



Paloalto-Networks

Exam Questions PCNSA

Palo Alto Networks Certified Network Security Administrator

NEW QUESTION 1

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

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

Answer: B

NEW QUESTION 2

Which security policy rule would be needed to match traffic that passes between the Outside zone and Inside zone, but does not match traffic that passes within the zones?

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

Answer: B

NEW QUESTION 3

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 4

Which object would an administrator create to enable access to all applications in the office-programs subcategory?

- A. application filter
- B. URL category
- C. HIP profile
- D. application group

Answer: A

NEW QUESTION 5

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 6

DRAG DROP

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 7

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 8

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 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				Modified
				Apps Allowed	Apps Seen	Days with No New Apps	Compare	
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

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

Palo Alto Networks User-ID Agent Setup

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

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

Answer: BC

NEW QUESTION 10

What are two differences between an implicit dependency and an explicit dependency in App-ID? (Choose two.)

- A. An implicit dependency does not require the dependent application to be added in the security policy
- B. An implicit dependency requires the dependent application to be added in the security

policy

- C. An explicit dependency does not require the dependent application to be added in the security policy
- D. An explicit dependency requires the dependent application to be added in the security policy

Answer: AD**NEW QUESTION 11**

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 12**

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 17

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 19

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 24

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 28

What are three factors that can be used in domain generation algorithms? (Choose three.)

- A. cryptographic keys
- B.

time of day

- C. other unique values
- D. URL custom categories
- E. IP address

Answer: ABC

Explanation:

Domain generation algorithms (DGAs) are used to auto-generate domains, typically in large numbers within the context of establishing a malicious command-and-control (C2) communications channel. DGA-based malware (such as Pushdo, BankPatch, and CryptoLocker) limit the number of domains from being blocked by hiding the location of their active C2 servers within a large number of possible suspects, and can be algorithmically generated based on factors such as time of day, cryptographic keys, or other unique values.

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/threat-prevention/dns-security/domain-generation-algorithm-detection>

NEW QUESTION 32

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 35

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

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

Answer: A

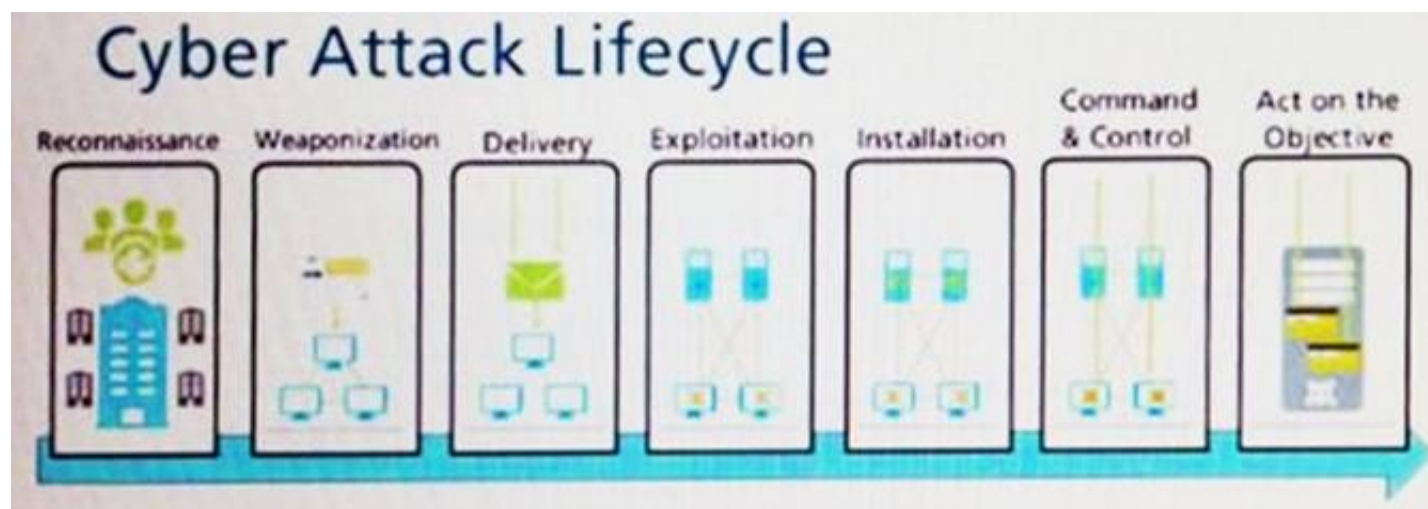
Explanation:

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

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

NEW QUESTION 36

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 39

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

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

Answer: A

Explanation:

You can use an address object of type IP Wildcard Mask only in a Security policy rule.

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/objects/objects-addresses>

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

NEW QUESTION 42

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 46

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 49

DRAG DROP

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

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

Answer:

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 53

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 56

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 58

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 59

You must configure which firewall feature to enable a data-plane interface to submit DNS queries on behalf of the control plane?

- A. Admin Role profile
- B. virtual router
- C. DNS proxy
- D. service route

Answer: A

NEW QUESTION 63

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?

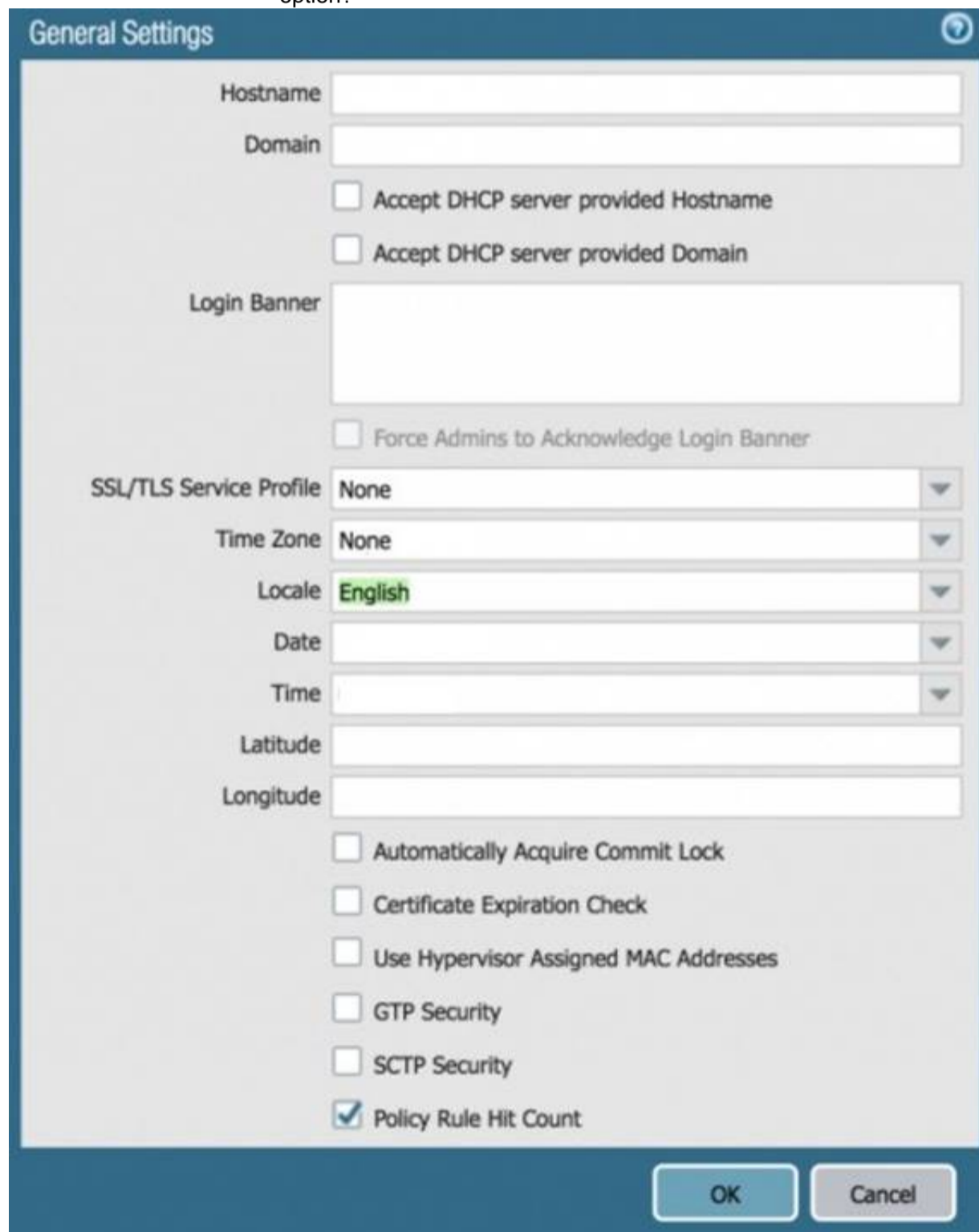
- A. Create a custom-service-object called SERVICE-SSH for destination-port-TCP-22. Create a security-rule between zone USERS and OUTSIDE to allow traffic from any source IP-address to any destination IP-address for SERVICE-SSH
- B. Create a security-rule that allows traffic from zone USERS to OUTSIDE 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 68

Based on the graphic, what is the purpose of the SSL/TLS Service profile configuration option?



The image shows a 'General Settings' dialog box with various configuration options. The 'SSL/TLS Service Profile' is set to 'None'. Other options include 'Time Zone' (None), 'Locale' (English), 'Date', 'Time', 'Latitude', 'Longitude', and several checkboxes: 'Accept DHCP server provided Hostname', 'Accept DHCP server provided Domain', 'Force Admins to Acknowledge Login Banner', 'Automatically Acquire Commit Lock', 'Certificate Expiration Check', 'Use Hypervisor Assigned MAC Addresses', 'GTP Security', 'SCTP Security', and 'Policy Rule Hit Count' (which is checked). 'OK' and 'Cancel' buttons are at the bottom.

- A. It defines the SSUTLS encryption strength used to protect the management interface.
- B. It defines the CA certificate used to verify the client's browser.
- C. It defines the certificate to send to the client's browser from the management interface.

D. It defines the firewall's global SSL/TLS timeout values.

Answer: C

Explanation:

Reference: <https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g0000000C1FGCA0>

NEW QUESTION 70

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 75

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 76

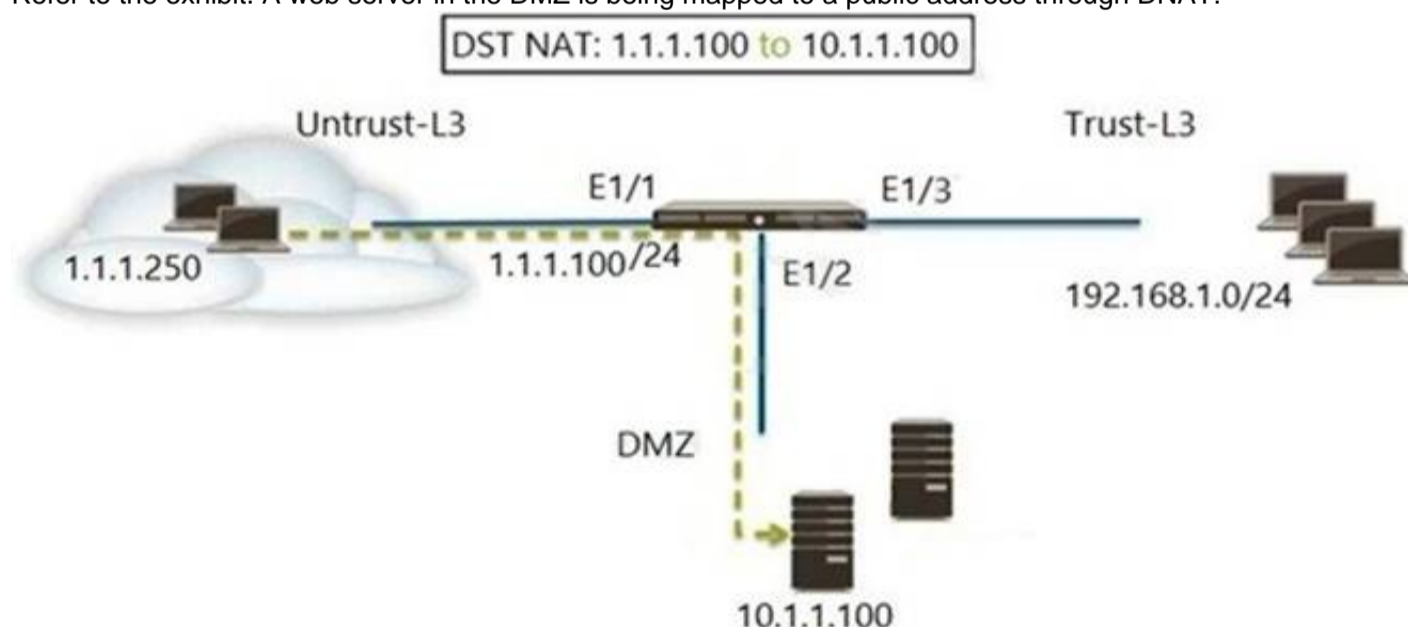
What are the requirements for using Palo Alto Networks EDL Hosting Service?

- 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 79

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-exampleone-to-one-mapping>

NEW QUESTION 84

DRAG DROP

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 86

Based on the graphic which statement accurately describes the output shown in the server monitoring panel?

User MappingConnection SecurityUser-ID AgentsTerminal Services AgentsGroup Mapping SettingsCaptive Portal Settings

Domain's DNS Name lab.localKerberos Server Profile lab-kerberos

Enable Security Log ☒

Server Log Monitor Frequency (sec) 2

Enable Session ☒

Server Session Read Frequency (sec) 10

Novell eDirectory Query Interval (sec) 30

Syslog Service Profile

Enable Probing ☒

Prove Interval (min) 20

Enable User Identification Timeout ☒

User Identification Timeout (min) 45

Allow matching usernames without domains ☐

Enable NTLM ☐

NTLM Domain

User-ID Collector Name

Server Monitoring

Name	Enabled	Type	Network Address	Status
lab-client	<input checked="" type="checkbox"/>	Microsoft Active Directory	client-a.lab.local	Connected

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

Answer: A

NEW QUESTION 90

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 94

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

		Source			Destination					
Name	Type	Zone	Address	User	Zone	Address	Application	Service	Action	
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 95

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

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

Answer: B

Explanation:

Reference:

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

NEW QUESTION 97

What do dynamic user groups you to do?

- A. create a QoS policy that provides auto-remediation for anomalous user behavior and malicious activity
- B. create a policy that provides auto-sizing for anomalous user behavior and malicious activity
- C. create a policy that provides auto-remediation for anomalous user behavior and malicious activity
- D. create a dynamic list of firewall administrators

Answer: C

Explanation:

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/user-id-features/dynamic-user-groups#:~:text=Dynamic%20user%20groups%20help%20you,activity%20while%20maintaining%20user%20visibility>.

NEW QUESTION 98

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 101

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

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

Answer: D

Explanation:

NEW QUESTION 103

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 108

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 112

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 113

Which tab would an administrator click to create an address object?

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

Answer: D

NEW QUESTION 114

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

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

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

Answer: C

NEW QUESTION 116

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

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

Answer: D

Explanation:

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

NEW QUESTION 118

By default, what is the maximum number of templates that can be added to a template stack?

- A. 6

- B. 8
- C. 10
- D. 12

Answer: B

Explanation:

By default, the maximum number of templates that can be added to a template stack is 8. This is the recommended limit for performance reasons, as adding more templates may result in sluggish responses on the user interface. However, starting from PAN-OS 8.1.10 and 9.0.4, you can use a debug command to increase the maximum number of templates per stack to 16. This command requires a commit operation to take effect.

A template stack is a collection of templates that you can use to push common settings to multiple firewalls or Panorama managed collectors. A template contains the network and device settings that you want to share across devices, such as interfaces, zones, virtual routers, DNS, NTP, and login banners. You can create multiple templates for different device groups or locations and add them to a template stack in a hierarchical order. The settings in the lower templates override the settings in the higher templates if there are any conflicts. You can then assign a template stack to one or more devices and push the configuration changes.

NEW QUESTION 122

Within an Anti-Spyware security profile, which tab is used to enable machine learning based engines?

- A. Inline Cloud Analysis
- B. Signature Exceptions
- C. Machine Learning Policies
- D. Signature Policies

Answer: A

Explanation:

? An Anti-Spyware security profile is a set of rules that defines how the firewall detects and prevents spyware from compromising hosts on the network. Spyware is a type of malware that collects information from the infected system, such as keystrokes, browsing history, or personal data, and sends it to an external command-and-control (C2) server¹.

? An Anti-Spyware security profile consists of four tabs: Signature Policies, Signature Exceptions, Machine Learning Policies, and Inline Cloud Analysis¹.

? The Signature Policies tab allows you to configure the actions and log settings for each spyware signature category, such as adware, botnet, keylogger, phishing, or worm. You can also enable DNS Security to block malicious DNS queries and responses¹.

? The Signature Exceptions tab allows you to create exceptions for specific spyware signatures that you want to override the default action or log settings. For example, you can allow a signature that is normally blocked by the profile, or block a signature that is normally alerted by the profile¹.

? The Machine Learning Policies tab allows you to configure the actions and log settings for machine learning based signatures that detect unknown spyware variants. You can also enable WildFire Analysis to submit unknown files to the cloud for further analysis¹.

? The Inline Cloud Analysis tab allows you to enable machine learning based engines that detect unknown spyware variants in real time. These engines use cloud-based models to analyze the behavior and characteristics of network traffic and identify malicious patterns. You can enable inline cloud analysis for HTTP/HTTPS traffic, SMTP/SMTPS traffic, or IMAP/IMAPS traffic¹.

Therefore, the tab that is used to enable machine learning based engines is the Inline

Cloud Analysis tab. References:

1: Security Profile: Anti-Spyware - Palo Alto Networks

NEW QUESTION 127

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 128

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 129

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 133

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 134

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 136

In which section of the PAN-OS GUI does an administrator configure URL Filtering profiles?

Policies

- ~~A~~: Network
- C. Objects
- D. Device

Answer: C

Explanation:

An administrator can configure URL Filtering profiles in the Objects section of the PAN-OS GUI. A URL Filtering profile is a collection of URL filtering controls that you can apply to individual Security policy rules that allow access to the internet¹. You can set site access for URL categories, allow or disallow user credential submissions, enable safe search enforcement, and various other settings¹.

To create a URL Filtering profile, go to Objects > Security Profiles > URL Filtering and click Add. You can then specify the profile name, description, and settings for each URL category and action². You can also configure other options such as User Credential Detection, HTTP Header Insertion, and URL Filtering Inline ML². After creating the profile, you can attach it to a Security policy rule that allows web traffic².

NEW QUESTION 138

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

				Source				Destination		File Usage						
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Hit Count	Last Hit	First Hit	Application	Service	Action	Profile
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

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 142

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 143

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 146

To what must an interface be assigned before it can process traffic?

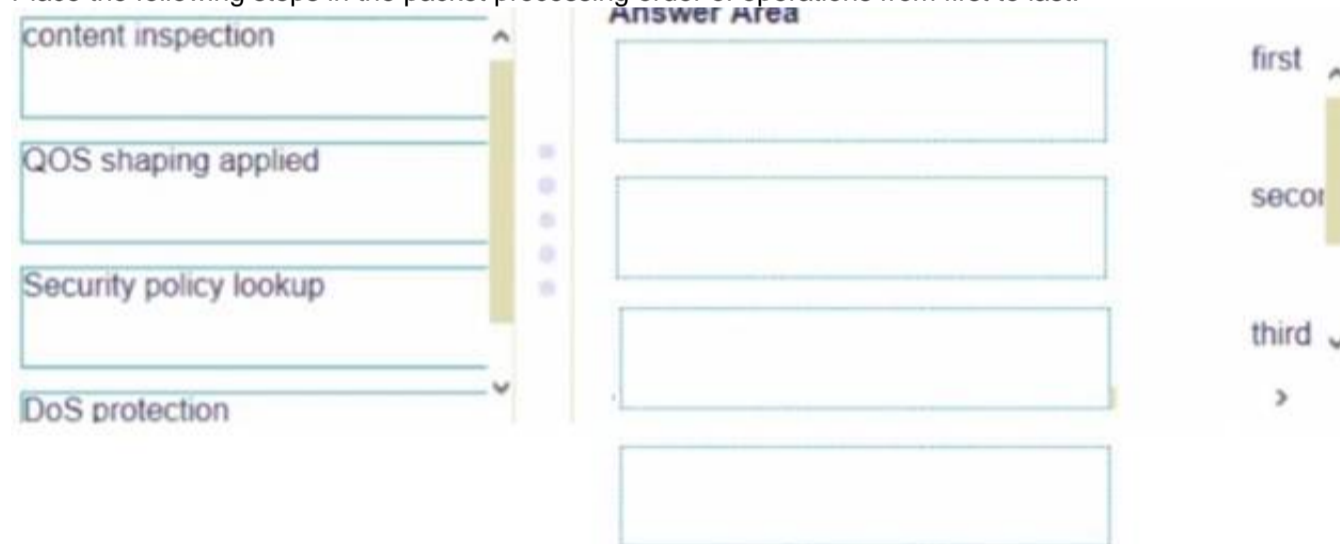
- A. Security Zone
- B. Security policy
- C. Security Protection
- D. Security profile

Answer: A

NEW QUESTION 147

DRAG DROP

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



The interface shows a list of steps on the left and an 'Answer Area' on the right. The steps are: content inspection, QOS shaping applied, Security policy lookup, and DoS protection. The Answer Area has five empty boxes. To the right of the Answer Area is a vertical bar with labels 'first', 'second', and 'third' and arrows indicating the order.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 148

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 150

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

- A. Mastered
- B. Not Mastered

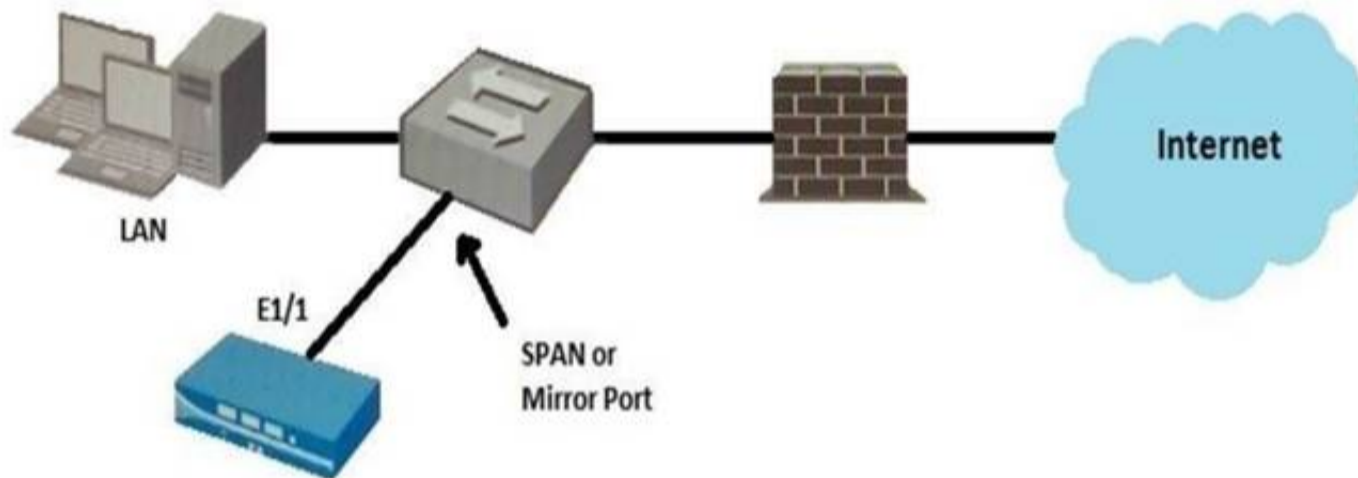
Answer: A

Explanation:

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

NEW QUESTION 151

Given the topology, which zone type should you configure for firewall interface E1/1?



- A. Tap
- B. Tunnel
- C. Virtual Wire
- D. Layer3

Answer: A

NEW QUESTION 153

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

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

Answer: D

NEW QUESTION 156

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

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

Answer: B

Explanation:

Reference:

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

NEW QUESTION 160

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

Explanation:

Reference:

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/authentication/configure-an-authenticationprofile-and-sequence>

NEW QUESTION 165

Which statement is true regarding a Best Practice Assessment?

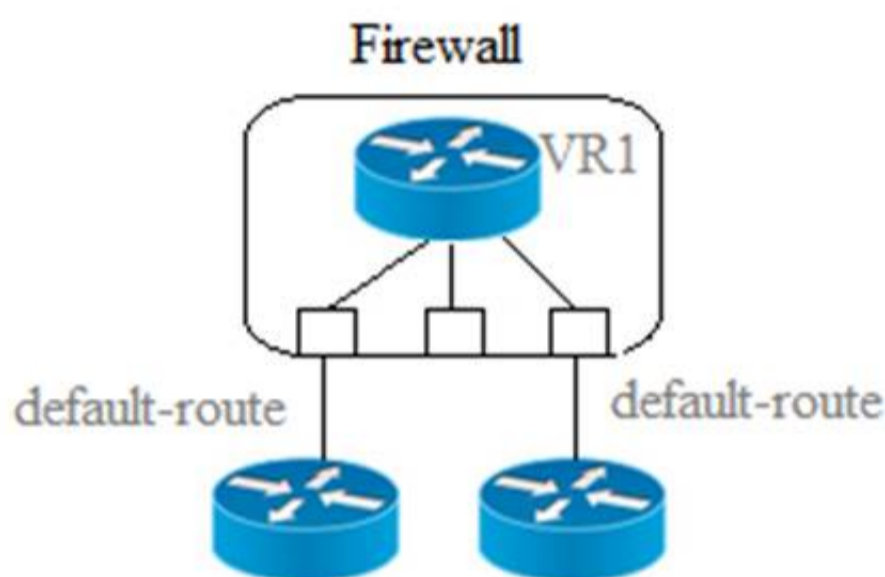
- The BPA tool can be run only on firewalls
- A: It provides a percentage of adoption for each assessment data
- C. The assessment, guided by an experienced sales engineer, helps determine the areas of greatest risk where you should focus prevention activities
- D. It provides a set of questionnaires that help uncover security risk prevention gaps across all areas of network and security architecture

Answer: C

NEW QUESTION 169

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

Multiple Static Default Routes



- Path monitoring does not determine if route is useable
- A: Route with highest metric is actively used
- C. Path monitoring determines if route is useable
- D. Route with lowest metric is actively used

Answer: CD

NEW QUESTION 171

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 176

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?

NAT Policy Rule

General Original Packet Translated Packet

Source Address Translation

Translation Type

Address Type

Interface

IP Address

Destination Address Translation

Translation Type

OK Cancel

- A. Translation Type
- B. Interface

- C. Address Type
- D. IP Address

Answer: A

NEW QUESTION 178

A network administrator is required to use a dynamic routing protocol for network connectivity.

Which three dynamic routing protocols are supported by the NGFW Virtual Router for this purpose? (Choose three.)

- A. RIP
- B. OSPF
- C. IS-IS
- D. EIGRP
- E. BGP

Answer: ABE

NEW QUESTION 179

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.

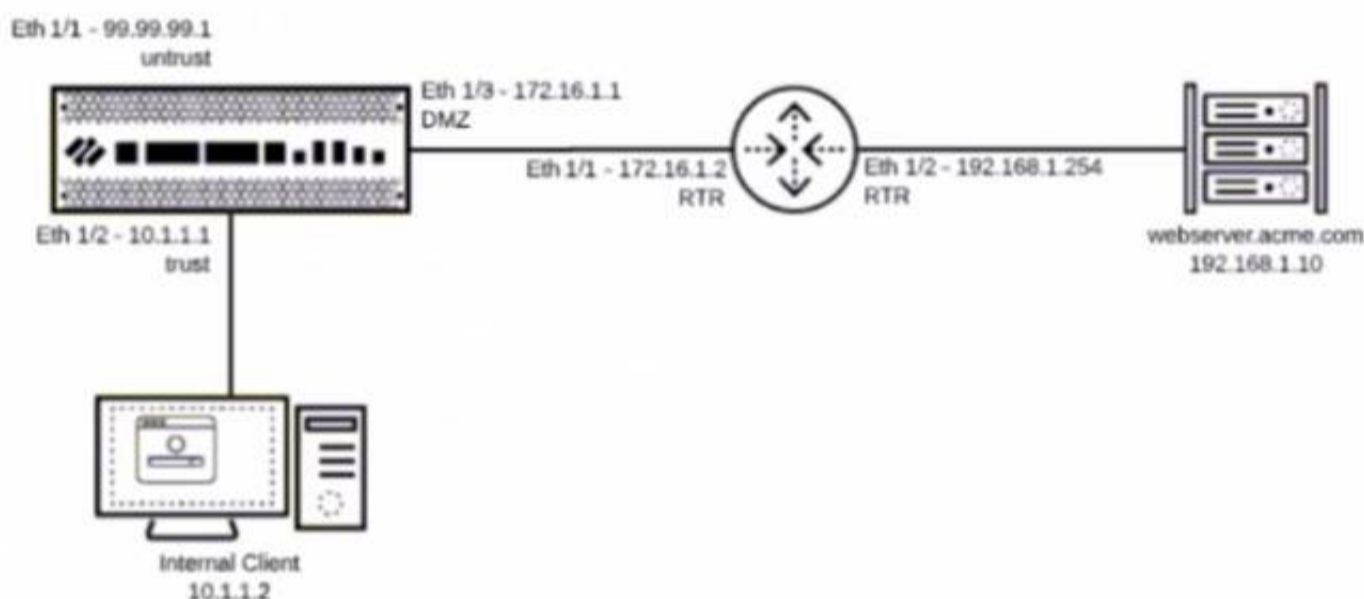
- A. syslog
- B. RADIUS
- C. UID redistribution
- D. XFF headers

Answer: A

NEW QUESTION 180

You have been tasked to configure access to a new web server located in the DMZ

Based on the diagram what configuration changes are required in the NGFW virtual router to route traffic from the 10.1.1.0/24 network to 192.168.1.0/24?



- A. Add a route with the destination of 192.168.1.0/24 using interface Eth 1/3 with a next- hop of 192.168.1.10
- B. Add a route with the destination of 192.168.1.0/24 using interface Eth 1/2 with a next- hop of 172.16.1.2
- C. Add a route with the destination of 192.168.1.0/24 using interface Eth 1/3 with a next- hop of 172.16.1.2
- D. Add a route with the destination of 192.168.1.0/24 using interface Eth 1/3 with a next- hop of 192.168.1.254

Answer: C

NEW QUESTION 182

Where within the firewall GUI can all existing tags be viewed?

- A. Network > Tags
- B. Monitor > Tags
- C. Objects > Tags
- D. Policies > Tags

Answer: C

NEW QUESTION 185

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

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

Answer: A

Explanation:

Reference:<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g00000 0CIVHCA0>

NEW QUESTION 187

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

- A. authentication
- B. decryptionC 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 191

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 193

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 196

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

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

Answer: D

Explanation:

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

NEW QUESTION 197

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 199

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

Explanation:

Reference:

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/user-id/map-ip-addresses-to-users/configureuser-mapping-using-the-windows-user-id-agent/configure-the-windows-based-user-id-agent-for-usermapping.html>

NEW QUESTION 203

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

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

Answer: A

NEW QUESTION 208

Given the screenshot what two types of route is the administrator configuring? (Choose two)

Virtual Router - Static Route - IPv4

Name

0.0.0.0

Destination

0.0.0.0/0

Interface

ethernet1/1

Next Hop

IP Address

10.46.172.1

Admin Distance

10 - 240

Metric

10

Route Table

Unicast

BFD Profile

Disable BFD

☐ Path Monitoring

Failure Condition

☒ Any

☐ All

Preemptive Hold Time (min)

2

☐

NAME

ENABLE

SOURCE IP

DESTINATION IP

PING INTERVAL(SEC)

PING COUNT

- A. default route
- B. OSPF
- C. BGP
- D. static route

Answer: A

NEW QUESTION 213

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 216

Which prevention technique will prevent attacks based on packet count?

- A. zone protection profile
- B. URL filtering profile
- C. antivirus profile
- D. vulnerability profile

Answer: A

NEW QUESTION 220

An administrator is troubleshooting an issue with traffic that matches the intrazone-default rule, which is set to default configuration. What should the administrator do?

- A. Mastered
- B. Not Mastered

Answer: A

NEW QUESTION 222

Files are sent to the WildFire cloud service via the WildFire Analysis Profile. How are these files used?

- A. WildFire signature updates
- B. Malware analysis
- C. Domain Generation Algorithm (DGA) learning
- D. Spyware analysis

Answer: B

NEW QUESTION 225

Starting with PAN-OS version 9.1, application dependency information is now reported in which two locations? (Choose two.)

- A. on the App Dependency tab in the Commit Statuswindow
- B. on the Policy Optimizer'sRule UsagepageC ontheApplication tab in the Security Policy Rulecreation window
- C. ontheObjects>Applicationsbrowser pages

Answer: AC

Explanation:

Reference:<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/app-id/use-application-objects-in-policy/resolve-application-dependencies.html>

NEW QUESTION 227

Recently changes were made to the firewall to optimize the policies and the security team wants to see if those changes are helping. What is the quickest way to reset the hit counter to zero in all the security policy rules?

- A. At the CLI enter the command reset rules and press Enter
- B. Highlight a rule and use the Reset Rule Hit Counter > Selected Rules for each rule
- C. Reboot the firewall
- D. Use the Reset Rule Hit Counter > All Rules option

Answer: D

NEW QUESTION 231

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

PCNSA Practice Exam Features:

- * PCNSA Questions and Answers Updated Frequently
- * PCNSA Practice Questions Verified by Expert Senior Certified Staff
- * PCNSA Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * PCNSA Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

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