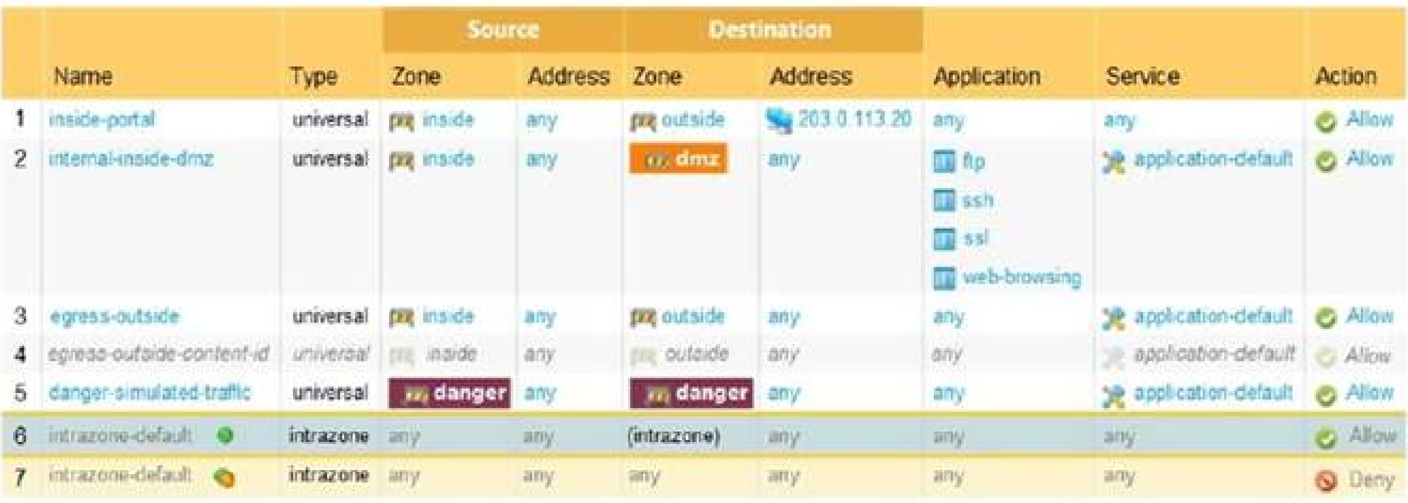
Paloalto-Networks

Exam Questions PCNSA

Palo Alto Networks Certified Network Security Administrator

NEW QUESTION 1
Based on the show security policy rule would match all FTP traffic from the inside zone to the outside zone?



			Source		Destination				
	Name	Type	Zone	Address	Zone	Address	Application	Service	Action
1	inside-portal	universal	inside	any	outside	203.0.113.20	any	any	Allow
2	internal-inside-dmz	universal	inside	any	dmz	any	ftp ssh ssl web-browsing	application-default	Allow
3	egress-outside	universal	inside	any	outside	any	any	application-default	Allow
4	egress-outside-content-id	universal	inside	any	outside	any	any	application-default	Allow
5	danger-simulated-traffic	universal	danger	any	danger	any	any	application-default	Allow
6	intrazone-default	intrazone	any	any	(intrazone)	any	any	any	Allow
7	intrazone-default	intrazone	any	any	any	any	any	any	Deny

A. internal-inside-dmz
B. engress outside
C. inside-portal
D. intercone-default

Answer: B

NEW QUESTION 2
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 rote
D. server profile

Answer: CD

NEW QUESTION 3
Which object would an administrator create to enable access to all applications in the office-programs subcategory?

A. HIP profile
B. Application group
C. URL category
D. Application filter

Answer: C

NEW QUESTION 4
Which action related to App-ID updates will enable a security administrator to view the existing security policy rule that matches new application signatures?

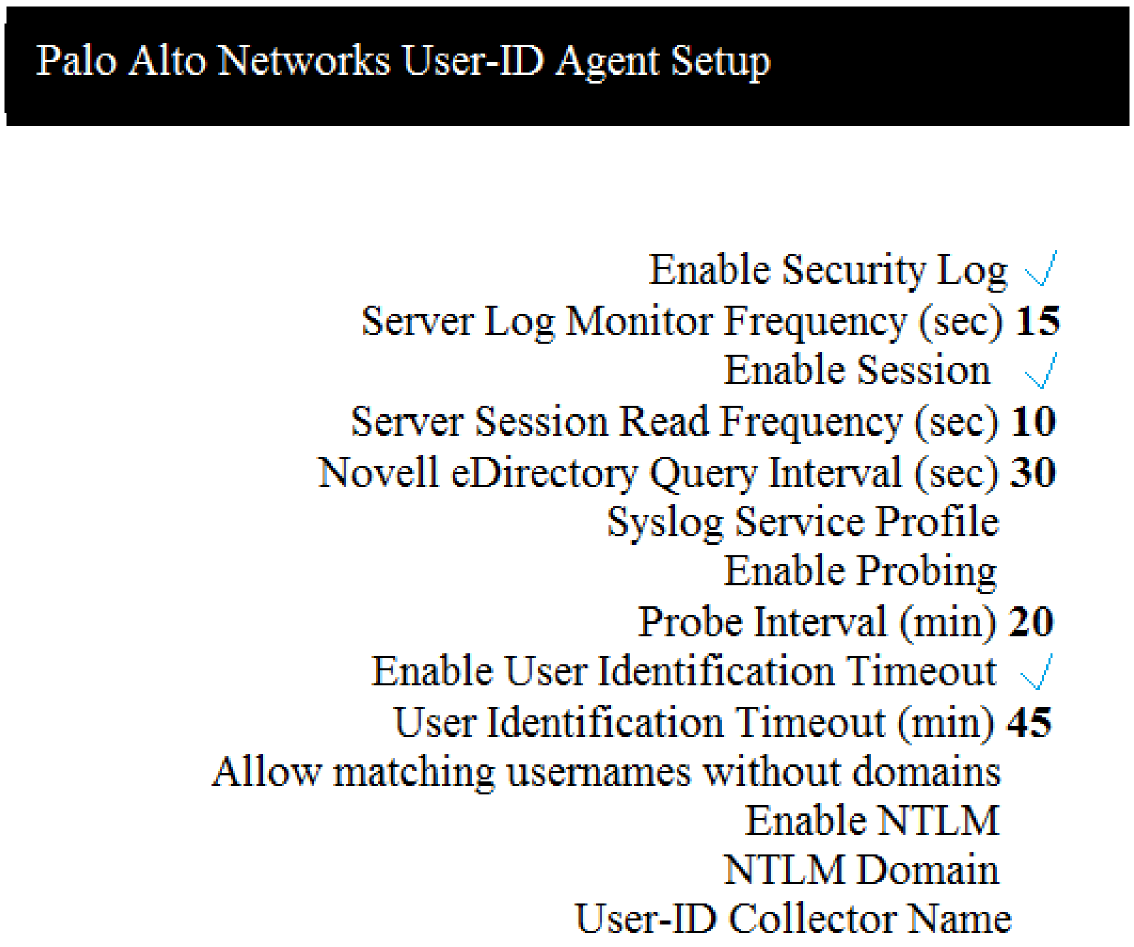
A. Review Policies
B. Review Apps
C. Pre-analyze
D. Review App Matches

Answer: A

Explanation:
References:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/app-id/manage-new- app-ids-introduced- incontent-releases/review-new-app-id-impact-on- existing-policy-rules

NEW QUESTION 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
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 Secunty 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 7
What can be achieved by selecting a policy target prior to pushing policy rules from Panorama?

A. Doing so limits the templates that receive the policy rules
B. Doing so provides audit information prior to making changes for selected policy rules
C. You can specify the firewalls m a device group to which to push policy rules
D. You specify the location as pre can - or post-rules to push policy rules

Answer: C

NEW QUESTION 8
What two authentication methods on the Palo Alto Networks firewalls support authentication and authorization for role-based access control? (Choose two.)

A. SAML
B. TACACS+
C. LDAP
D. Kerberos

Answer: AB

Explanation:

Reference:https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/firewall-administration/manage-firewall-administrators/administrative-authentication.html
The administrative accounts are defined on an external SAML, TACACS+, or RADIUS server. The server performs both authentication and authorization. For authorization, you define Vendor-Specific Attributes (VSAs) on the TACACS+ or RADIUS server, or SAML attributes on the SAML server. PAN-OS maps the attributes to administrator roles, access domains, user groups, and virtual systems that you define on the firewall.

NEW QUESTION 9
Which two App-ID applications will need to be allowed to use Facebook-chat? (Choose two.)

A. facebook
B. facebook-chat
C. facebook-base
D. facebook-email

Answer: BC

NEW QUESTION 10
An administrator is implementing an exception to an external dynamic list by adding an entry to the list manually. The administrator wants to save the changes, but the OK button is grayed out.
What are two possible reasons the OK button is grayed out? (Choose two.)

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

Answer: BC

NEW QUESTION 10
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 14
Which option is part of the content inspection process?

A. IPsec tunnel encryption
B.

Packet egress process
C. SSL Proxy re-encrypt
D. Packet forwarding process

Answer: C

NEW QUESTION 15
By default, which action is assigned to the interzone-default rule?

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

Answer: C

NEW QUESTION 16
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 20
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 24
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 25
What is the minimum timeframe that can be set on the firewall to check for new WildFire signatures?

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

Answer: D

NEW QUESTION 28
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 33
You receive notification about new malware that infects hosts through malicious files transferred by FTP.
Which Security profile detects and protects your internal networks from this threat after you update your firewall's threat signature database?

A. URL Filtering profile applied to inbound Security policy rules.
B. Data Filtering profile applied to outbound Security policy rules.
C. Antivirus profile applied to inbound Security policy rules.
D. Vulnerability Protection profile applied to outbound Security policy rules.

Answer: C

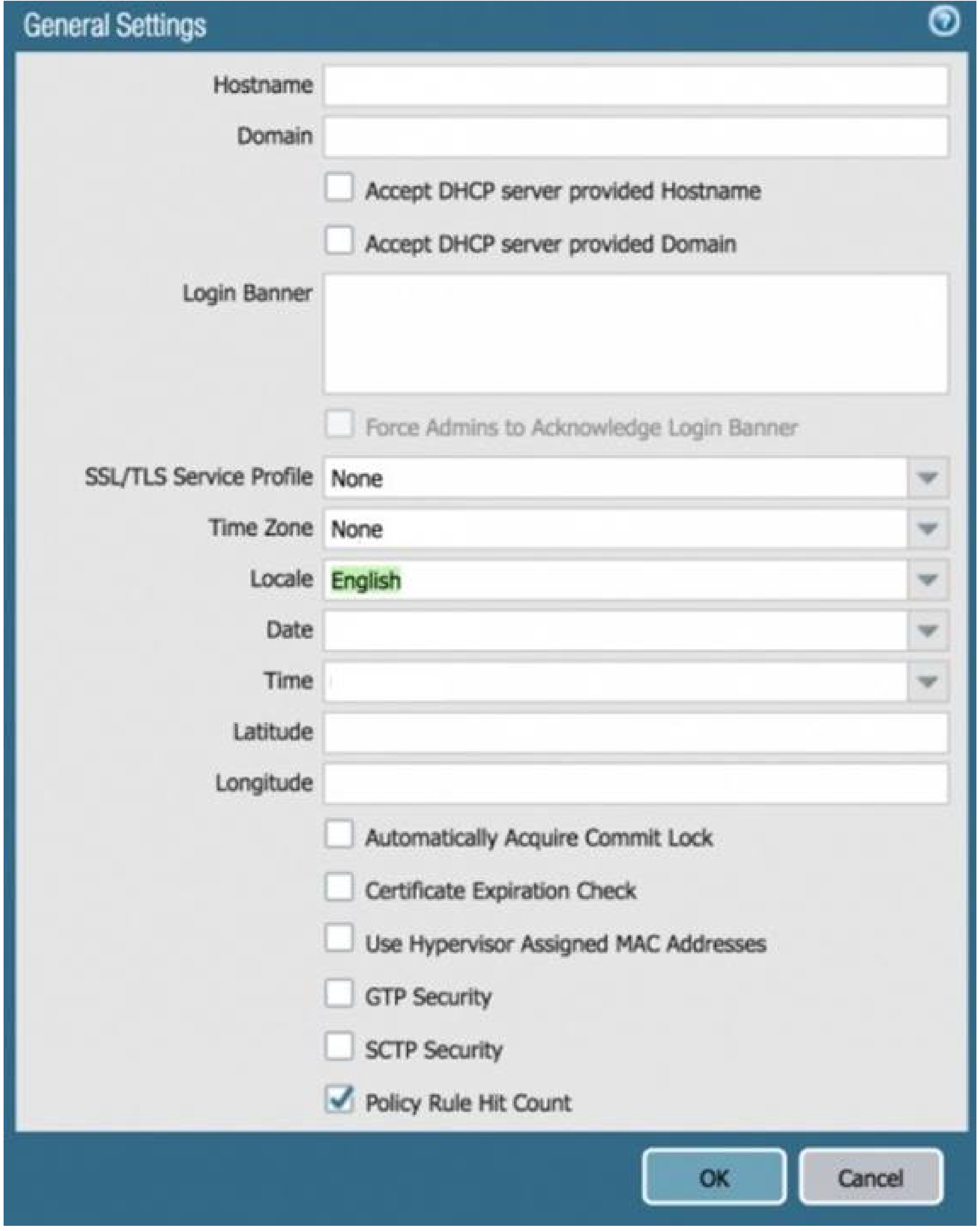
Explanation:
Reference:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/security-profiles

NEW QUESTION 34
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 35
Based on the graphic, what is the purpose of the SSL/TLS Service profile configuration option?



General Settings

Hostname

Domain

□ Accept DHCP server provided Hostname

□ Accept DHCP server provided Domain

Login Banner

□ Force Admins to Acknowledge Login Banner

SSL/TLS Service Profile: None

Time Zone: None

Locale: English

Date

Time

Latitude

Longitude

□ Automatically Acquire Commit Lock

□ Certificate Expiration Check

□ Use Hypervisor Assigned MAC Addresses

□ GTP Security

□ SCTP Security

☑ Policy Rule Hit Count

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 0ClFGCA0

NEW QUESTION 39
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

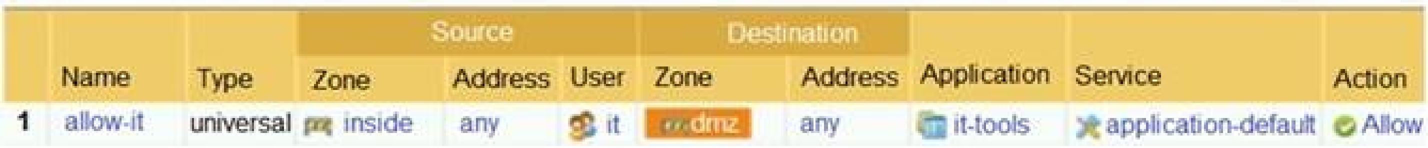
Explanation:
? If you have Universal Groups, create an LDAP server profile to connect to the root domain of the Global Catalog server on port 3268 or 3269 for SSL, then create another LDAP server profile to connect to the root domain controllers on port 389. This helps ensure that users and group information 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 44
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 46
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 51
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 verity

Answer: C

Explanation:

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

NEW QUESTION 52
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 55
Which administrator type provides more granular options to determine what the administrator can view and modify when creating an administrator account?

A. Root
B. Dynamic
C. Role-based
D. Superuser

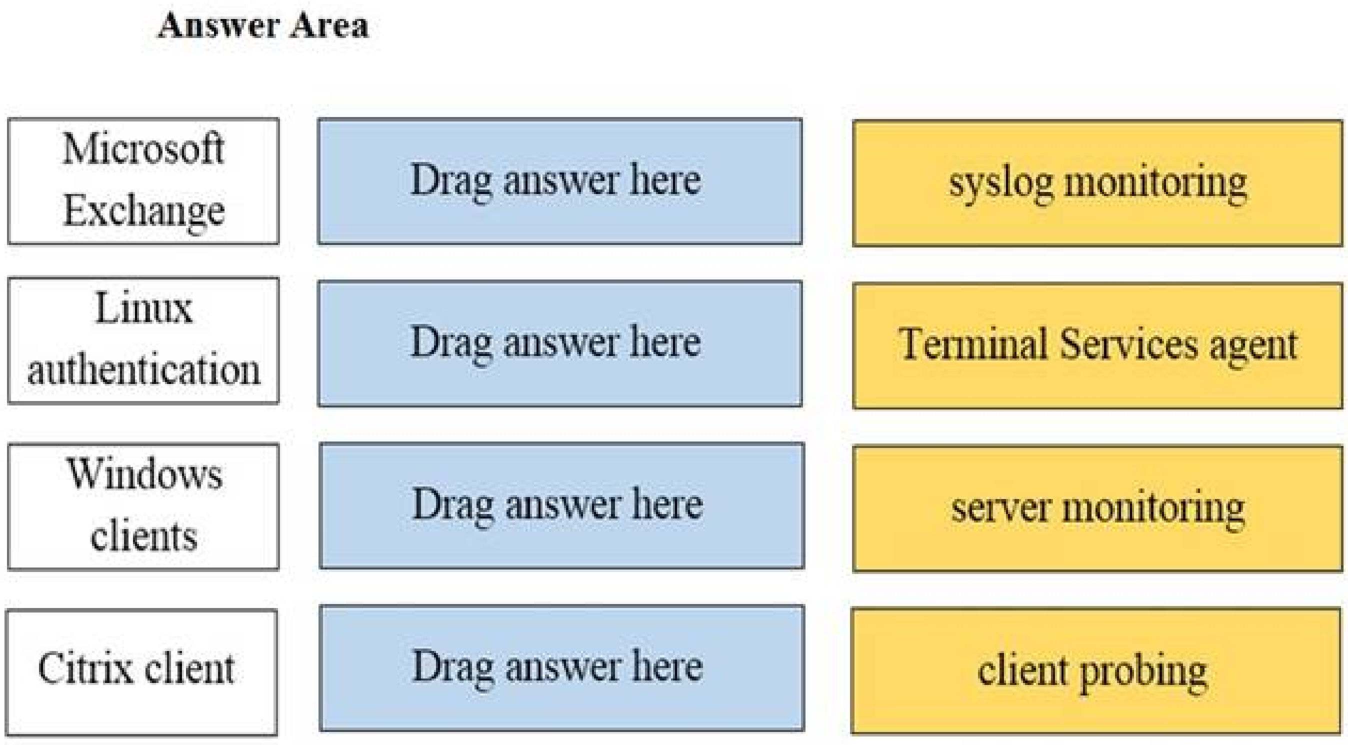
Answer: C

NEW QUESTION 58
Which license must an Administrator acquire prior to downloading Antivirus Updates for use with the firewall?

A. Threat Prevention License
B. Threat Implementation License
C. Threat Environment License
D. Threat Protection License

Answer: A

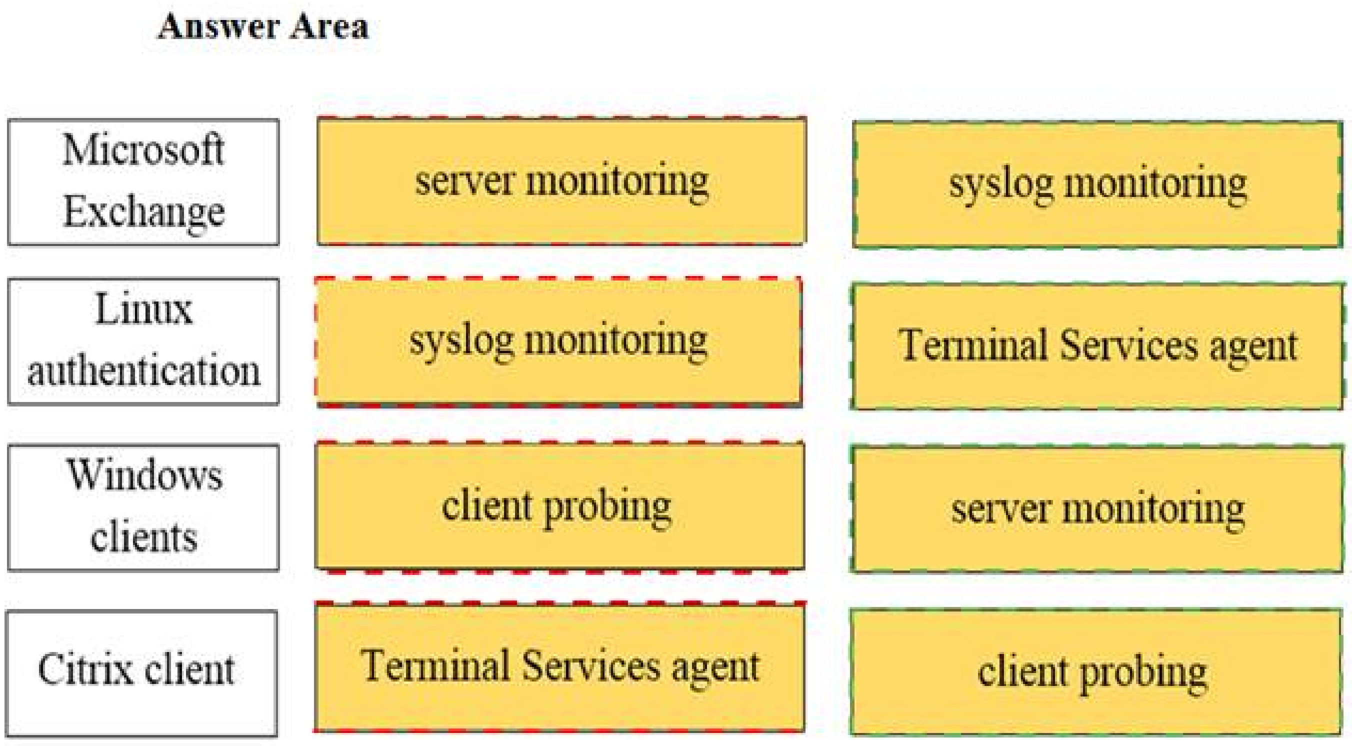
NEW QUESTION 59
DRAG DROP
Match the network device with the correct User-ID technology.



Answer Area

Microsoft Exchange	Drag answer here	syslog monitoring
Linux authentication	Drag answer here	Terminal Services agent
Windows clients	Drag answer here	server monitoring
Citrix client	Drag answer here	client probing

Answer:



Answer Area

Microsoft Exchange	server monitoring	syslog monitoring
Linux authentication	syslog monitoring	Terminal Services agent
Windows clients	client probing	server monitoring
Citrix client	Terminal Services agent	client probing

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Microsoft Exchange – Server monitoring
Linux authentication – syslog monitoring
Windows Client – client probing
Citrix client – Terminal Services agent

NEW QUESTION 61
When creating a custom URL category object, which is a valid type?

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

Answer: D

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

NEW QUESTION 64
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 67
What is the main function of Policy Optimizer?

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

Answer: D

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

NEW QUESTION 70
Which path in PAN-OS 10.0 displays the list of port-based security policy rules?

A. Policies> Security> Rule Usage> No App Specified
B. Policies> Security> Rule Usage> Port only specified
C. Policies> Security> Rule Usage> Port-based Rules
D. Policies> Security> Rule Usage> Unused Apps

Answer: A

Explanation:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/app-id/security-policy-rule-optimization/migrate-port-based-to-app-id-based-security-policy-rules.html

NEW QUESTION 71
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=kA10g000000ClN7CAK

NEW QUESTION 73
What is the maximum volume of concurrent administrative account sessions?

A. Unlimited
B. 2
C. 10
D. 1

Answer: C

NEW QUESTION 77
Which service protects cloud-based applications such as Dropbox and Salesforce by administering permissions and scanning files for sensitive information?

A. Aperture
B. AutoFocus
C. Parisma SaaS
D. GlobalProtect

Answer: C

NEW QUESTION 78
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

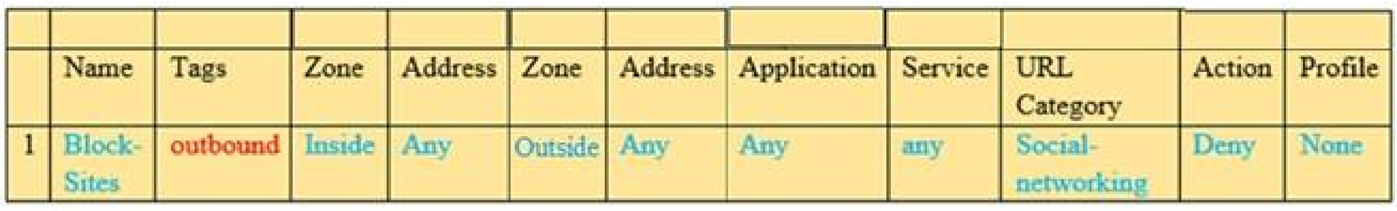
Explanation:
? An Anti-Spyware security profile is a set of rules that defines how the firewall detects and prevents spyware from compromising hosts on the network. Spyware is a type of malware that collects information from the infected system, such as keystrokes, browsing history, or personal data, 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 82
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 84
In the example security policy shown, which two websites fcked? (Choose two.)



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

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

Answer: AB

NEW QUESTION 86
What are three Palo Alto Networks best practices when implementing the DNS Security Service? (Choose three.)

A. Implement a threat intel program.
B. Configure a URL Filtering profile.
C. Train your staff to be security aware.
D. Rely on a DNS resolver.
E. Plan for mobile-employee risk

Answer: ABD

NEW QUESTION 90
Which administrative management services can be configured to access a management interface?

A. HTTP, CLI, SNMP, HTTPS
B. HTTPS, SSH telnet SNMP
C. SSH: telnet HTTP, HTTPS
D. HTTPS, HTT
E. CLI, API

Answer: D

Explanation:
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/firewall-administration/management-interfaces
You can use the following user interfaces to manage the Palo Alto Networks firewall:
? Use the Web Interface to perform configuration and monitoring tasks with relative ease. This graphical interface allows you to access the firewall using HTTPS

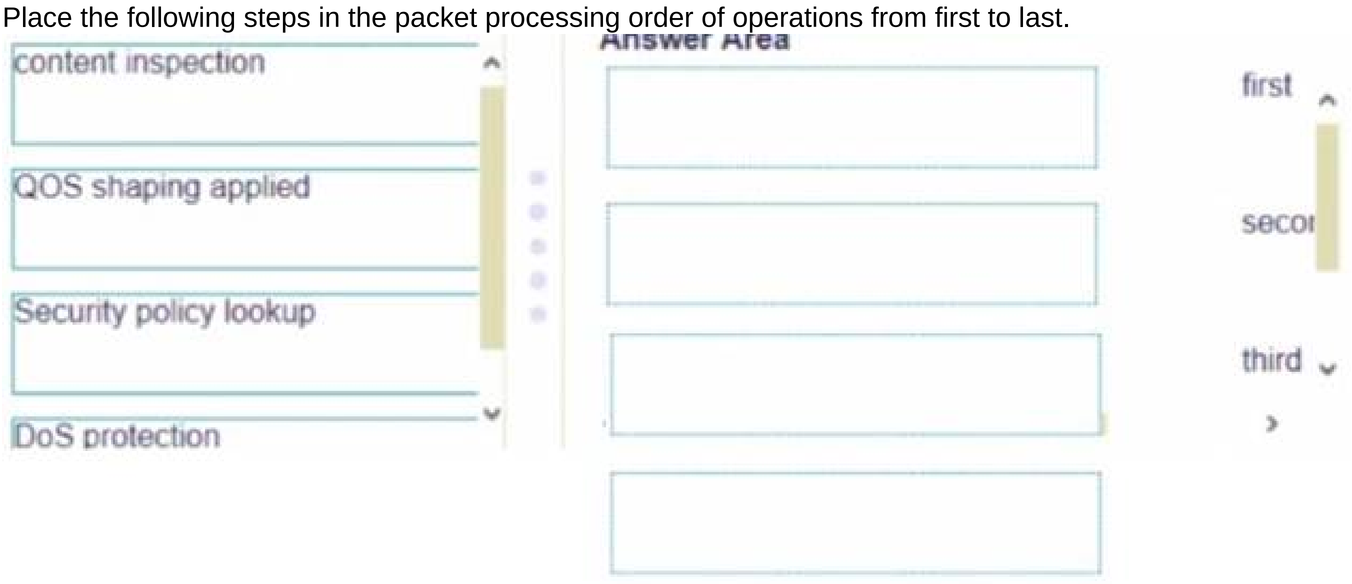
(recommended) or HTTP and it is the best way to perform administrative tasks.
? Use the Command Line Interface (CLI) to perform a series of tasks by entering
commands in rapid succession over SSH (recommended), Telnet, or the console port. The CLI is a no-frills interface that supports two command modes, operational and configure, each with a distinct hierarchy of commands and statements. When you become familiar with the nesting structure and syntax of the commands, the CLI provides quick response times and administrative efficiency.
? Use the XML API to streamline your operations and integrate with existing,
internally developed applications and repositories. The XML API is a web service implemented using HTTP/HTTPS requests and responses.
? Use Panorama to perform web-based management, reporting, and log collection
for multiple firewalls. The Panorama web interface resembles the firewall web interface but with additional functions for centralized management.

NEW QUESTION 94
What is a function of application tags?

A. creation of new zones
B. application prioritization
C. automated referenced applications in a policy
D. IP address allocations in DHCP

Answer: C

NEW QUESTION 99
DRAG DROP
Place the following steps in the packet processing order of operations from first to last.



A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 102
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 103
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 105

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.
adding it to the Manual Exceptions list.
B. Add each IP address in the range as a list entry and then exclude the IP address by
C. Select the address range in the List Entries lis
D. A column will open with the IP addresse
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 110
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%

NEW QUESTION 115
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 118
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 120
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 124
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 127
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 131
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 133
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 136
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 137
Which component is a building block in a Security policy rule?

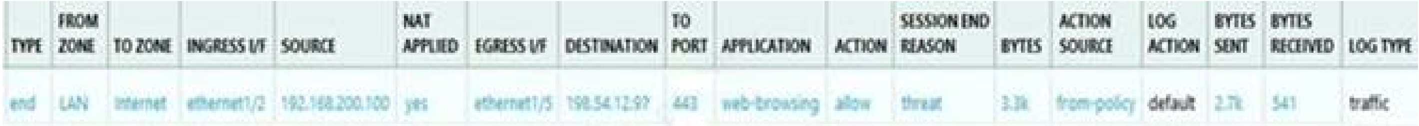
A. decryption profile
B. destination interface
C. timeout (min)
D. application

Answer: D

Explanation:

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

NEW QUESTION 138
Given the screenshot, what are two correct statements about the logged traffic? (Choose two.)



TYPE	FROM ZONE	TO ZONE	INGRESS I/F	SOURCE	NAT APPLIED	EGRESS I/F	DESTINATION	TO PORT	APPLICATION	ACTION	SESSION END REASON	BYTES	ACTION SOURCE	LOG ACTION	BYTES SENT	BYTES RECEIVED	LOG TYPE
end	LAN	internet	ethernet1/2	192.168.200.100	yes	ethernet1/5	198.54.12.97	443	web-browsing	allow	threat	3.3k	from-policy	default	2.7k	541	traffic

A. The web session was unsuccessfully decrypted.
B. The traffic was denied by security profile.
C. The traffic was denied by URL filtering.
D. The web session was decrypted.

Answer: D

NEW QUESTION 139
Which object would an administrator create to block access to all high-risk applications?

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Reference:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClKECA0

NEW QUESTION 143
The NetSec Manager asked to create a new firewall Local Administrator profile with customized privileges named NewAdmin. This new administrator has to authenticate without inserting any username or password to access the WebUI.
What steps should the administrator follow to create the New_Admin Administrator profile?
A.
* 1. Select the "Use only client certificate authentication" check box.
* 2. Set Role to Role Based.
* 3. Issue to the Client a Certificate with Common Name = NewAdmin
B.
* 1. Select the "Use only client certificate authentication" check box.
* 2. Set Role to Dynamic.
* 3. Issue to the Client a Certificate with Certificate Name = NewAdmin
C.
* 1. Set the Authentication profile to Local.
* 2. Select the "Use only client certificate authentication" check box.
* 3. Set Role to Role Based.
D.
* 1. Select the "Use only client certificate authentication" check box.
* 2. Set Role to Dynamic.
* 3. Issue to the Client a Certificate with Common Name = New Admin

A.

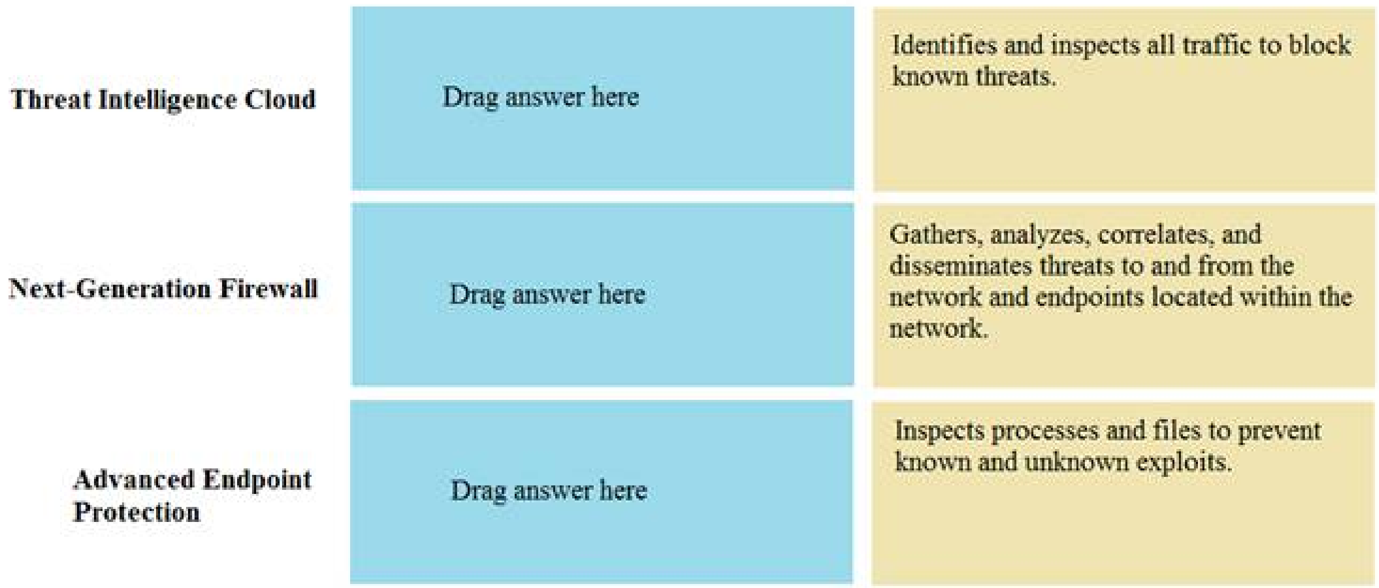
Answer: B

NEW QUESTION 148
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 149
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 152
Which two statements are true for the DNS security service introduced in PAN-OS version 10.0?

A. It functions like PAN-DB and requires activation through the app portal.
B. It removes the 100K limit for DNS entries for the downloaded DNS updates.

C. IT eliminates the need for dynamic DNS updates.
D. IT is automatically enabled and configured.

Answer: AB

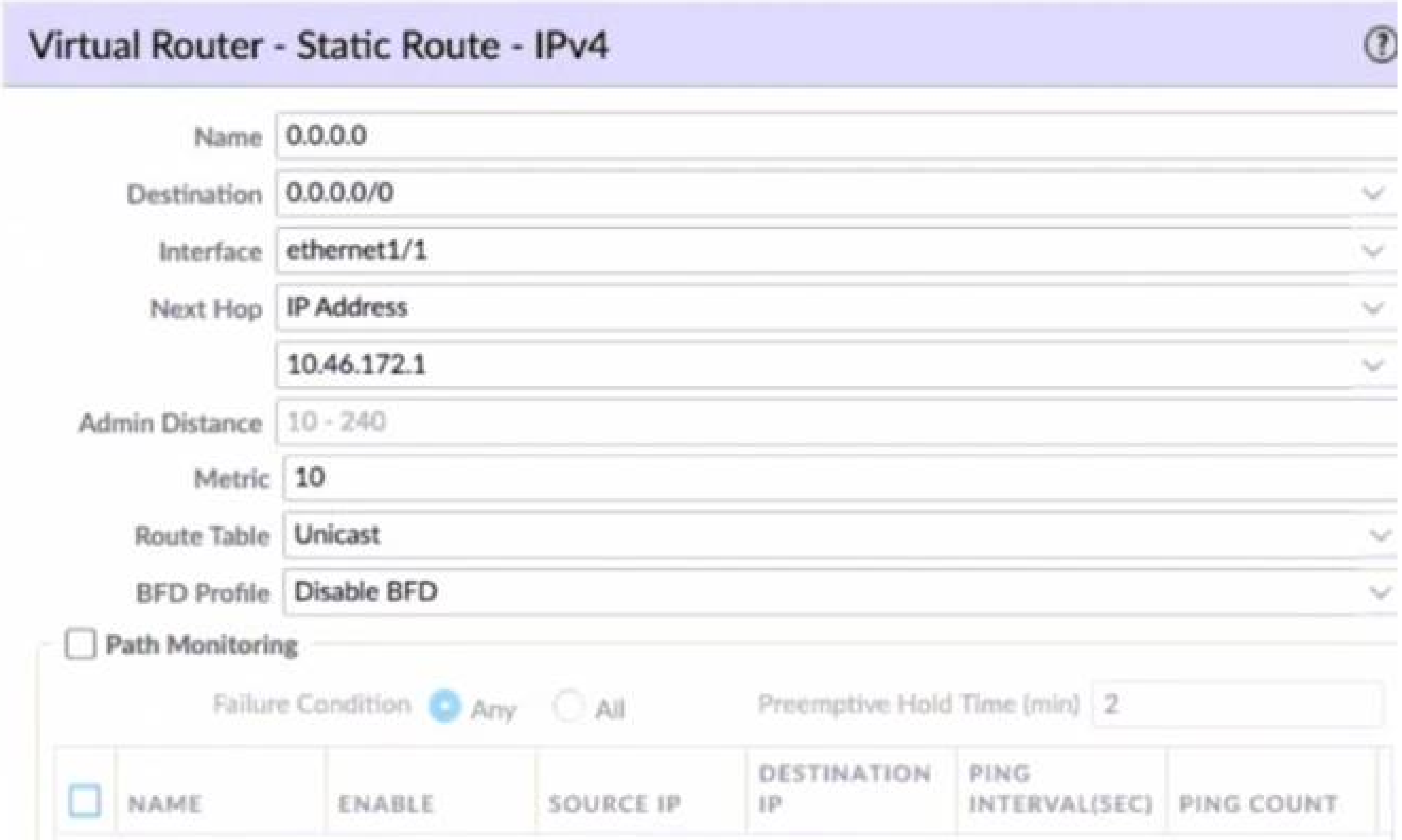
NEW QUESTION 153

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 157
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 159
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 160
Starting with PAN_OS version 9.1 which new type of object is supported for use within the user field of a security policy rule?

A. local username
B. dynamic user group
C. remote username
D. static user group

Answer: B

NEW QUESTION 162
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 164
An administrator is reviewing another administrator s Security policy log settings Which log setting configuration is consistent with best practices tor normal traffic?

A. Log at Session Start and Log at Session End both enabled
B. Log at Session Start disabled Log at Session End enabled
C. Log at Session Start enabled Log at Session End disabled
D. Log at Session Start and Log at Session End both disabled

Answer: B

NEW QUESTION 165
......