



Paloalto-Networks

Exam Questions PCNSA

Palo Alto Networks Certified Network Security Administrator

NEW QUESTION 1

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

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

Answer: C

Explanation:

NEW QUESTION 2

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 lookups 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 3

Which User-ID mapping method should be used for an environment with clients that do not authenticate to Windows Active Directory?

- A. Windows session monitoring via a domain controller
- B. passive server monitoring using the Windows-based agent
- C. Captive Portal
- D. passive server monitoring using a PAN-OS integrated User-ID agent

Answer: C

Explanation:

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/user-id/map-ip-addresses-to-users/map-ip-addresses-to-usernames-using-captive-portal.html>

NEW QUESTION 4

Which two rule types allow the administrator to modify the destination zone? (Choose two)

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

Answer: AC

NEW QUESTION 5

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 6

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 7

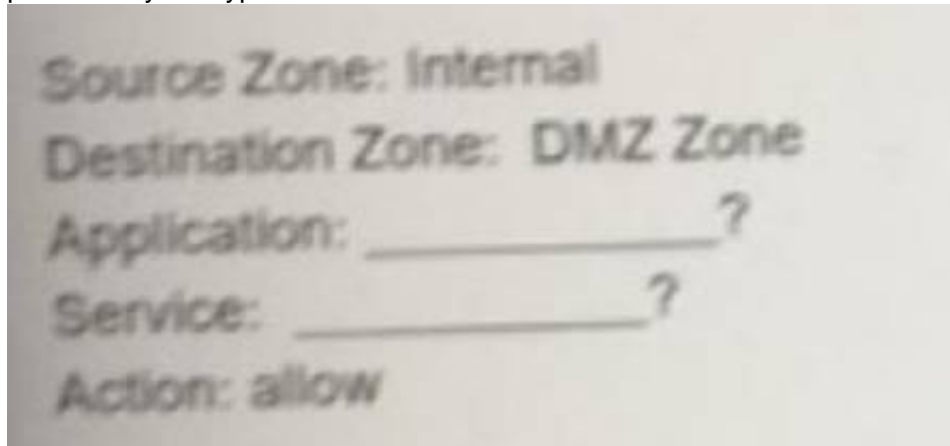
What do you configure if you want to set up a group of objects based on their ports alone?

- A. Application groups
- B. Service groups
- C. Address groups
- D. Custom objects

Answer: B

NEW QUESTION 8

All users from the internal zone must be allowed only Telnet access to a server in the DMZ zone. Complete the two empty fields in the Security Policy rules that permits only this type of access.



Choose two.

A.

Service = "any"

- B. Application = "Telnet"
- C. Service - "application-default"
- D. Application = "any"

Answer: BC

NEW QUESTION 9

Which built-in IP address EDL would be useful for preventing traffic from IP addresses that are verified as unsafe based on WildFire analysis Unit 42 research and data gathered from telemetry?

A.

Palo Alto Networks C&C IP Addresses

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

Answer: D

Explanation:

? Palo Alto Networks Known Malicious IP Addresses

—Contains IP addresses that are verified malicious based on WildFire analysis, Unit 42 research, and data gathered from telemetry (Share ThreatIntelligence with Palo Alto Networks). Attackers use these IP addresses almost exclusively to distribute malware, initiate command-and-control activity, and launch attacks.

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/policy/use-an-external-dynamic-list-in-policy/built-in-edls>

NEW QUESTION 10

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 10

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 12

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

Answer: B

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

Device SN 007251000516345	Interface ethernet1/4	NAT IP 8.8.4.4
IP Protocol udp	NAT IP 67.290.64.58	NAT Port 53
Log Action global-logs	NAT Port 26351	
Generated Time 2021/08/27 02:02:49	X-Forwarded-For IP 0.0.0.0	
Receive Time 2021/08/27 02:02:53		
Tunnel Type Null		
	Details	Flags
	Threat Type spyware	Captive Portal <input type="checkbox"/>
	Threat ID/Name Phishing:151.116.74.in-addr.arpa	Proxy Transaction <input type="checkbox"/>
	ID 109010001 (View in Threat Vault)	Decrypted <input type="checkbox"/>
	Category dns-phishing	Packet Capture <input type="checkbox"/>
	Content Version AppThreat-0-0	Client to Server <input checked="" type="checkbox"/>
	Severity low	Server to Client <input type="checkbox"/>
	Repeat Count 2	Tunnel Inspected <input type="checkbox"/>
	File Name	DeviceID
	URL 151.116.74.in-addr.arpa	Source Device Category Virtual Machine
	Partial Hash 0	Source Device Profile VMware
	Prap ID 0	Source Device Model
	Source UUID	Source Device Vendor VMware, Inc.
	Destination UUID	Source Device OS Family
	Dynamic User Group	Source Device OS Version
	Network Slice ID SST 0	Source Device Host ubuntu-server
	Network Slice ID SD	Source Device MAC 00:50:56:a2:19:a3
	App Category networking	Destination Device Category
	App Subcategory infrastructure	Destination Device Profile
	App Technology network-protocol	Destination Device Model
	App Characteristic used-by-malware-has-known-vulnerability-periodic-use	
	App Container	
	App Risk 3	

- A. It was blocked by the Vulnerability Protection profile action.
- B. It was blocked by the Anti-Virus Security profile action.
- C. It was blocked by the Anti-Spyware Profile action.
- D. It was blocked by the Security policy action.

Answer: C

NEW QUESTION 21

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

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

Answer: BC

NEW QUESTION 25

An administrator is implementing an exception to an external dynamic list by adding an entry to the list manually. The administrator wants to save the changes, but the OK button is grayed out.

What are two possible reasons the OK button is grayed out? (Choose two.)

- A. The entry contains wildcards.
- B. The entry is duplicated.
- C. The entry doesn't match a list entry.
- D. The entry matches a list entry.

Answer: BC

NEW QUESTION 30

At which point in the app-ID update process can you determine if an existing policy rule is affected by an app-ID update?

- A.

after clicking Check New in the Dynamic Update window

- B. after connecting the firewall configuration
- C. after downloading the update
- D. after installing the update

Answer: A

Explanation:

Reference: <https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/device/device-dynamicupdates>

NEW QUESTION 32

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 36

Which stage of the cyber-attack lifecycle makes it important to provide ongoing education to users on spear phishing links, unknown emails, and risky websites?

- A. reconnaissance
- B. delivery
- C. exploitation
- D. installation

Answer: B

Explanation:

Weaponization and Delivery: Attackers will then determine which methods to use in order to deliver malicious payloads. Some of the methods they might utilize are automated tools, such as exploit kits, spear phishing attacks with malicious links, or attachments and malvertizing.

? Gain full visibility into all traffic, including SSL, and block high-risk applications.

Extend those protections to remote and mobile devices.

? Protect against perimeter breaches by blocking malicious or risky websites through URL filtering.

? Block known exploits, malware and inbound command-and-control communications using multiple threat prevention disciplines, including IPS, anti-malware, anti-CnC, DNS monitoring and sinkholing, and file and content blocking.

? Detect unknown malware and automatically deliver protections globally to thwart new attacks.

? Provide ongoing education to users on spear phishing links, unknown emails, risky websites, etc.

<https://www.paloaltonetworks.com/cyberpedia/how-to-break-the-cyber-attack-lifecycle>

NEW QUESTION 37

Which license must an administrator acquire prior to downloading Antivirus updates for use with the firewall?

- A. URL filtering

- B. Antivirus
- C. WildFire
- D. Threat Prevention

Answer: D

NEW QUESTION 41

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 45

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

Explanation:

Explanation/Reference: Reference:
<https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-web-interface-help/objects/objects- application- filters>

NEW QUESTION 47

Which DNS Query action is recommended for traffic that is allowed by Security policy and matches Palo Alto Networks Content DNS Signatures?

- A. block
- B. sinkhole
- C. alert
- D. allow

Answer: B

Explanation:

To enable DNS sinkholing for domain queries using DNS security, you must activate your DNS Security subscription, create (or modify) an Anti-Spyware policy to reference the DNS Security service, configure the log severity and policy settings for each DNS signature category, and then attach the profile to a security policy rule. <https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/threat-prevention/dns- security/enable-dns-security>

NEW QUESTION 48

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

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

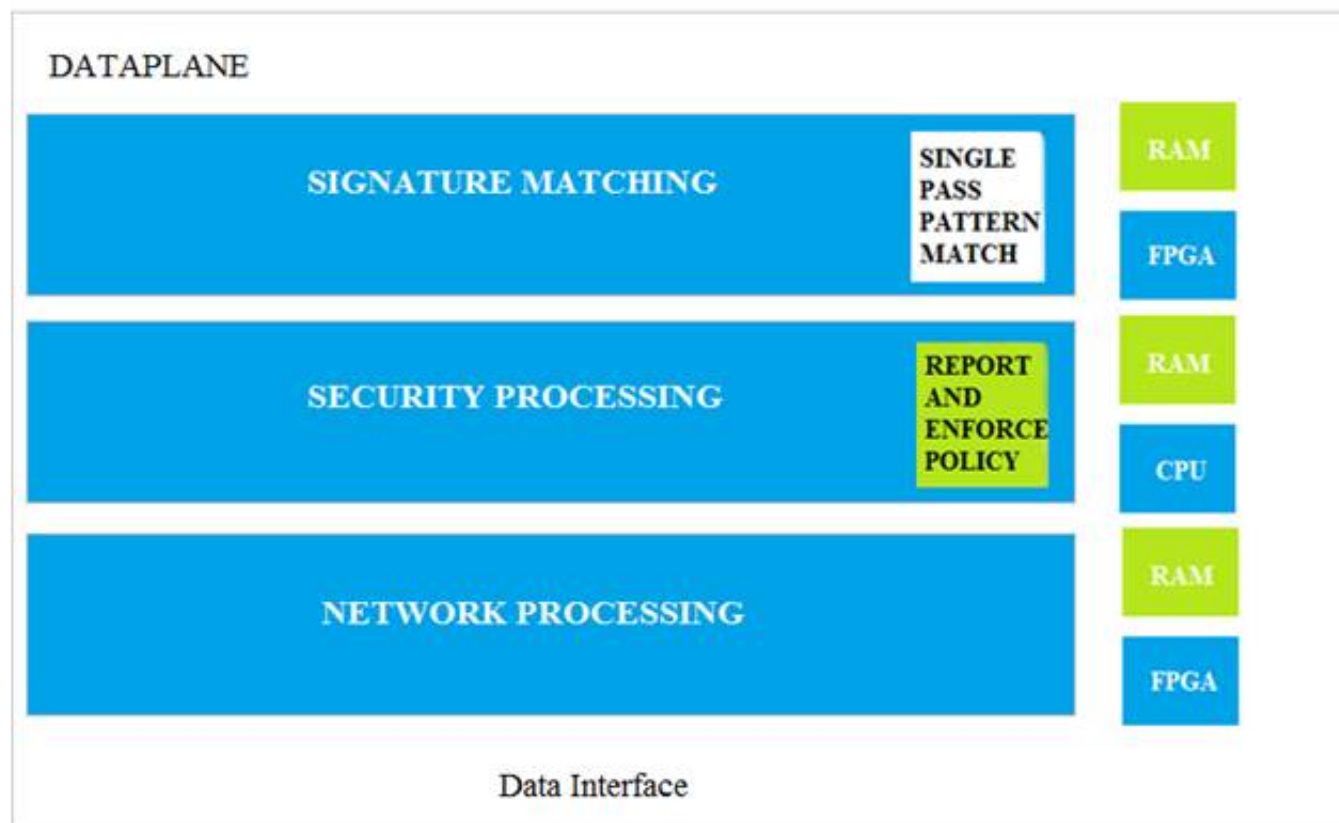
Answer: B

Explanation:

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

NEW QUESTION 51

Which data-plane processor layer of the graphic shown provides uniform matching for spyware and vulnerability exploits on a Palo Alto Networks Firewall?



- A. Signature Matching
- B. Network Processing
- C. Security Processing
- D. Security Matching

Answer: A

NEW QUESTION 54

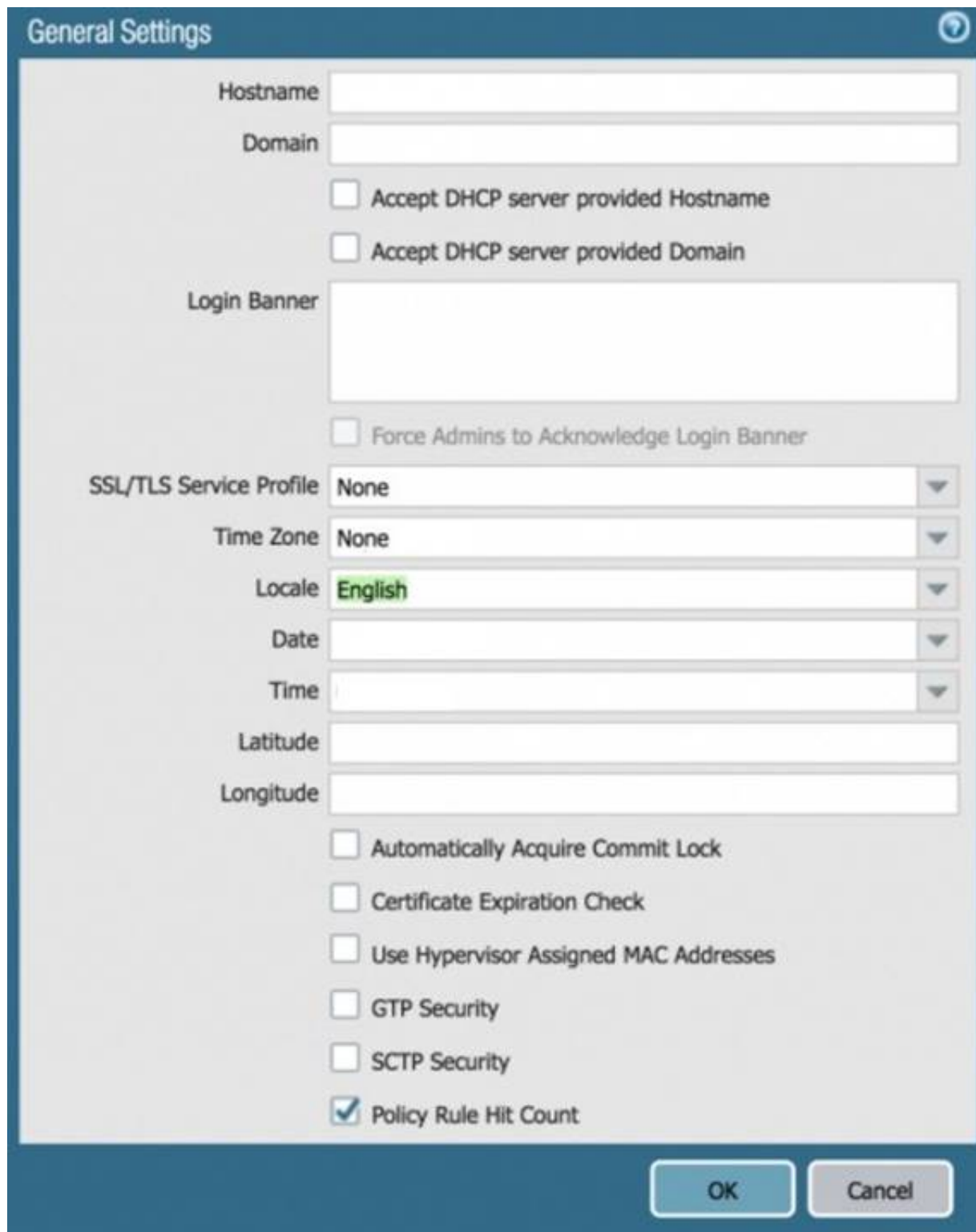
An administrator configured a Security policy rule with an Antivirus Security profile. The administrator did not change the action (or the profile. If a virus gets detected, how will the firewall handle the traffic?

- 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 55

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 the following fields and options:

- Hostname: [Text Field]
- Domain: [Text Field]
- ☐ Accept DHCP server provided Hostname
- ☐ Accept DHCP server provided Domain
- Login Banner: [Text Field]
- ☐ Force Admins to Acknowledge Login Banner
- SSL/TLS Service Profile: [Dropdown Menu, None selected]
- Time Zone: [Dropdown Menu, None selected]
- Locale: [Dropdown Menu, English selected]
- Date: [Dropdown Menu]
- Time: [Dropdown Menu]
- Latitude: [Text Field]
- Longitude: [Text Field]
- ☐ Automatically Acquire Commit Lock
- ☐ Certificate Expiration Check
- ☐ Use Hypervisor Assigned MAC Addresses
- ☐ GTP Security
- ☐ SCTP Security
- ☒ Policy Rule Hit Count

Buttons: OK, Cancel

- 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=kA10g00000 0CIFGCA0>

NEW QUESTION 57

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 60

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 62

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 63

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

- A. Mastered
- B. Not Mastered

Answer: A

NEW QUESTION 65

During the packet flow process, which two processes are performed in application identification? (Choose two.)

- A. pattern based application identification
- B. application override policy match
- C. session application identified
- D. application changed from content inspection

Answer: AB

Explanation:

Reference: <http://live.paloaltonetworks.com/t5/image/serverpage/image-id/12862i950F549C7D4E6309>

NEW QUESTION 67

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

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

Answer: C

Explanation:

Reference:

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

NEW QUESTION 72

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 77

Which interface type can use virtual routers and routing protocols?

- A. Tap
- B. Layer3
- C. Virtual Wire
- D. Layer2

Answer: B

NEW QUESTION 82

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

- A. Biometric scanning results from iOS devices
- B. Firewall logs

- C. Custom API scripts
- D. Security Information and Event Management Systems (SIEMS), such as Splun
- E. DNS Security service

Answer: BCE

NEW QUESTION 86

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 89

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

- ~~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 92

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

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

Answer: D

NEW QUESTION 97

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 98

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

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

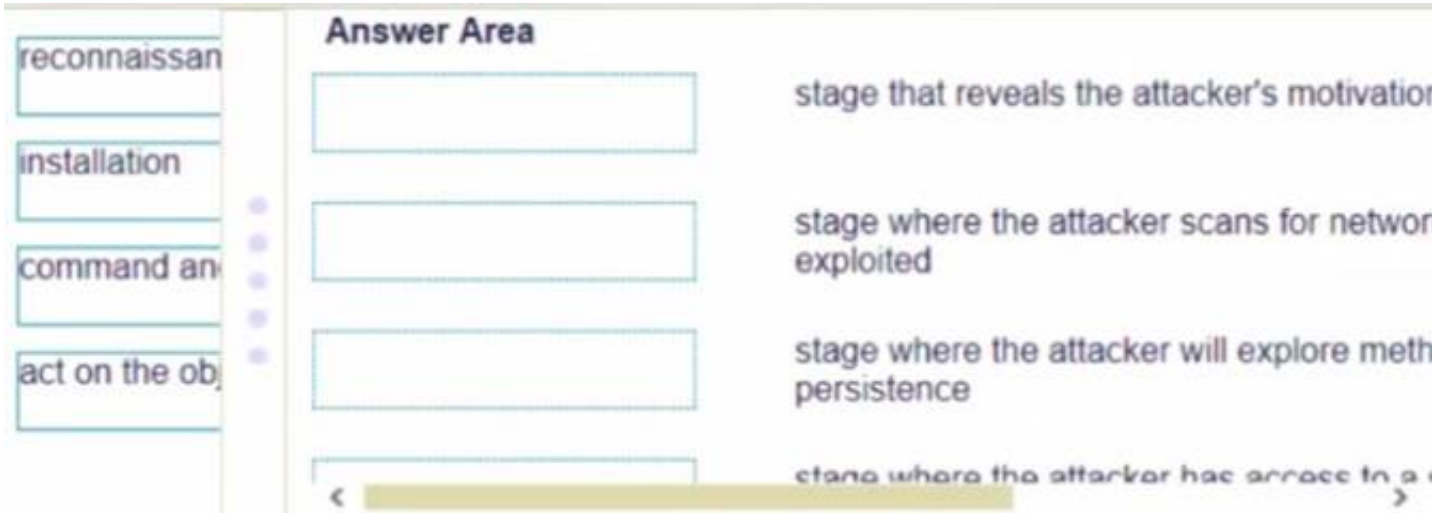
Answer: D

Explanation:

NEW QUESTION 103

DRAG DROP

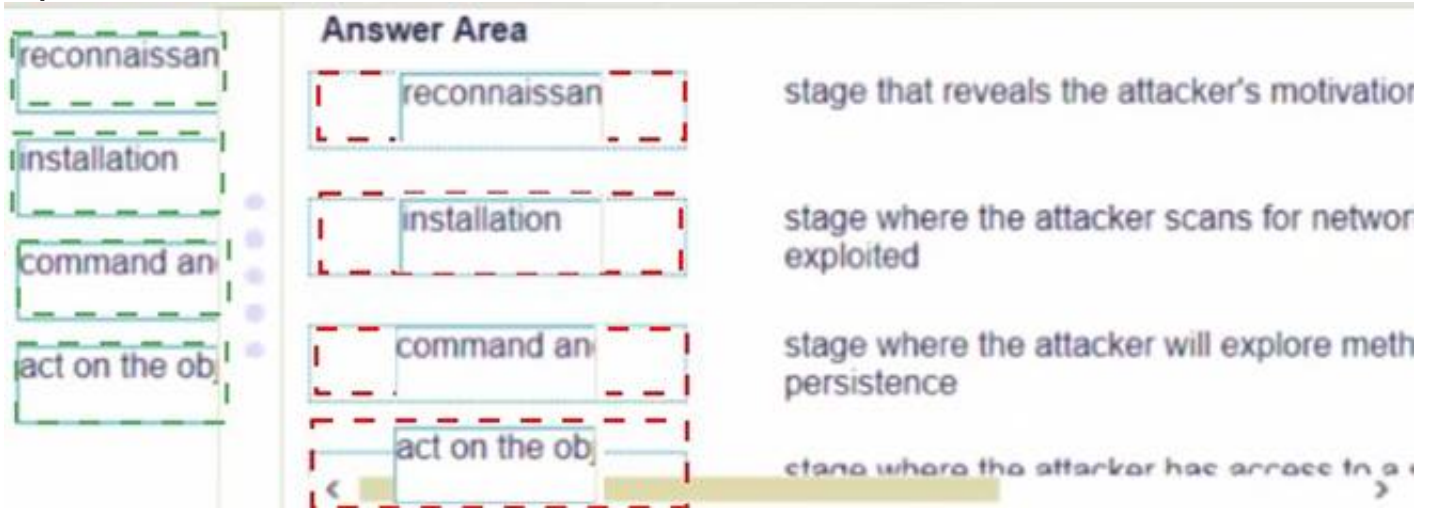
Match the cyber-attack lifecycle stage to its correct description.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 107

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 108

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 113

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 114

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

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

Answer: A

Explanation:

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

NEW QUESTION 119

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 122

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

	Name	Tags	Type	Source			Destination			Rate/Usage			Application	Service	Action	Profile
				Zone	Address	User	HIP Profile	Zone	Address	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

The Allow Office Programs rule is using an Application Filter

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

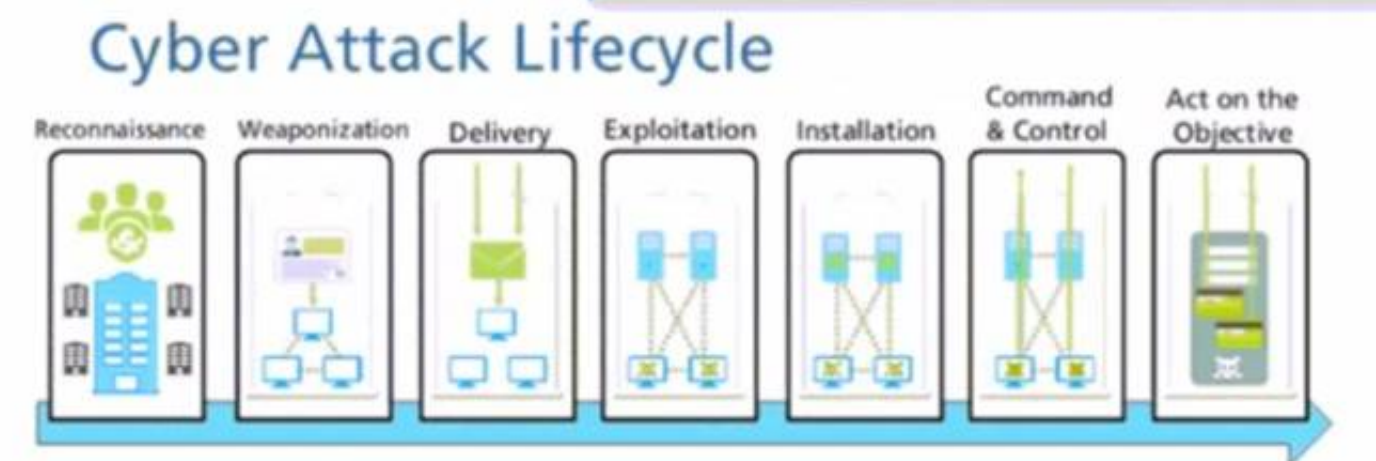
Answer: AD

Explanation:

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

NEW QUESTION 125

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



delivery

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

E. installation

Answer: A

NEW QUESTION 130

What is the purpose of the automated commit recovery feature?

- A. It reverts the Panorama configuration.
- B. It causes HA synchronization to occur automatically between the HA peers after a push from Panorama.
- C. It reverts the firewall configuration if the firewall recognizes a loss of connectivity to Panorama after the change.
- D. It generates a config log after the Panorama configuration successfully reverts to the last running configuration.

Answer: C

Explanation:

Reference: <https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/administer-panorama/enable-automated-commit-recovery.html>

NEW QUESTION 132

An administrator is reviewing the Security policy rules shown in the screenshot below. Which statement is correct about the information displayed?



- A. Eleven rules use the "Infrastructure*" tag.
- B. The view Rulebase as Groups is checked.
- C. There are seven Security policy rules on this firewall.
- D. Highlight Unused Rules is checked.

Answer: B

Explanation:

NEW QUESTION 133

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 134

An administrator would like to apply a more restrictive Security profile to traffic for file sharing applications. The administrator does not want to update the Security policy or object when new applications are released. Which object should the administrator use as a match condition in the Security policy?

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

Answer: D

NEW QUESTION 135

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

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

Answer: C

NEW QUESTION 136

Which statement best describes a common use of Policy Optimizer?

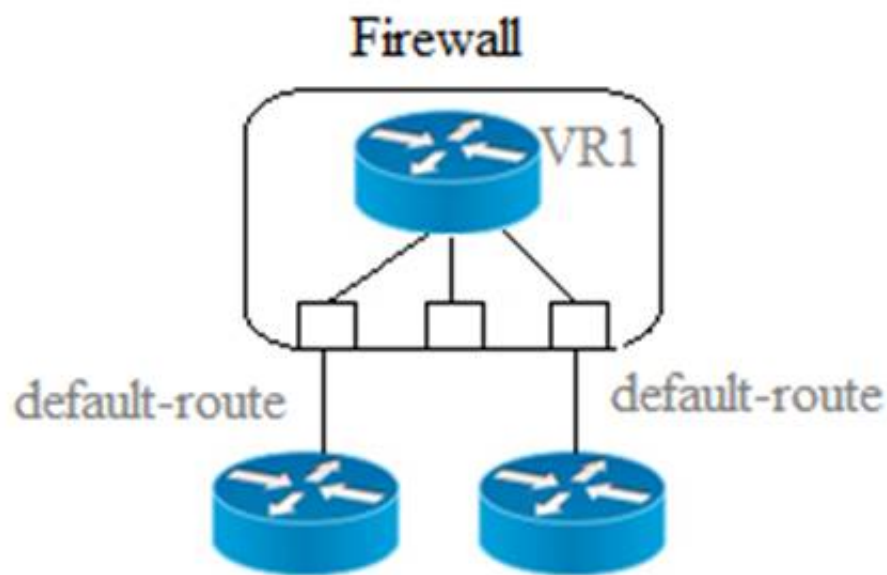
- A. Policy Optimizer on a VM-50 firewall can display which Layer 7 App-ID Security policies have unused applications.
- B. Policy Optimizer can add or change a Log Forwarding profile for each Security policy selected.
- C. Policy Optimizer can display which Security policies have not been used in the last 90 days.
- D. Policy Optimizer can be used on a schedule to automatically create a disabled Layer 7 App-ID Security policy for every Layer 4 policy that exist
- E. Admins can then manually enable policies they want to keep and delete ones they want to remove.

Answer: C

NEW QUESTION 137

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

Multiple Static Default Routes



- A. Path monitoring does not determine if route is useable
- B. 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 138

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

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

Answer: B

NEW QUESTION 140

An administrator wishes to follow best practices for logging traffic that traverses the firewall Which log setting is correct?

- A. Disable all logging
- B. Enable Log at Session End
- C. Enable Log at Session Start
- D. Enable Log at both Session Start and End

Answer: B

Explanation:

Reference:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Clt5CAC>

NEW QUESTION 145

Why does a company need an Antivirus profile?

- A. Mastered
- B. Not Mastered

Answer: A

NEW QUESTION 146

Which type of administrative role must you assign to a firewall administrator account, if the account must include a custom set of firewall permissions?

- A. SAML
- B. Multi-Factor Authentication
- C. Role-based
- D. Dynamic

Answer: C

Explanation:

Reference:<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/firewall-administration/manage-firewall-administrators/administrative-role-types.html>

NEW QUESTION 147

A website is unexpectedly allowed due to miscategorization.

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

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

Answer: CD

NEW QUESTION 149

Your company is highly concerned with their Intellectual property being accessed by unauthorized resources. There is a mature process to store and include metadata tags for all confidential documents.

Which Security profile can further ensure that these documents do not exit the corporate network?

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

Answer: B

Explanation:

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

NEW QUESTION 153

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

- A. authentication
- B. decryption
- C. application override
- D. 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 155

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 160

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 161

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 164

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 167

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

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

Answer: AB

NEW QUESTION 171

DRAG DROP

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 176

Access to which feature requires PAN-OS Filtering licens?

- A. PAN-DB database
- B. URL external dynamic lists

- C. Custom URL categories
- D. DNS Security

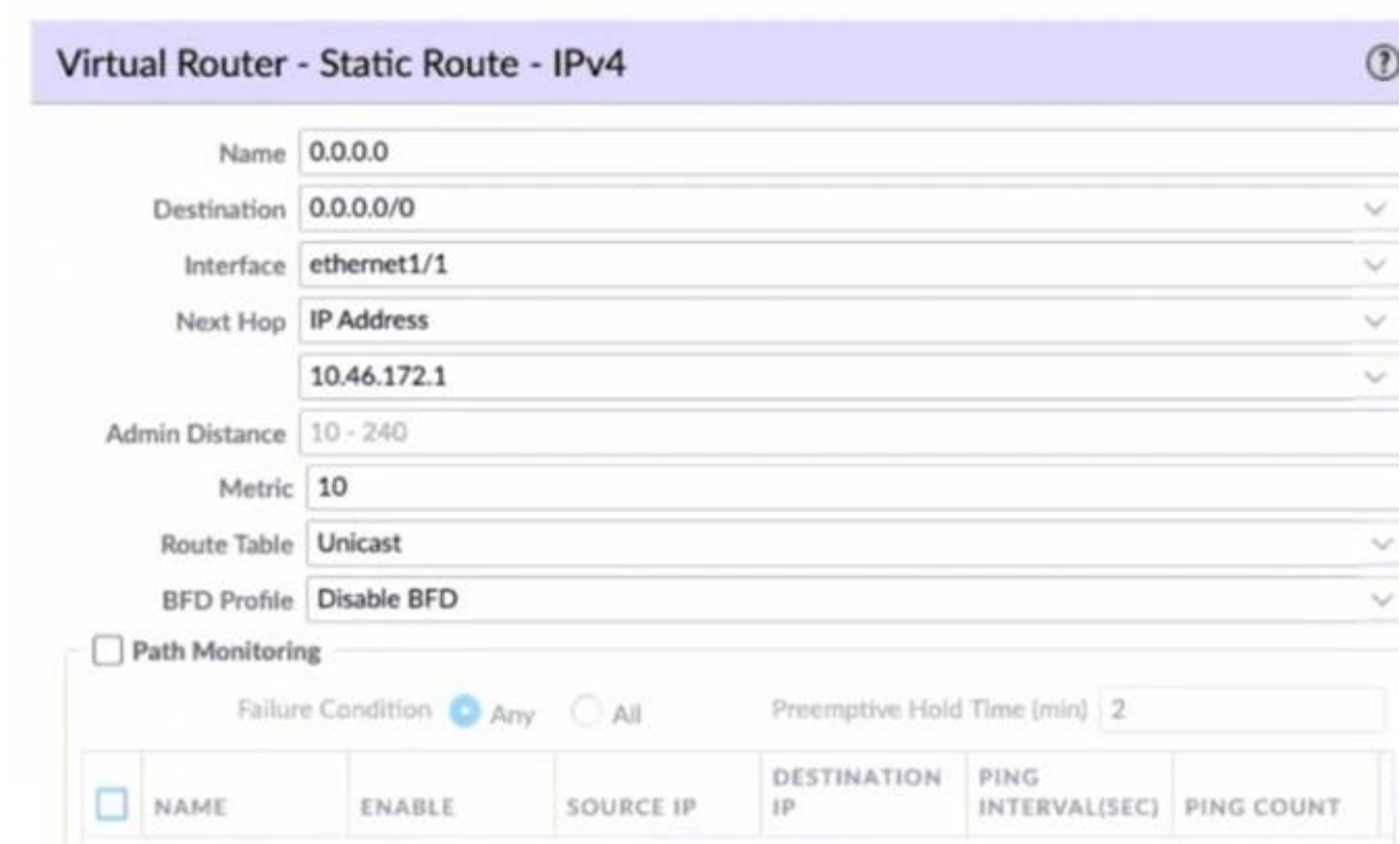
Answer: A

Explanation:

Reference:<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/getting-started/activate-licenses-and-subscriptions.html>

NEW QUESTION 180

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

<input type="checkbox"/>	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 185

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 189

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 192

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 197

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

Explanation:

Reference:

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/threat-prevention/dns-security/enable-dnssecurity.html>

NEW QUESTION 198

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 Status window
- B. on the Policy Optimizer's Rule Usage page
- C. on the Application tab in the Security Policy Rule creation window
- D. on the Objects > Applications browser 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 201

.....

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](#)