



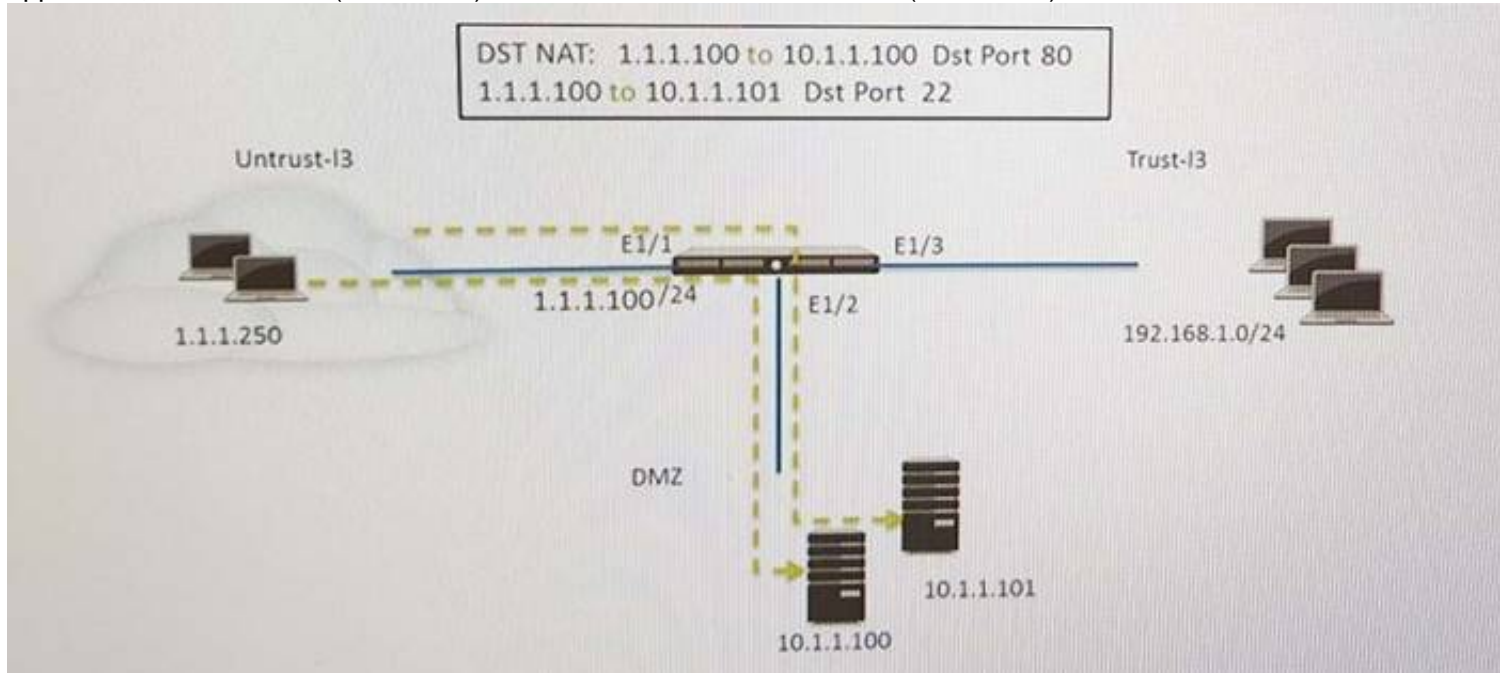
Paloalto-Networks

Exam Questions PCNSA

Palo Alto Networks Certified Network Security Administrator

NEW QUESTION 1

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

Answer: AE

NEW QUESTION 2

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 3

Which type of address object is www.paloaltonetworks.com?

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

Answer: D

NEW QUESTION 4

In which profile should you configure the DNS Security feature?

- A. URL Filtering Profile
- B. Anti-Spyware Profile
- C. Zone Protection Profile
- D. Antivirus Profile

Answer: B

NEW QUESTION 5

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

NEW QUESTION 6

Complete the statement. A security profile can block or allow traffic

- A. on unknown-tcp or unknown-udp traffic
- B. after it is matched by a security policy that allows traffic
- C. before it is matched by a security policy
- D. after it is matched by a security policy that allows or blocks traffic

Answer: B

Explanation:

Security profiles are objects added to policy rules that are configured with an action of allow.

NEW QUESTION 7

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

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

Answer: D

NEW QUESTION 8

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

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

Answer: A

NEW QUESTION 9

All users from the internal zone must be allowed only HTTP access to a server in the DMZ zone.

Complete the empty field in the Security policy using an application object to permit only this type of access. Source Zone: Internal Destination Zone: DMZ Zone Application:

Service: application-default - Action: allow

- A. Application = "any"
- B. Application = "web-browsing"
- C. Application = "ssl"
- D. Application = "http"

Answer: B

NEW QUESTION 10

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 10

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 14

An administrator configured a Security policy rule with an Antivirus Security profile. The administrator did not change the action (or the profile. If a virus gets detected, how will the firewall handle the traffic?

- A. It allows the traffic because the profile was not set to explicitly deny the traffic.
- B. It drops the traffic because the profile was not set to explicitly allow the traffic.
- C. It uses the default action assigned to the virus signature.

D. It allows the traffic but generates an entry in the Threat logs.

Answer: B

NEW QUESTION 17

The Palo Alto Networks NGFW was configured with a single virtual router named VR-1. What changes are required on VR-1 to route traffic between two interfaces on the NGFW?

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

Answer: D

NEW QUESTION 20

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 21

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 24

Which interface type requires no routing or switching but applies Security or NAT policy rules before passing allowed traffic?

- A. Layer 3
- B. Virtual Wire
- C. Tap
- D. Layer 2

Answer: A

NEW QUESTION 28

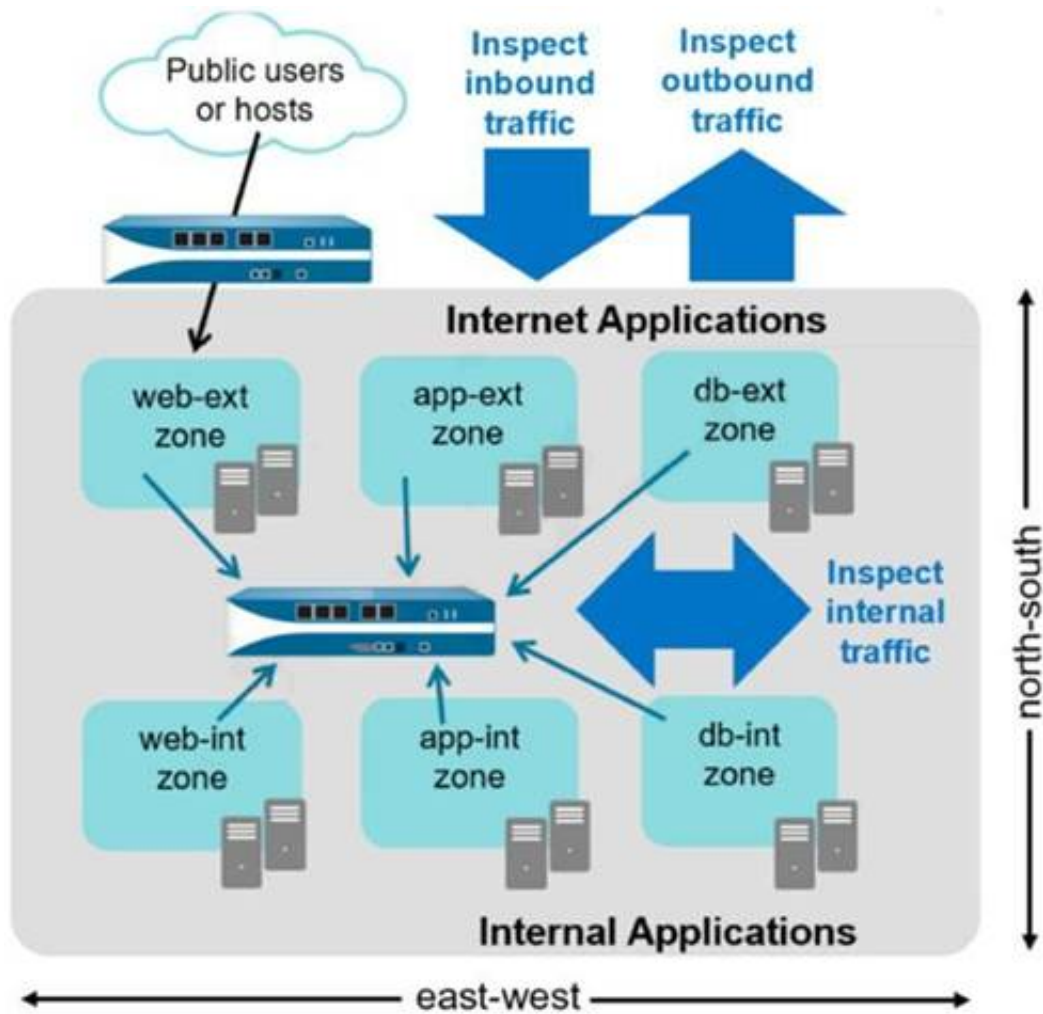
An administrator wants to create a NAT policy to allow multiple source IP addresses to be translated to the same public IP address. What is the most appropriate NAT policy to achieve this?

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

Answer: A

NEW QUESTION 32

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 37

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

Answer: C

NEW QUESTION 42

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

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

Answer: B

NEW QUESTION 45

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 47

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 52

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 55

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

NEW QUESTION 57

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

- A. Layer 2
- B. Tap
- C. Layer 3
- D. Virtual Wire

Answer: B

NEW QUESTION 59

A security administrator has configured App-ID updates to be automatically downloaded and installed. The company is currently using an application identified by App-ID as SuperApp_base.

On a content update notice, Palo Alto Networks is adding new app signatures labeled SuperApp_chat and SuperApp_download, which will be deployed in 30 days. Based on the information, how is the SuperApp traffic affected after the 30 days have passed?

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

Answer: A

Explanation:

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/app-id/manage-new-app-ids-introduced-in-content>

NEW QUESTION 61

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

	Name	Tags	Type	Source			Destination			Hit Usage			Application	Service	Action	Profile
				Zone	Address	User	Zone	Address	HIP Profile	Hit Count	Last Hit	First Hit				
1	Allow Office Programs	None	Universal	Inside	Any	Any	Any	Outside	Any	-	-	-	Office-program	Application-d...	Allow	None
2	Allow FTP to web ser..	None	Universal	Inside	Any	Any	Any	Outside	ftp-server	-	-	-	any	ftp-service...	Allow	None
3	Allow Social Networkin..	None	Universal	Inside	Any	Any	Any	Outside	Any	-	-	-	facebook	Application-d...	Allow	None

- A. The Allow Office Programs rule is using an Application Filter
- B. In the Allow FTP to web server rule, FTP is allowed using App-ID
- C. The Allow Office Programs rule is using an Application Group
- D. In the Allow Social Networking rule, allows all of Facebook's functions

Answer: AD

Explanation:

In the Allow FTP to web server rule, FTP is allowed using port based rule and not APP-ID.

NEW QUESTION 65

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

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

Answer: BC

NEW QUESTION 69

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 73

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 74

Which type of administrator account cannot be used to authenticate user traffic flowing through the firewall's data plane?

- A. Kerberos user
- B. SAML user
- C. local database user
- D. local user

Answer: B

NEW QUESTION 76

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 81

What must be configured before setting up Credential Phishing Prevention?

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

Answer: B

Explanation:

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/threat-prevention/prevent-credential-phishing/set-u>

NEW QUESTION 85

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

NEW QUESTION 88

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?

- A. Security policy = drop, Gambling category in URL profile = allow
- B. 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 93

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 97

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

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

Answer: B

NEW QUESTION 99

Which statement is true regarding a Best Practice Assessment?

- A. The BPA tool can be run only on firewalls
- B. It provides a percentage of adoption for each assessment data
- C. The assessment, guided by an experienced sales engineer, helps determine the areas of greatest risk where you should focus prevention activities

D. It provides a set of questionnaires that help uncover security risk prevention gaps across all areas of network and security architecture

Answer: C

NEW QUESTION 100

Your company occupies one floor in a single building you have two active directory domain controllers on a single networks the firewall s management plane is only slightly utilized.

Which user-ID agent sufficient in your network?

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

Answer: D

NEW QUESTION 105

An administrator needs to add capability to perform real-time signature lookups to block or sinkhole all known malware domains.

Which type of single unified engine will get this result?

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

Answer: A

NEW QUESTION 109

For the firewall to use Active Directory to authenticate users, which Server Profile is required in the Authentication Profile?

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

Answer: C

NEW QUESTION 114

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 117

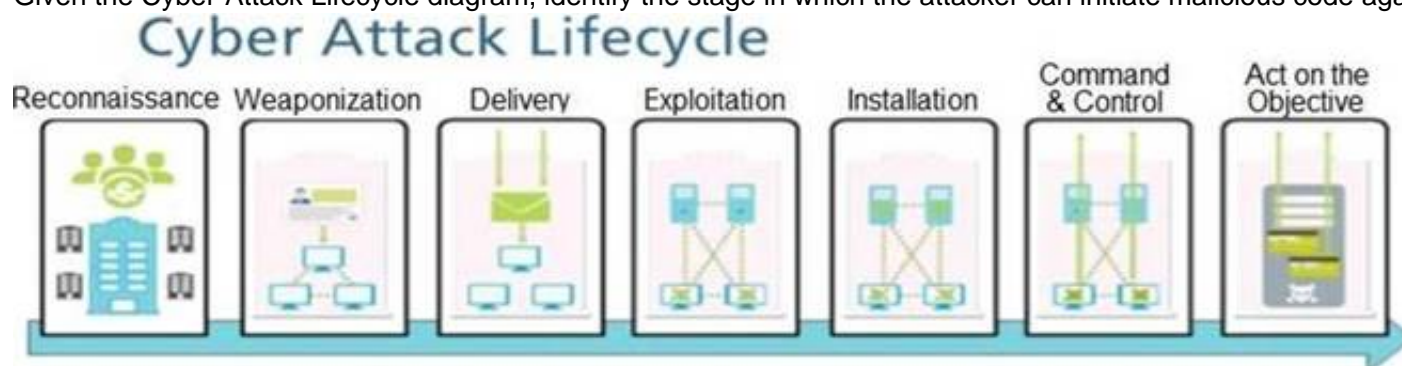
Why should a company have a File Blocking profile that is attached to a Security policy?

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

Answer: A

NEW QUESTION 120

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 122

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 124

An address object of type IP Wildcard Mask can be referenced in which part of the configuration?

- A. Security policy rule
- B. ACC global filter
- C. external dynamic list
- D. NAT address pool

Answer: A

Explanation:

You can use an address object of type IP Wildcard Mask only in a Security policy rule. [https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/objects/objects-addresses IP Wildcard Mask](https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/objects/objects-addresses/IP-Wildcard-Mask)

—Enter an IP wildcard address in the format of an IPv4 address followed by a slash and a mask (which must begin with a zero); for example, 10.182.1.1/0.127.248.0. In the wildcard mask, a zero (0) bit indicates that the bit being compared must match the bit in the IP address that is covered by the 0. A one (1) bit in the mask is a wildcard bit, meaning the bit being compared need not match the bit in the IP address that is covered by the 1. Convert the IP address and the wildcard mask to binary. To illustrate the matching: on binary snippet 0011, a wildcard mask of 1010 results in four matches (0001, 0011, 1001, and 1011).

NEW QUESTION 125

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

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

Answer: B

NEW QUESTION 128

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

- A. password profile
- B. access domain
- C. admin role
- D. server profile

Answer: CD

NEW QUESTION 129

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 132

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 135

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. save named configuration snapshot
- B. export device state
- C. export named configuration snapshot
- D. save candidate config

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 136

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 140

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 141

Which statement is true regarding NAT rules?

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

Answer: C

Explanation:

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

NEW QUESTION 143

Match the Palo Alto Networks Security Operating Platform architecture to its description.

Threat Intelligence Cloud	Drag answer here	Identifies and inspects all traffic to block known threats.
Next-Generation Firewall	Drag answer here	Gathers, analyzes, correlates, and disseminates threats to and from the network and endpoints located within the network.
Advanced Endpoint Protection	Drag answer here	Inspects processes and files to prevent known and unknown exploits.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Threat Intelligence Cloud – Gathers, analyzes, correlates, and disseminates threats to and from the network and endpoints located within the network.
Next-Generation Firewall – Identifies and inspects all traffic to block known threats
Advanced Endpoint Protection - Inspects processes and files to prevent known and unknown exploits

NEW QUESTION 146

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

NEW QUESTION 147

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

- 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 151

Place the following steps in the packet processing order of operations from first to last.

content inspection		first
QOS shaping applied		second
Security policy lookup		third
DoS protection		fourth

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 152

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

NEW QUESTION 157

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 161

An administrator wants to prevent users from submitting corporate credentials in a phishing attack. Which Security profile should be applied?

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

Answer: B

NEW QUESTION 165

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 166

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

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

Answer: B

NEW QUESTION 170

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 172

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

	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. Allows users to access IT applications on all ports
- B. 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 175

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 177

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 179

Which path is used to save and load a configuration with a Palo Alto Networks firewall?

- A. Device>Setup>Services
- B. Device>Setup>Management
- C. Device>Setup>Operations
- D. Device>Setup>Interfaces

Answer: C

NEW QUESTION 180

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 183

Match the Cyber-Attack Lifecycle stage to its correct description.

Reconnaissance	Drag answer here	stage where the attacker has motivation for attacking a network to deface web property
Installation	Drag answer here	stage where the attacker scans for network vulnerabilities and services that can be exploited
Command and Control	Drag answer here	stage where the attacker will explore methods such as a root kit to establish persistence
Act on the Objective	Drag answer here	stage where the attacker has access to a specific server so they can communicate and pass data to and from infected devices within a network

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reconnaissance – stage where the attacker scans for network vulnerabilities and services that can be exploited. Installation – stage where the attacker will explore methods such as a root kit to establish persistence Command and Control – stage where the attacker has access to a specific server so they can communicate and pass data to and from infected devices within a network.
 Act on the Objective – stage where an attacker has motivation for attacking a network to deface web property

NEW QUESTION 186

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 188

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

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

Answer: C

NEW QUESTION 193

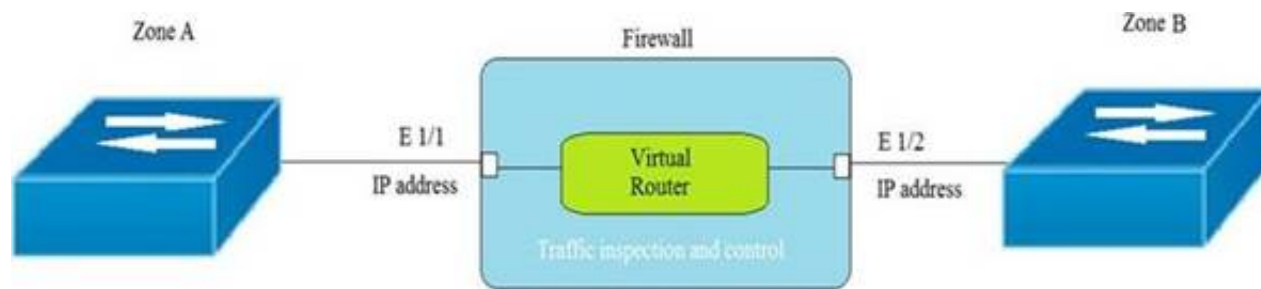
Which rule type is appropriate for matching traffic occurring within a specified zone?

- A. Interzone
- B. Universal
- C. Intrazone
- D. Shadowed

Answer: C

NEW QUESTION 196

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 200

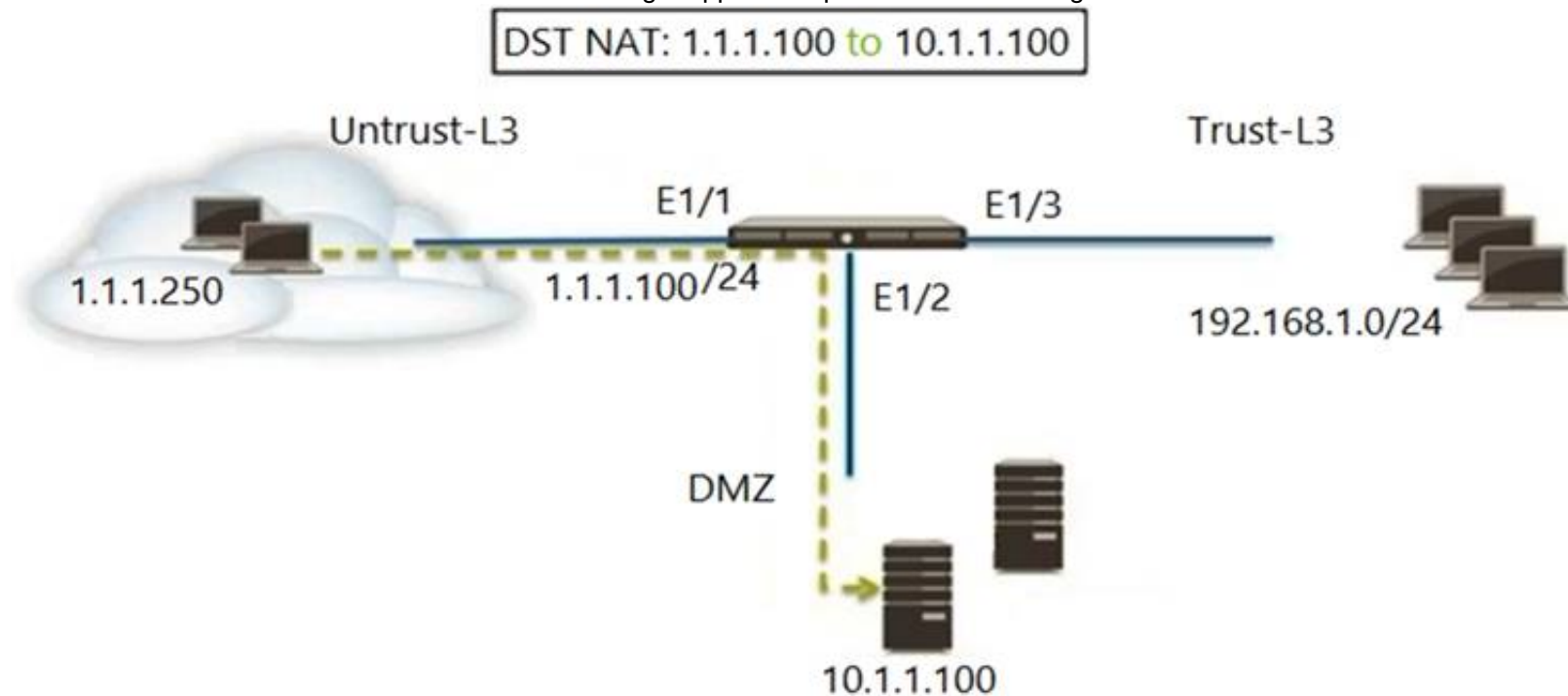
How are Application Fillers or Application Groups used in firewall policy?

- A. An Application Filter is a static way of grouping applications and can be configured as a nested member of an Application Group
- B. An Application Filter is a dynamic way to group applications and can be configured as a nested member of an Application Group
- C. An Application Group is a dynamic way of grouping applications and can be configured as a nested member of an Application Group
- D. An Application Group is a static way of grouping applications and cannot be configured as a nested member of Application Group

Answer: B

NEW QUESTION 204

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. Untrust (any) to DMZ (10.1.1.100), web browsing -Allow
- B. Untrust (any) to Untrust (1.1.1.100), web browsing - Allow
- C. Untrust (any) to Untrust (10.1.1.100), web browsing -Allow
- D. Untrust (any) to DMZ (1.1.1.100), web browsing - Allow

Answer: D

NEW QUESTION 208

What must be configured for the firewall to access multiple authentication profiles for external services to authenticate a non-local account?

- A. authentication sequence
- B. LDAP server profile
- C. authentication server list
- D. authentication list profile

Answer: A

NEW QUESTION 211

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/creating-a-device-group>

NEW QUESTION 214

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.com>. Submit for "request change", identifying the appropriate categorization, and wait for confirmation before testing again.
- D. 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 policy.
- E. Set the policy action to Deny.

Answer: CD

NEW QUESTION 216

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

NEW QUESTION 221

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 224

What is considered best practice with regards to committing configuration changes?

- A. Disable the automatic commit feature that prioritizes content database installations before committing
- B. Validate configuration changes prior to committing
- C. Wait until all running and pending jobs are finished before committing
- D. Export configuration after each single configuration change performed

Answer: A

NEW QUESTION 226

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

Explanation:

Because new WildFire signatures are now available every five minutes, it is a best practice to use this setting to ensure the firewall retrieves these signatures within a minute of availability.

NEW QUESTION 230

To use Active Directory to authenticate administrators, which server profile is required in the authentication profile?

- A. domain controller
- B. TACACS+
- C. LDAP
- D. RADIUS

Answer: C

NEW QUESTION 234

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

NEW QUESTION 238

Your company requires positive username attribution of every IP address used by wireless devices to support a new compliance requirement. You must collect IP-to-user mappings as soon as possible with minimal downtime and minimal configuration changes to the wireless devices themselves. The wireless devices are from various manufactures.

Given the scenario, choose the option for sending IP-to-user mappings to the NGFW.

- A. syslog
- B. RADIUS
- C. UID redistribution
- D. XFF headers

Answer: A

NEW QUESTION 243

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 246

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

NEW QUESTION 250

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

Answer: B

NEW QUESTION 255

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-profi>

NEW QUESTION 259

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 261

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 262

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 265

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

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

Answer: D

NEW QUESTION 268

Which statement is true regarding a Prevention Posture Assessment?

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

Answer: B

NEW QUESTION 272

Which option lists the attributes that are selectable when setting up an Application filters?

- A. Category, Subcategory, Technology, and Characteristic
- B. Category, Subcategory, Technology, Risk, and Characteristic
- C. Name, Category, Technology, Risk, and Characteristic
- D. Category, Subcategory, Risk, Standard Ports, and Technology

Answer: B

NEW QUESTION 276

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 277

Which action results in the firewall blocking network traffic with out notifying the sender?

- A. Drop
- B. Deny
- C. Reset Server
- D. Reset Client

Answer: B

NEW QUESTION 278

Place the steps in the correct packet-processing order of operations.

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
Text, application, table Description automatically generated with medium confidence

NEW QUESTION 280
Which Security profile would you apply to identify infected hosts on the protected network using DNS traffic?

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

Answer: C

NEW QUESTION 284
A network administrator created an intrazone Security policy rule on the firewall. The source zones were set to IT. Finance, and HR. Which two types of traffic will the rule apply to? (Choose two)

- A. traffic between zone IT and zone Finance
- B. traffic between zone Finance and zone HR
- C. traffic within zone IT
- D. traffic within zone HR

Answer: CD

NEW QUESTION 285
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 288
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 292
Which Palo Alto Networks firewall security platform provides network security for mobile endpoints by inspecting traffic deployed as internet gateways?

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

D. Panorama

Answer: A

Explanation:

GlobalProtect: GlobalProtect safeguards your mobile workforce by inspecting all traffic using your next-generation firewalls deployed as internet gateways, whether at the perimeter, in the Demilitarized Zone (DMZ), or in the cloud.

NEW QUESTION 295

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. EDL in URL Filtering Profile.
- B. Custom URL category in Security Policy rule.
- C. Custom URL category in URL Filtering Profile.
- D. PAN-DB URL category in URL Filtering Profile.

Answer: D

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 300

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

NEW QUESTION 302

Which object would an administrator create to block access to all high-risk applications?

- A. HIP profile
- B. application filter
- C. application group
- D. Vulnerability Protection profile

Answer: B

NEW QUESTION 303

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 308

Which type firewall configuration contains in-progress configuration changes?

- A. backup
- B. running
- C. candidate
- D. committed

Answer: C

NEW QUESTION 310

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

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

Answer: C

NEW QUESTION 312

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

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

Answer: C

NEW QUESTION 317

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

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

Answer: BD

NEW QUESTION 321

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 326

.....

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](#)