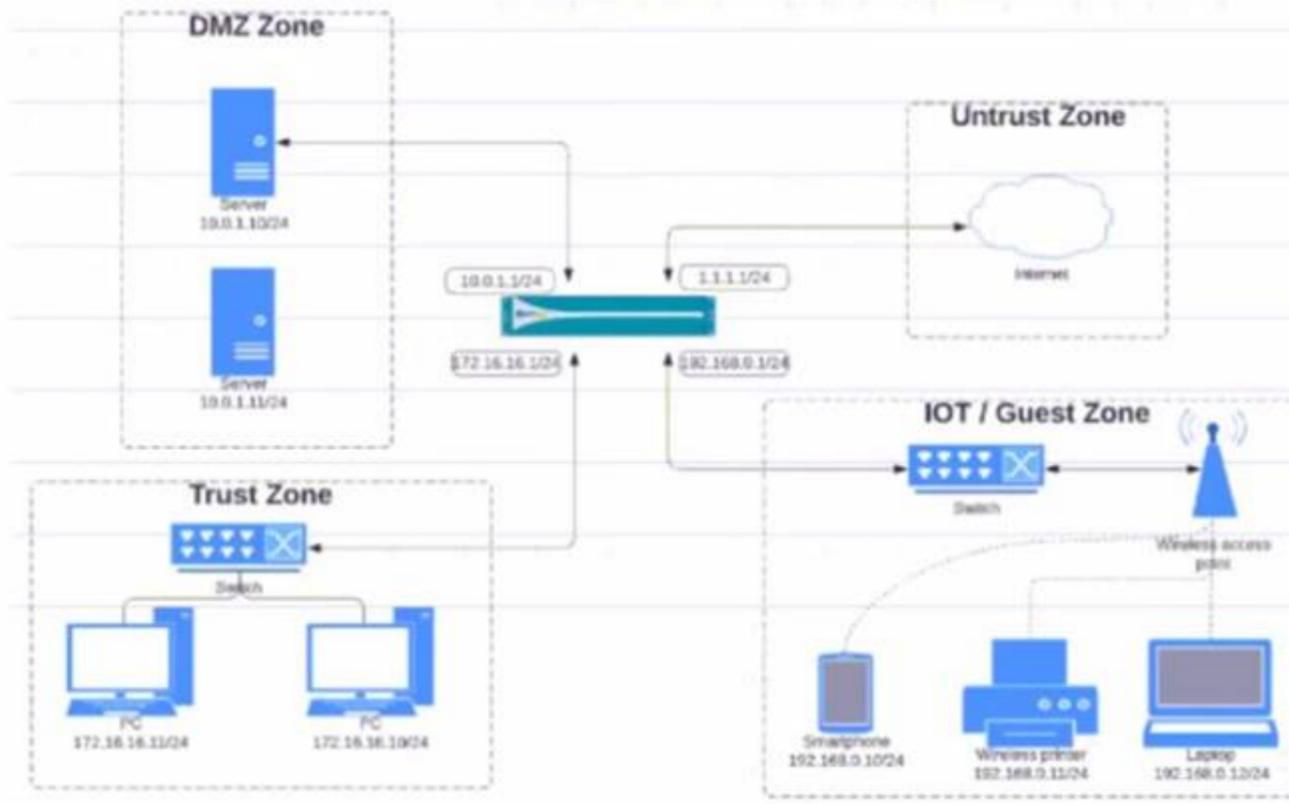
Explanation:

Reference:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIt5CAC>

NEW QUESTION 307

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



Which policy achieves the desired results?

A)

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

B)

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

C)

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

D)

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

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

Answer: C

NEW QUESTION 308

How often does WildFire release dynamic updates?

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

Answer: A

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 314

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 317

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 318

URL categories can be used as match criteria on which two policy types? (Choose two.)

- A. authentication
- B. decryption
- C. application override
- C. NAT

Answer: AB

Explanation:

Reference: <https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/url-filtering/url-filtering-concepts/url-category-as-policy-match-criteria.html>

NEW QUESTION 322

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 325

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 329

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 334

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 338

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 340

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 345

The NetSec Manager asked to create a new firewall Local Administrator profile with customized privileges named NewAdmin. This new administrator has to authenticate without inserting any username or password to access the WebUI.

What steps should the administrator follow to create the New_Admin Administrator profile?

A.

- * 1. Select the "Use only client certificate authentication" check box.
- * 2. Set Role to Role Based.
- * 3. Issue to the Client a Certificate with Common Name = NewAdmin

B.

- * 1. Select the "Use only client certificate authentication" check box.
- * 2. Set Role to Dynamic.
- * 3. Issue to the Client a Certificate with Certificate Name = NewAdmin

C.

- * 1. Set the Authentication profile to Local.
- * 2. Select the "Use only client certificate authentication" check box.
- * 3. Set Role to Role Based.

D.

- * 1. Select the "Use only client certificate authentication" check box.
- * 2. Set Role to Dynamic.
- * 3. Issue to the Client a Certificate with Common Name = New Admin

A.

Answer: B

NEW QUESTION 350

The compliance officer requests that all evasive applications need to be blocked on all perimeter firewalls out to the internet The firewall is configured with two zones;

- * 1. trust for internal networks

* 2. untrust to the internet

Based on the capabilities of the Palo Alto Networks NGFW, what are two ways to configure a security policy using App-ID to comply with this request? (Choose two)

- A. Create a deny rule at the top of the policy from trust to untrust with service application- default and add an application filter with the evasive characteristic
- B. Create a deny rule at the top of the policy from trust to untrust over any service and select evasive as the application
- C. Create a deny rule at the top of the policy from trust to untrust with service application- default and select evasive as the application
- D. Create a deny rule at the top of the policy from trust to untrust over any service and add an application filter with the evasive characteristic

Answer: AD

NEW QUESTION 353

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 356

Which three filter columns are available when setting up an Application Filter? (Choose three.)

- A. Parent App
- B. Category
- C. Risk
- D. Standard Ports
- E. Subcategory

Answer: BCE

Explanation:

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/objects/objects- application-filters>

NEW QUESTION 361

Access to which feature requires PAN-OS Filtering licenses?

- 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 365

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 366

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 369

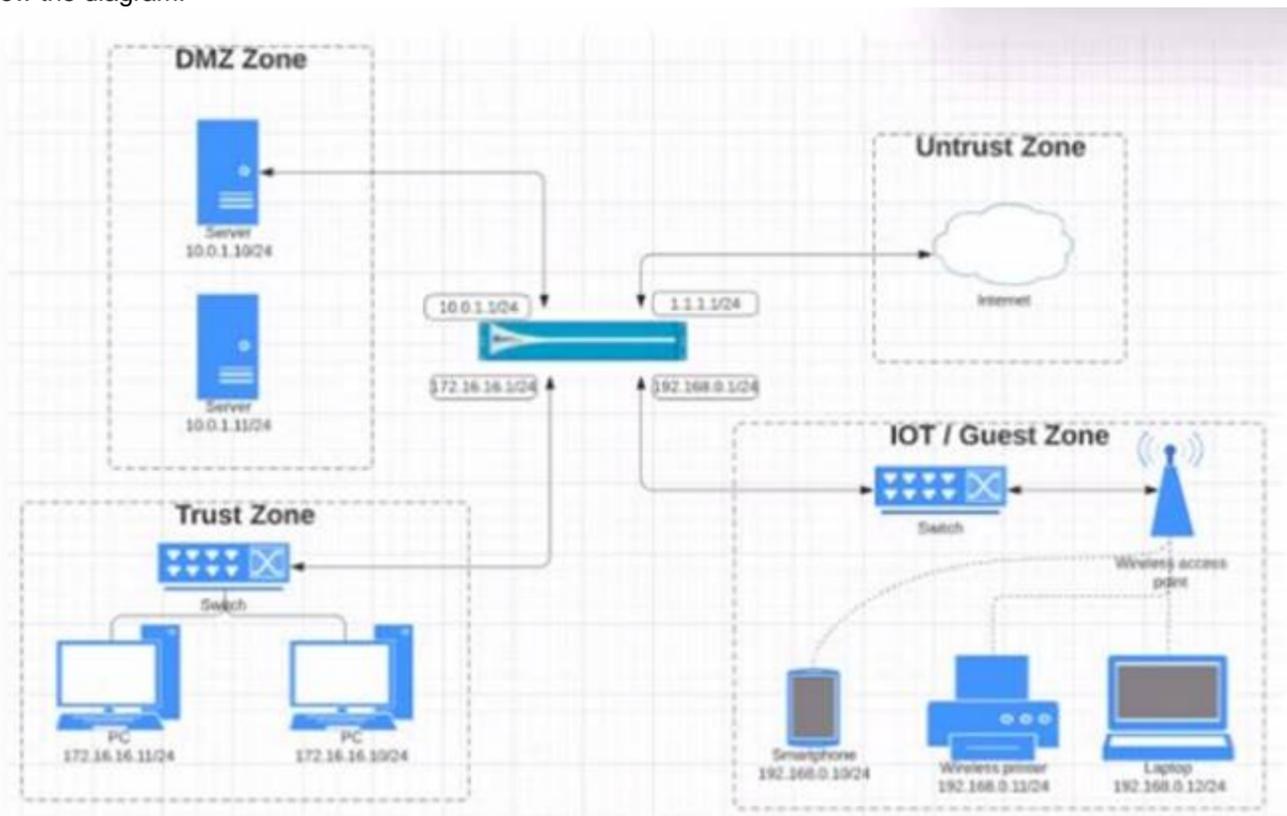
Which two matching criteria are used when creating a Security policy involving NAT? (Choose two.)

- A. Post-NAT address
- B. Post-NAT zone
- C. Pre-NAT zone
- D. Pre-NAT address

Answer: BD

NEW QUESTION 372

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 IOT/Guest and Trust Zones?

A)

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE		
03-A	None	universal	IOT-Guest	172.16.16.0/24	any	any	DMZ	any	any	ssh	application-default
			Trust	192.168.0.0/24			Untrust			ssh	web-browsing

B)

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE		
03-A	None	universal	IOT-Guest	172.16.16.0/24	any	any	DMZ	1.1.1.0/24	any	ssh	application-default
			Trust	192.168.0.0/24			Untrust	10.0.1.0/24		ssh	web-browsing

C)

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE		
03-A	None	universal	IOT-Guest	10.0.1.0/24	any	any	DMZ	1.1.1.0/24	any	ssh	application-default
			Trust	172.16.16.0/24			Untrust	192.168.0.0/24		ssh	web-browsing

D)

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE		

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

Answer: C

NEW QUESTION 373

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 374

An administrator is reviewing another administrator's Security policy log settings. Which log setting configuration is consistent with best practices for 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 377

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 380

An administrator would like to see the traffic that matches the interzone-default rule in the traffic logs. What is the correct process to enable this logging?

- A. Select the interzone-default rule and edit the rule on the Actions tab select Log at Session Start and click OK
- B. Select the interzone-default rule and edit the rule on the Actions tab select Log at Session End and click OK
- C. This rule has traffic logging enabled by default no further action is required
- D. Select the interzone-default rule and click Override on the Actions tab select Log at Session End and click OK

Answer: D

NEW QUESTION 384

.....

Relate Links

100% Pass Your PCNSA Exam with ExamBible Prep Materials

<https://www.exambible.com/PCNSA-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>