Paloalto-Networks

Exam Questions PCNSA

Palo Alto Networks Certified Network Security Administrator

NEW QUESTION 1
What are three ways application characteristics are used? (Choose three.)

A. As an attribute to define an application group
B. As a setting to define a new custom application
C. As an Object to define Security policies
D. As an attribute to define an application filter
E. As a global filter in the Application Command Center (ACC)

Answer: ABD

Explanation:

NEW QUESTION 2
Which Security policy match condition would an administrator use to block traffic from IP addresses on the Palo Alto Networks EDL of Known Malicious IP Addresses list?

A.

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

Answer: B

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

NEW QUESTION 3
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?

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

Answer: C

NEW QUESTION 4
Which security profile will provide the best protection against ICMP floods, based on individual combinations of a packet`s source and destination IP address?

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

Answer: A

NEW QUESTION 5
Which information is included in device state other than the local configuration?

A.
uncommitted changes
B. audit logs to provide information of administrative account changes
C. system logs to provide information of PAN-OS changes
D. device group and template settings pushed from Panorama

Answer: D

Explanation:
Reference:https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/device/device-setup-operations.html

NEW QUESTION 6
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 7
Which type of security policy rule will match traffic that flows between the Outside zone and inside zone, but would not match traffic that flows within the zones?

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

Answer: C

Explanation:
Reference:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/software-and-content- updates/dynamic-contentupdates.html#:~:text=WildFire%20signature%20updates%20are%20made,within% 20a%20minute%20of %20availability

NEW QUESTION 8
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 9
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

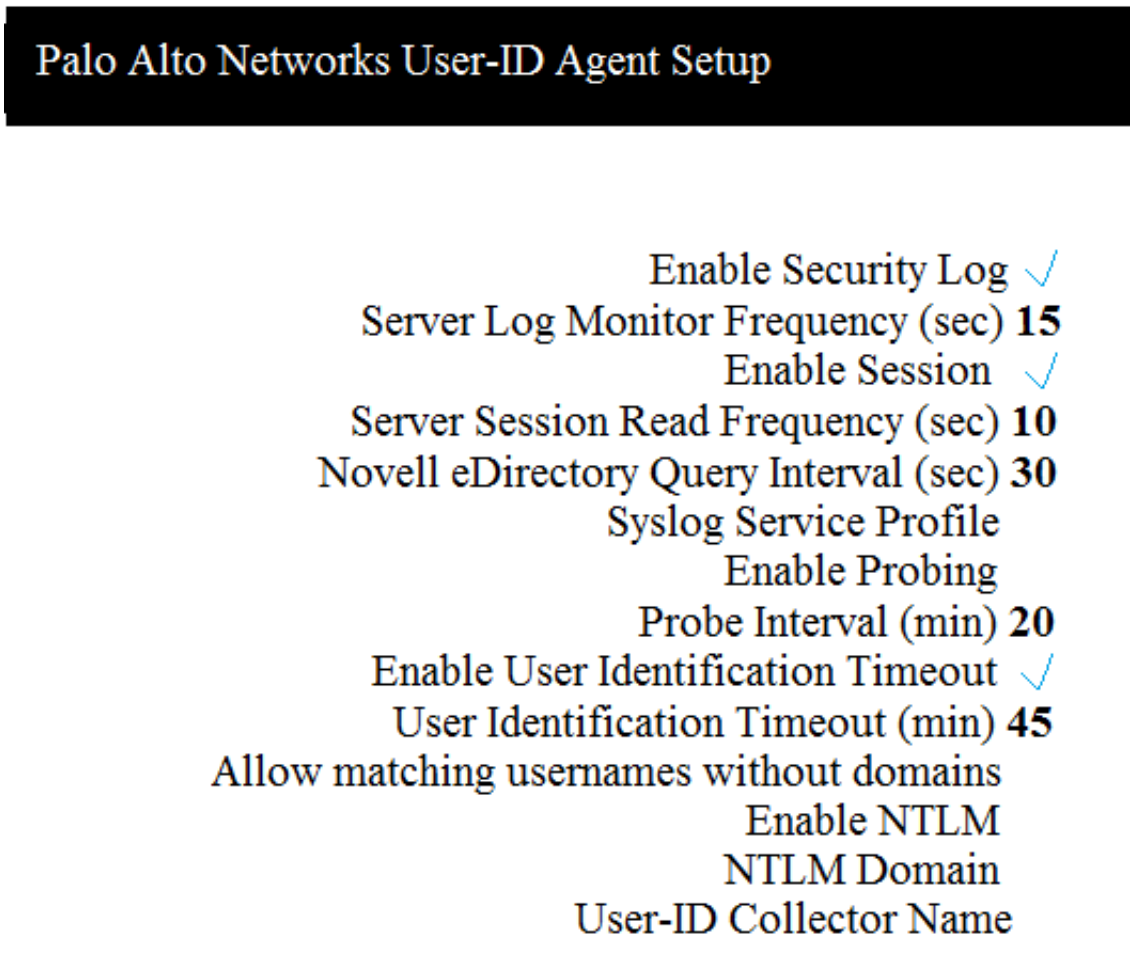
NEW QUESTION 10
What is considered best practice with regards to committing configuration changes?

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

Answer: A

NEW QUESTION 10

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



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

Answer: BC

NEW QUESTION 14
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 15
Which Palo Alto networks security operating platform service protects cloud-based application such as Dropbox and salesforce by monitoring permissions and shared and scanning files for Sensitive information?

A. Prisma SaaS
B. AutoFocus

C. Panorama
D. GlobalProtect

Answer: A

NEW QUESTION 16
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 23
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 26
What is an advantage for using application tags?

A. They are helpful during the creation of new zones
B. They help with the design of IP address allocations in DHCP.
C. They help content updates automate policy updates
D. They help with the creation of interfaces

Answer: C

NEW QUESTION 30
How are Application Fillers or Application Groups used in firewall policy?

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

Answer: B

NEW QUESTION 34
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 39
Which rule type is appropriate for matching traffic both within and between the source and destination zones?

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

Answer: A

NEW QUESTION 40
The PowerBall Lottery has reached an unusually high value this week. Your company has decided to raise morale by allowing employees to access the PowerBall

Lottery website (www.powerball.com) for just this week. However, the company does not want employees to access any other websites also listed in the URL filtering “gambling” category.
Which method allows the employees to access the PowerBall Lottery website but without unblocking access to the “gambling” URL category?

A. Add just the URL www.powerball.com to a Security policy allow rule.
B. Manually remove powerball.com from the gambling URL category.
C. Add *.powerball.com to the URL Filtering allow list.
D. Create a custom URL category, add *.powerball.com to it and allow it in the Security Profile.

Answer: CD

NEW QUESTION 44
What are two valid selections within an Antivirus profile? (Choose two.)

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

Answer: BC

NEW QUESTION 47
A security administrator has configured App-ID updates to be automatically downloaded and installed. The company is currently using an application identified by App-ID as SuperApp_base.
On a content update notice, Palo Alto Networks is adding new app signatures labeled SuperApp_chat and SuperApp_download, which will be deployed in 30 days.
Based on the information, how is the SuperApp traffic affected after the 30 days have passed?

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

Answer: A

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

NEW QUESTION 48
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 52
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 57
Which two features can be used to tag a username so that it is included in a dynamic user group? (Choose two.)

A. GlobalProtect agent
B. XML API
C.

User-ID Windows-based agent
D. log forwarding auto-tagging

Answer: BC

NEW QUESTION 58
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 63
Which solution is a viable option to capture user identification when Active Directory is not in use?

A. Cloud Identity Engine
B. group mapping
C. Directory Sync Service
D. Authentication Portal

Answer: D

NEW QUESTION 68
To use Active Directory to authenticate administrators, which server profile is required in the authentication profile?

A. Mastered
B. Not Mastered

Answer: A

NEW QUESTION 73

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

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

Answer: AD

NEW QUESTION 76
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 81
Which two components are utilized within the Single-Pass Parallel Processing architecture on a Palo Alto Networks Firewall? (Choose two.)

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

Answer: BD

Explanation:

NEW QUESTION 82
Which interface type is used to monitor traffic and cannot be used to perform traffic shaping?

A. Mastered
B. Not Mastered

Answer: A

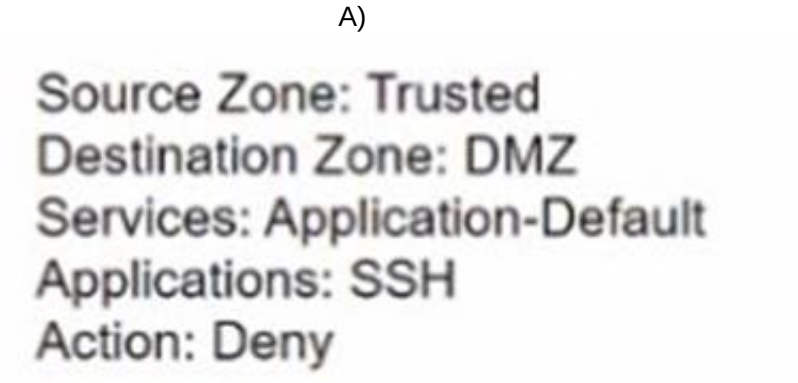
NEW QUESTION 85
What allows a security administrator to preview the Security policy rules that match new application signatures?

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

Answer: B

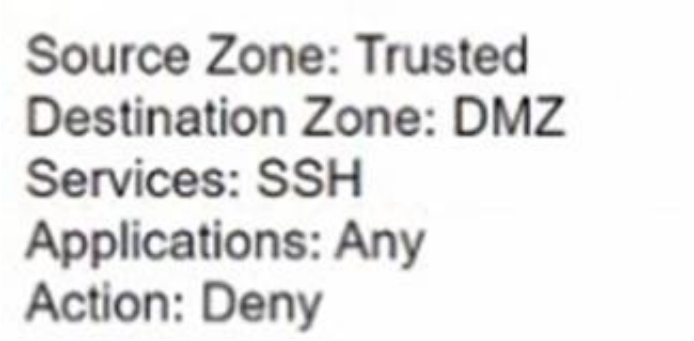
Explanation:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/app-id/manage- new-app-ids-introduced-in-content-releases/review-new-app-id-impact-on-existing-policy- rules

NEW QUESTION 90
If users from the Trusted zone need to allow traffic to an SFTP server in the DMZ zone, how should a Security policy with App-ID be configured?
A)

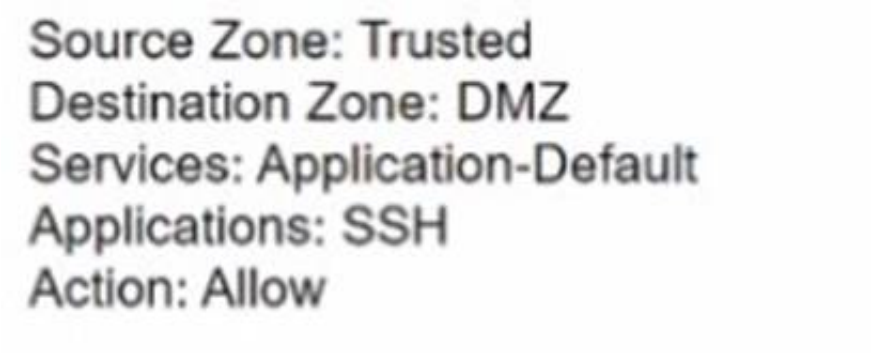


B)

C)



D)



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

Answer: D

NEW QUESTION 95
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 96
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 97
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 99
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 104
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 0ClQSCA0

NEW QUESTION 107
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 112
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 113
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 114
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

SSH from any source-IP-address to any
E. In addition to option c, an additional rule from zone OUTSIDE to USERS for application
destination-IP-address is required to allow the return-traffic from the SSH-servers to reach the server-admin

Answer: B

NEW QUESTION 117
Which URL Filtering Profile action does not generate a log entry when a user attempts to access a URL?

A. override
B. allow
C. block
D. continue

Answer: B

NEW QUESTION 122
Which profile should be used to obtain a verdict regarding analyzed files?

A. WildFire analysis
B. Vulnerability profile
Content-ID
C
D: Advanced threat prevention

Answer: A

Explanation:
? A profile is a set of rules or settings that defines how the firewall performs a specific function, such as detecting and preventing threats, filtering URLs, or decrypting traffic1.
? There are different types of profiles that can be applied to different types of traffic or scenarios, such as Antivirus, Anti-Spyware, Vulnerability Protection, URL Filtering, File Blocking, Data Filtering, Decryption, or WildFire Analysis1.
? The WildFire Analysis profile is a profile that enables the firewall to submit unknown files or email links to the cloud-based WildFire service for analysis and verdict determination2. WildFire is the industry's most advanced analysis and prevention engine for highly evasive zero-day exploits and malware3. WildFire uses a variety of malware detection techniques, such as static analysis, dynamic analysis, machine learning, and intelligent run-time memory analysis, to identify and protect against unknown threats34.
? The Vulnerability Protection profile is a profile that protects the network from exploits that target known software vulnerabilities. It allows the administrator to configure the actions and log settings for each vulnerability severity level, such as critical, high, medium, low, or informational5.
? Content-ID is not a profile, but a feature of the firewall that performs multiple functions to identify and control applications, users, content, and threats on the network. Content-ID consists of four components: App-ID, User-ID, Content Inspection, and Threat Prevention.
? Advanced Threat Prevention is not a profile, but a term that refers to the comprehensive approach of Palo Alto Networks to prevent sophisticated and unknown threats. Advanced Threat Prevention includes WildFire, but also other products and services, such as DNS Security, Cortex XDR, Cortex XSOAR, and AutoFocus.
Therefore, the profile that should be used to obtain a verdict regarding analyzed files is the WildFire Analysis profile.
References:
1: Security Profiles - Palo Alto Networks 2: WildFire Analysis Profile - Palo Alto
Networks 3: WildFire - Palo Alto Networks 4: Advanced Wildfire as an ICAP Alternative | Palo Alto Networks 5: Vulnerability Protection Profile - Palo Alto Networks
: [Content-ID - Palo Alto Networks] : [Advanced Threat Prevention - Palo Alto Networks]

NEW QUESTION 123
An administrator has configured a Security policy where the matching condition includes a single application and the action is deny
If the application s default deny action is reset-both what action does the firewall take*?

A. It sends a TCP reset to the client-side and server-side devices
B. It silently drops the traffic and sends an ICMP unreachable code
C. It silently drops the traffic
D. It sends a TCP reset to the server-side device

Answer: A

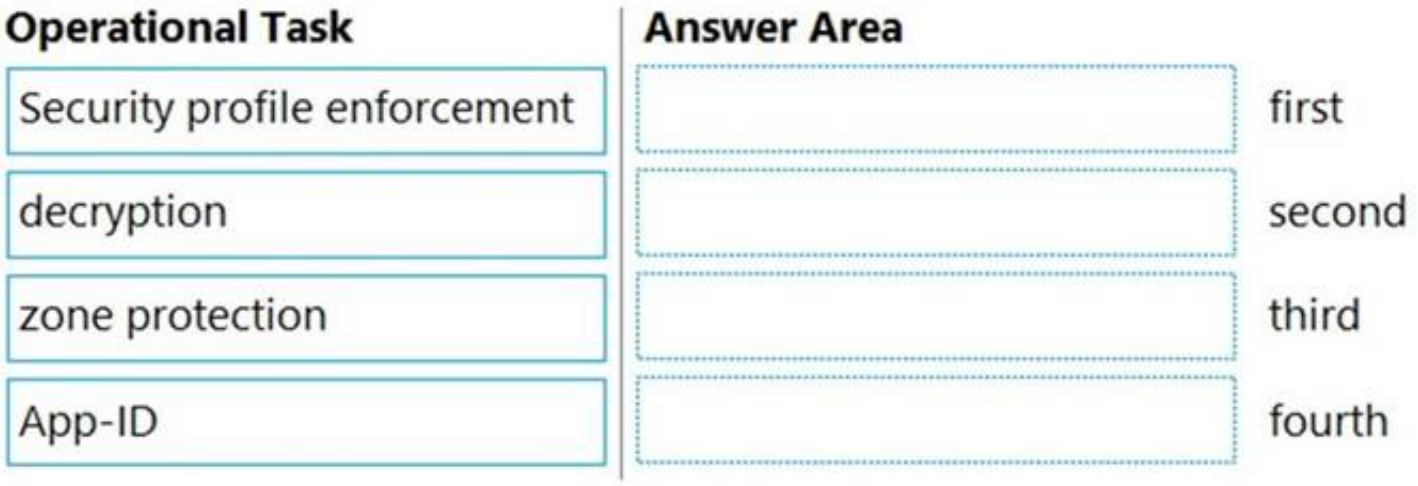
NEW QUESTION 124
If using group mapping with Active Directory Universal Groups, what must you do when configuring the User-ID?

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 128
DRAG DROP
Place the steps in the correct packet-processing order of operations.

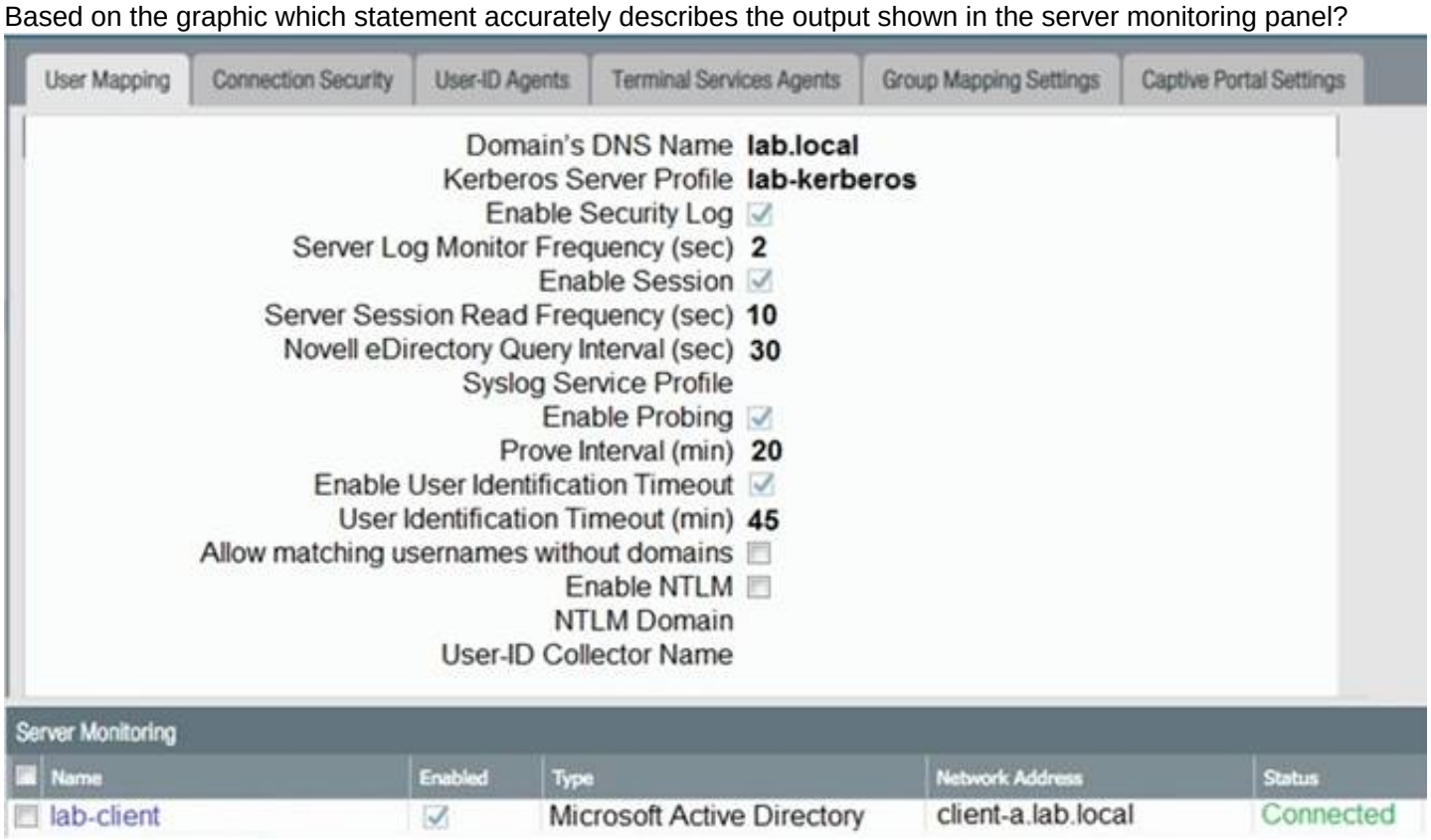


A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 130
Based on the graphic which statement accurately describes the output shown in the server monitoring panel?



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

Answer: A

NEW QUESTION 132
Based on the screenshot what is the purpose of the included groups?

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 133
Selecting the option to revert firewall changes will replace what settings?

A. Mastered
B. Not Mastered

Answer: A

NEW QUESTION 134
Based on the security policy rules shown, ssh will be allowed on which port?

			Source		Destination						
	Name	Type	Zone	Address	Zone	Address	Application	Service	URL Category	Action	Profile
1	Deny Google	Universal	Inside	Any	Outside	Any	Google-docs-base	Application-d	Any	Deny	None
2	Allowed-security serv...	Universal	Inside	Any	Outside	Any	Snmpv3 Ssh ssl	Application-d	Any	Allow	None
3	Intrazone-default	Intrazone	Any	Any	(intrazone)	Any	Any	Any	Any	Allow	None
4	Interzone-default	Interzone	Any	Any	Any	Any	Any	Any	Any	Deny	None

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

Answer: C

Explanation:

NEW QUESTION 137
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 142
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 147
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 151
Which User Credential Detection method should be applied within a URL Filtering Security profile to check for the submission of a valid corporate username and the associated password?

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

Answer: C

NEW QUESTION 154
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

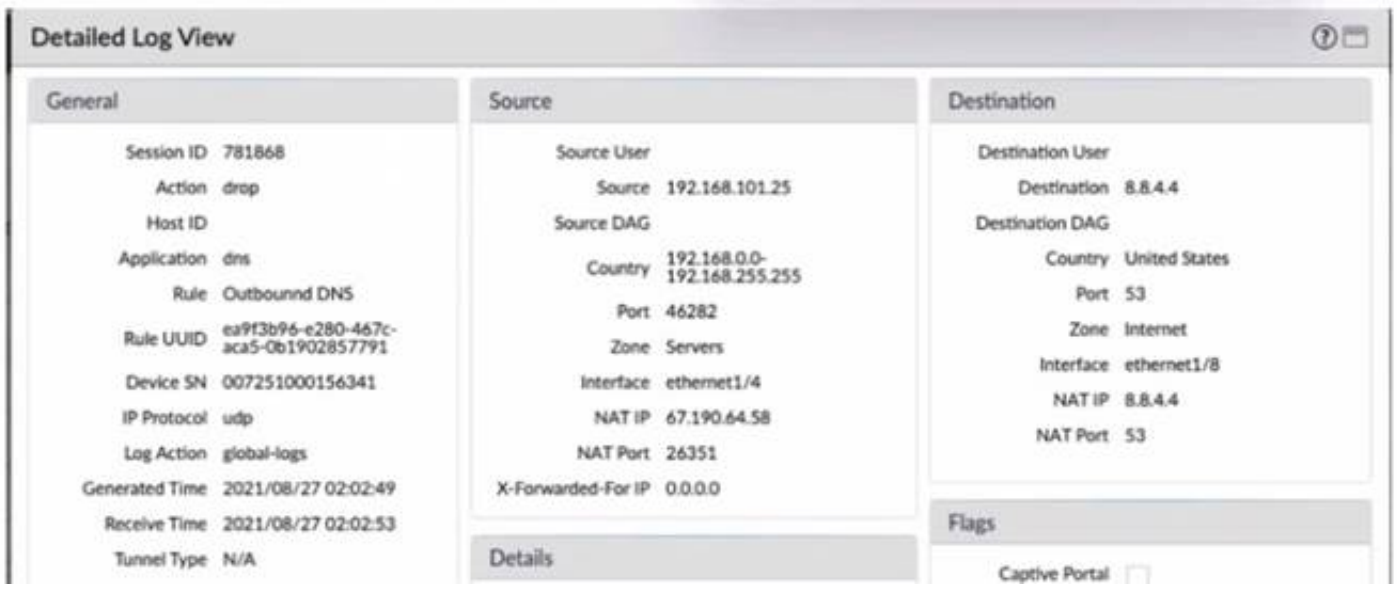
Explanation:

NEW QUESTION 155
Which interface type can use virtual routers and routing protocols?

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

Answer: B

NEW QUESTION 156
Given the detailed log information above, what was the result of the firewall traffic inspection?



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

Answer: B

NEW QUESTION 157
Which URL Filtering profile action would you set to allow users the option to access a site only if they provide a URL admin password?

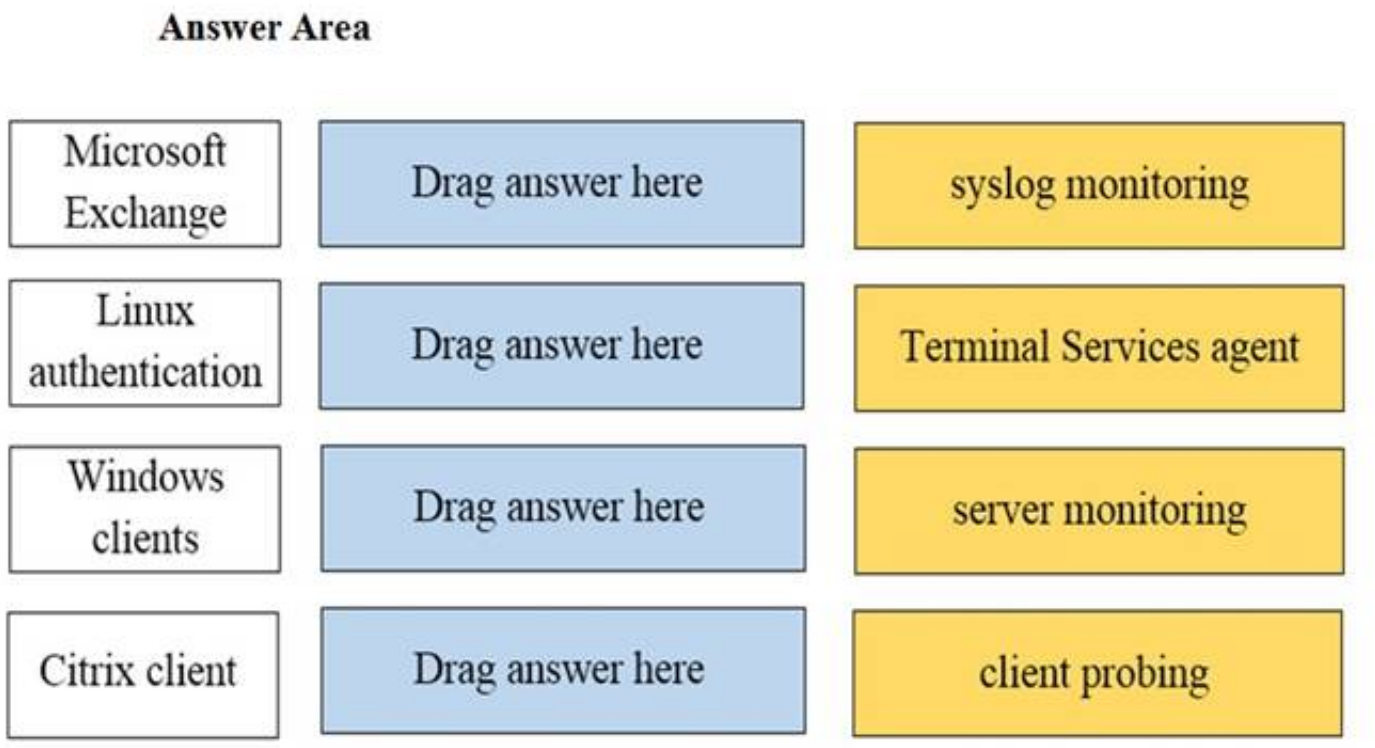
A. override
B. authorization
C. authentication
D. continue

Answer: B

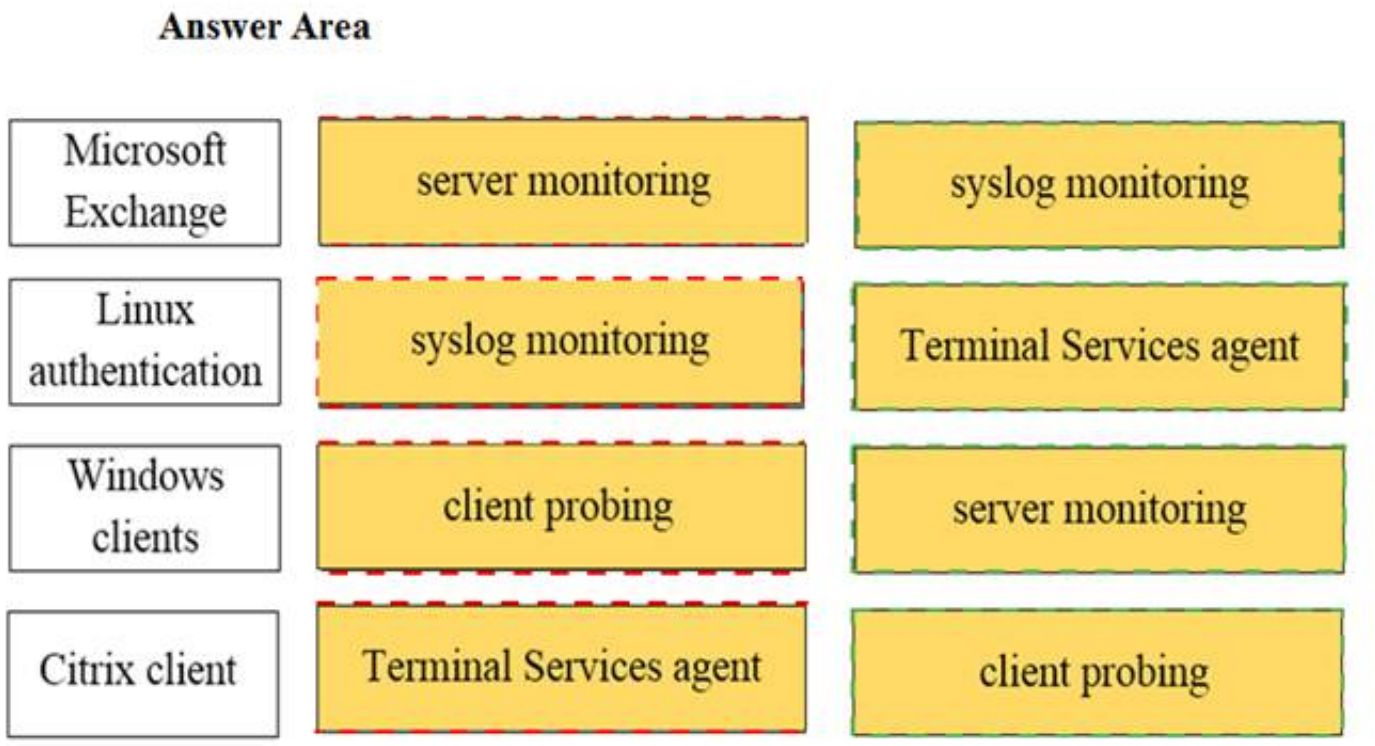
Explanation:

Reference:
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/url-filtering/url-filtering- concepts/url- filteringprofile-actions.html

NEW QUESTION 158
DRAG DROP
Match the network device with the correct User-ID technology.



Answer:



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 159
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 161
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 166
An administrator needs to allow users to use only certain email applications.
How should the administrator configure the firewall to restrict users to specific email applications?

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

Answer: B

NEW QUESTION 170
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 174
What is the maximum volume of concurrent administrative account sessions?

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

Answer: C

NEW QUESTION 177
Which Security profile must be added to Security policies to enable DNS Signatures to be checked?

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

Answer: D

NEW QUESTION 180
Which action results in the firewall blocking network traffic without notifying the sender?

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

Answer: C

NEW QUESTION 185
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 190
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

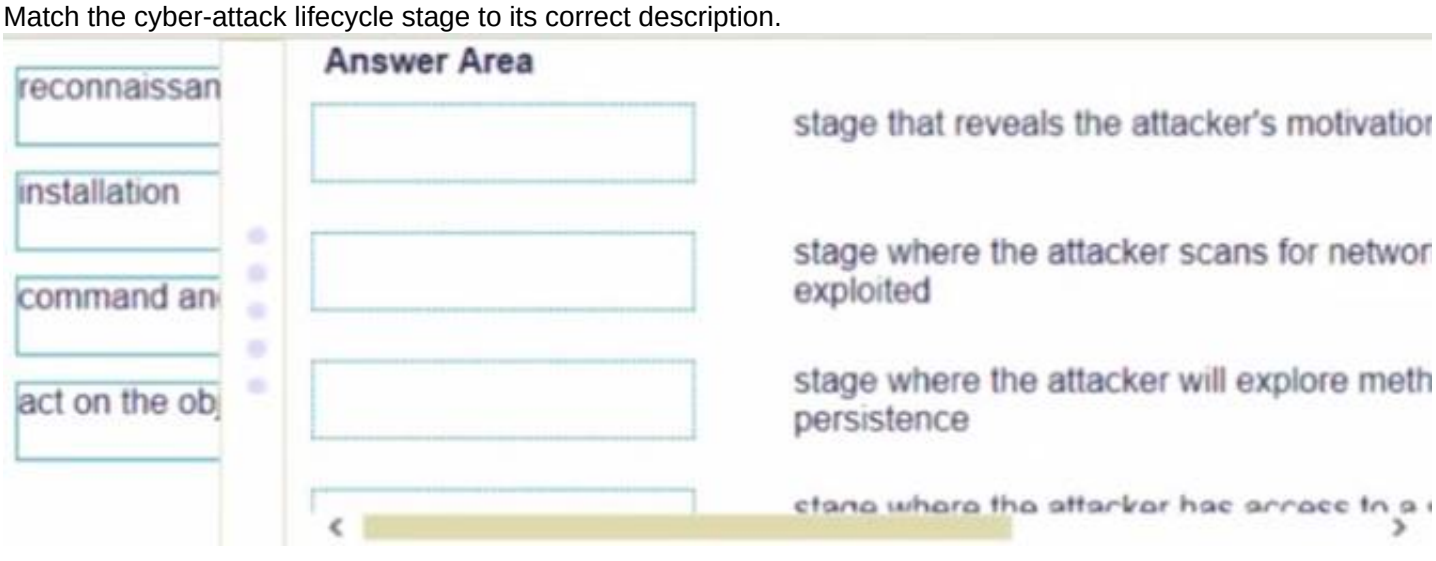
Explanation:

NEW QUESTION 192
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

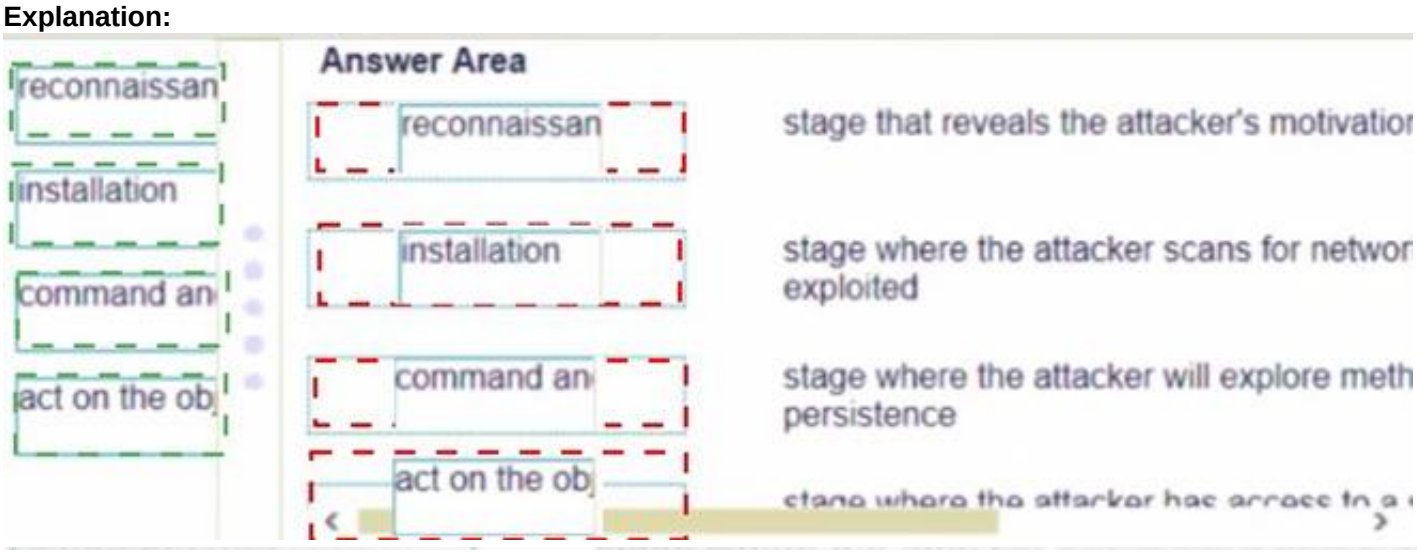
NEW QUESTION 194
DRAG DROP
Match the cyber-attack lifecycle stage to its correct description.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



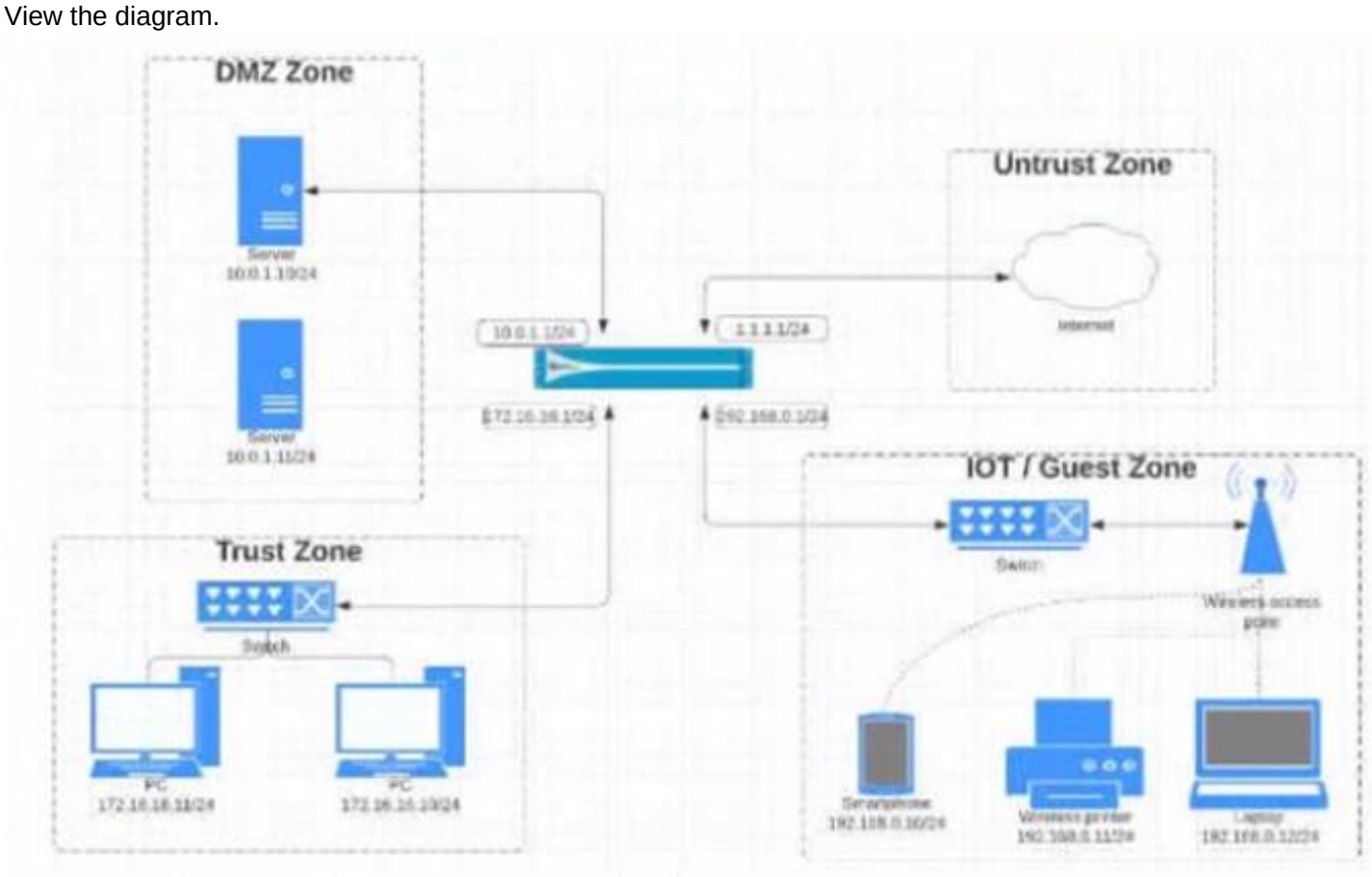
NEW QUESTION 195
An administrator is troubleshooting traffic that should match the interzone-default rule. However, the administrator doesn't see this traffic in the traffic logs on the

firewall. The interzone-default was never changed from its default configuration.
Why doesn't the administrator see the traffic?

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

Answer: D

NEW QUESTION 198
View the diagram.



What is the most restrictive yet fully functional rule to allow general Internet and SSH traffic into both the DMZ and Untrust/Internet zones from each of the IOT/Guest and Trust Zones?
A)

	Source			Destination						
	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	URL CATEGORY	ACTION
Guest	172.16.16.0/24 192.168.0.0/24	any	any	DMZ Untrust	1.1.1.0/24 10.0.1.5/24	any	ssh ssl web-browsing	application-default	any	Allow

B)

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

C)

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

D)

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

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

Answer: C

NEW QUESTION 199
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 203
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 207
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 210
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 215
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 217
What can be achieved by disabling the Share Unused Address and Service Objects with Devices setting on Panorama?

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

Answer: D

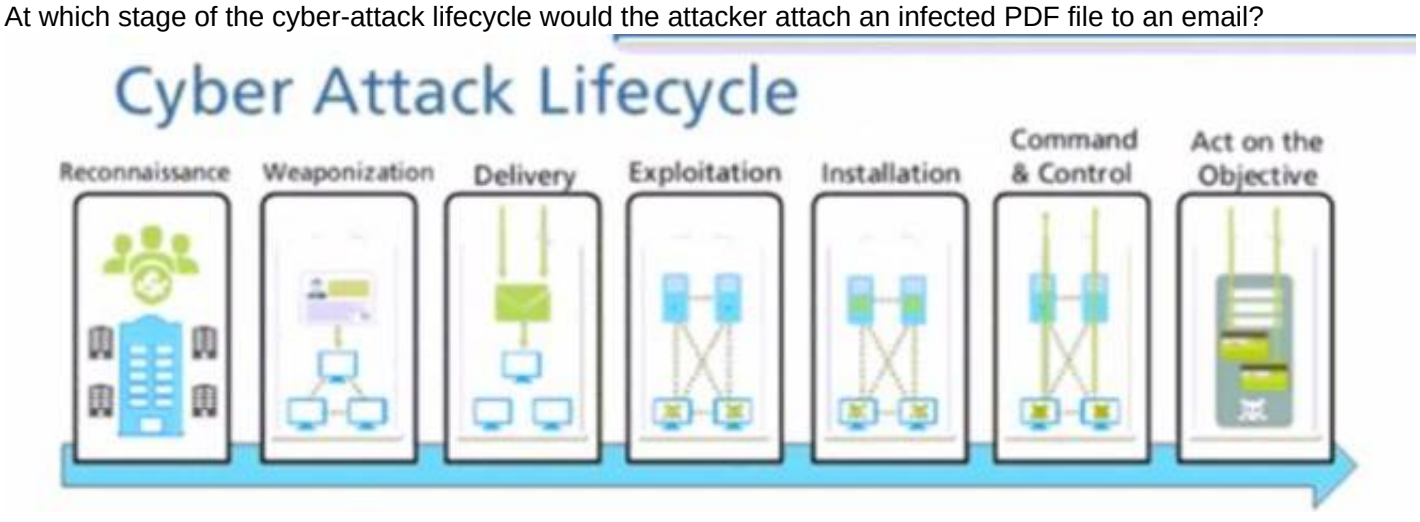
NEW QUESTION 219
In the example security policy shown, which two websites fcked? (Choose two.)

	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 222
At which stage of the cyber-attack lifecycle would the attacker attach an infected PDF file to an email?



delivery
A
B. command and control
C. explotation
D. reinsurance
E. installation

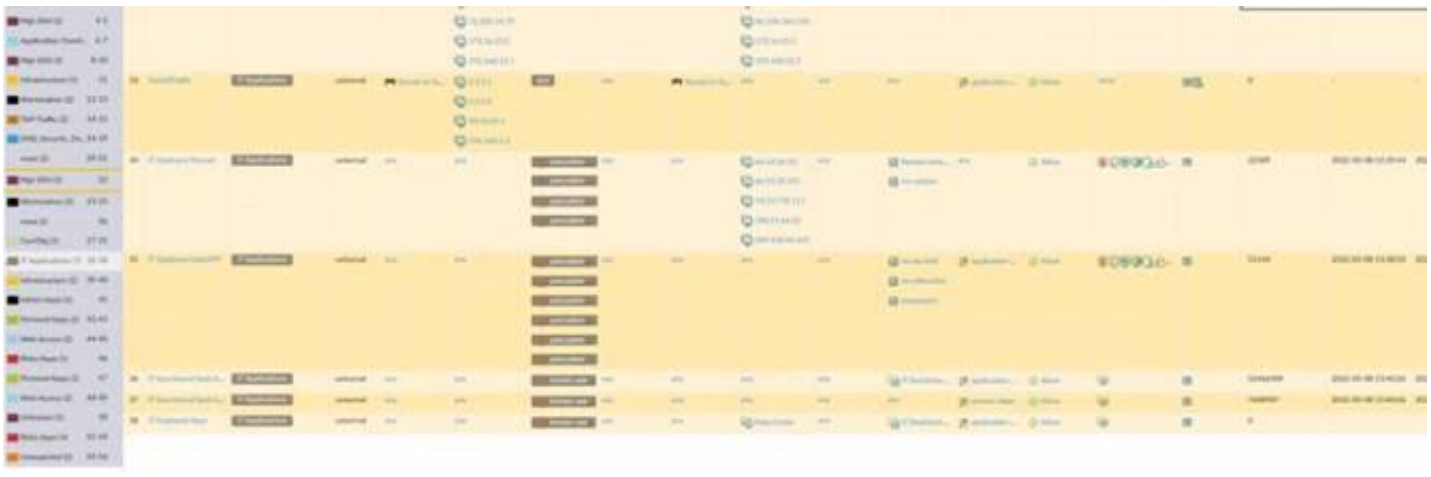
Answer: A

NEW QUESTION 226
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 227
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 230
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 234
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 237
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 241
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

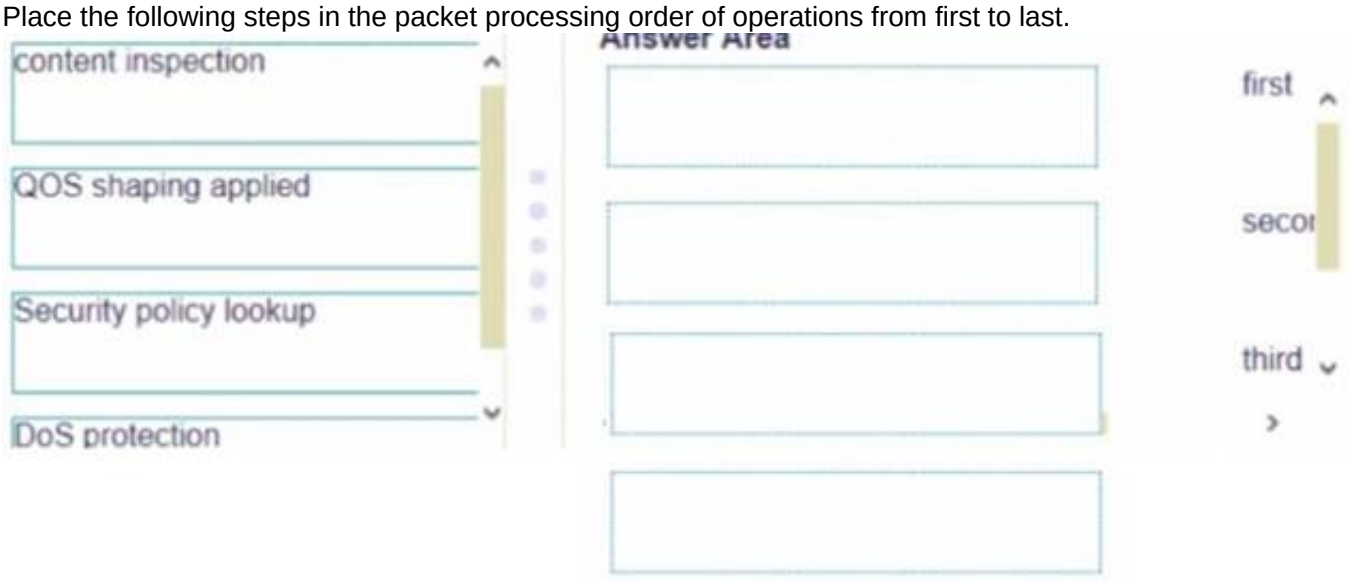
Answer: D

NEW QUESTION 244
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 246
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 251
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 252
According to the best practices for mission critical devices, what is the recommended interval for antivirus updates?

A. by minute
B. hourly
C. daily
D. weekly

Answer: C

Explanation:
Reference:https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/threat-prevention/best-practices-for-content-and-threat-content-updates/best-practices-mission- critical.html

NEW QUESTION 257

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 260
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 261
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

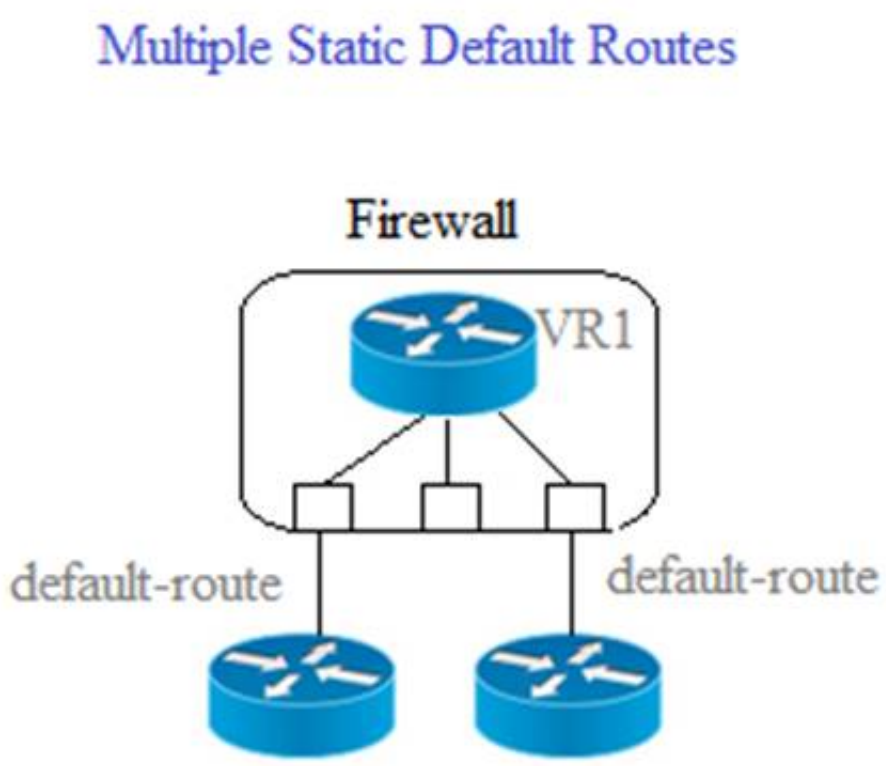
Answer: C

NEW QUESTION 262
Which statement is true regarding a Best Practice Assessment?

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

Answer: C

NEW QUESTION 267
Given the scenario, which two statements are correct regarding multiple static default routes? (Choose two.)



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 272

An administrator is investigating a log entry for a session that is allowed and has the end reason of aged-out. Which two fields could help in determining if this is normal? (Choose two.)

A. Packets sent/received
B. IP Protocol
C. Action
D. Decrypted

Answer: BD

NEW QUESTION 277
Palo Alto Networks firewall architecture accelerates content map minimizing latency using which two components'? (Choose two)

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

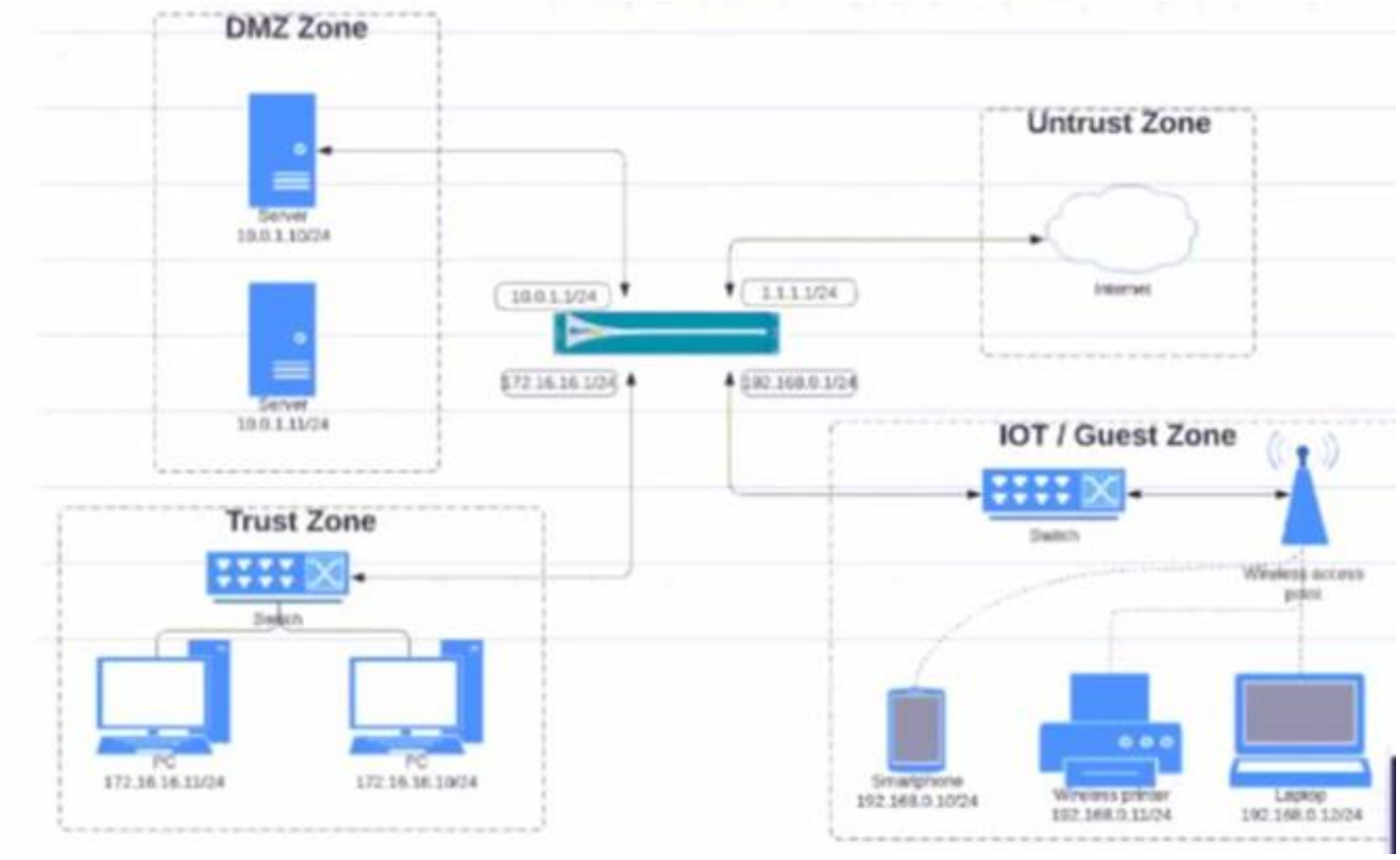
Answer: B

NEW QUESTION 282
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 287
Given the network diagram, traffic should be permitted for both Trusted and Guest users to access general Internet and DMZ servers using SSH. web-browsing and SSL applications



Which policy achieves the desired results?
A)

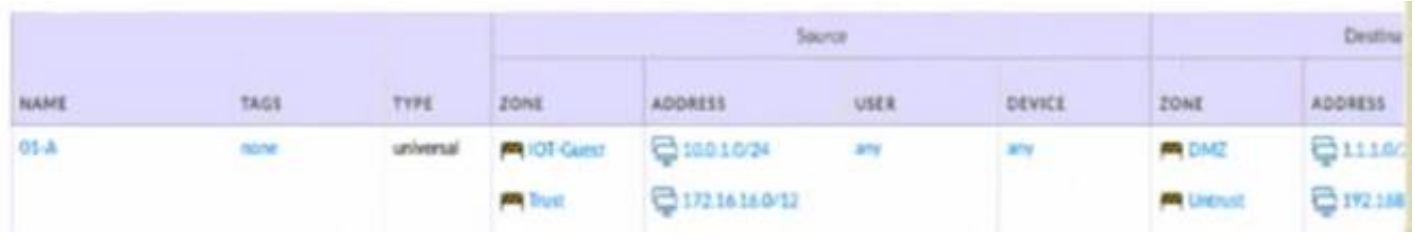
NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS
04-A	none	universal	IOT-Guest	172.16.16.0/24	any	any	DMZ	any
			Trust	192.168.0.0/24			Untrust	

B)

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

C)

D)



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

Answer: C

NEW QUESTION 288
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 291
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 polic
F. Set the policy action to Deny.

Answer: CD

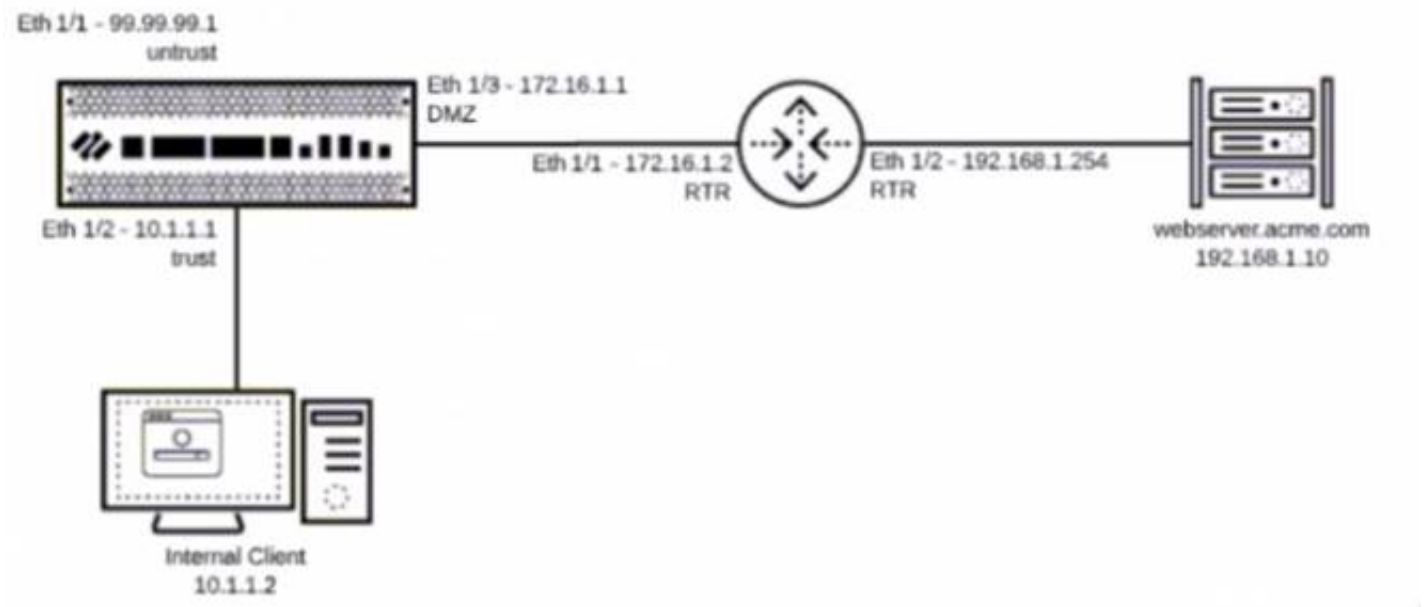
NEW QUESTION 294
Which two features can be used to tag a user name so that it is included in a dynamic user group? (Choose two)

A. XML API
B. log forwarding auto-tagging
C. GlobalProtect agent
D. User-ID Windows-based agent

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 299
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 301
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 305
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

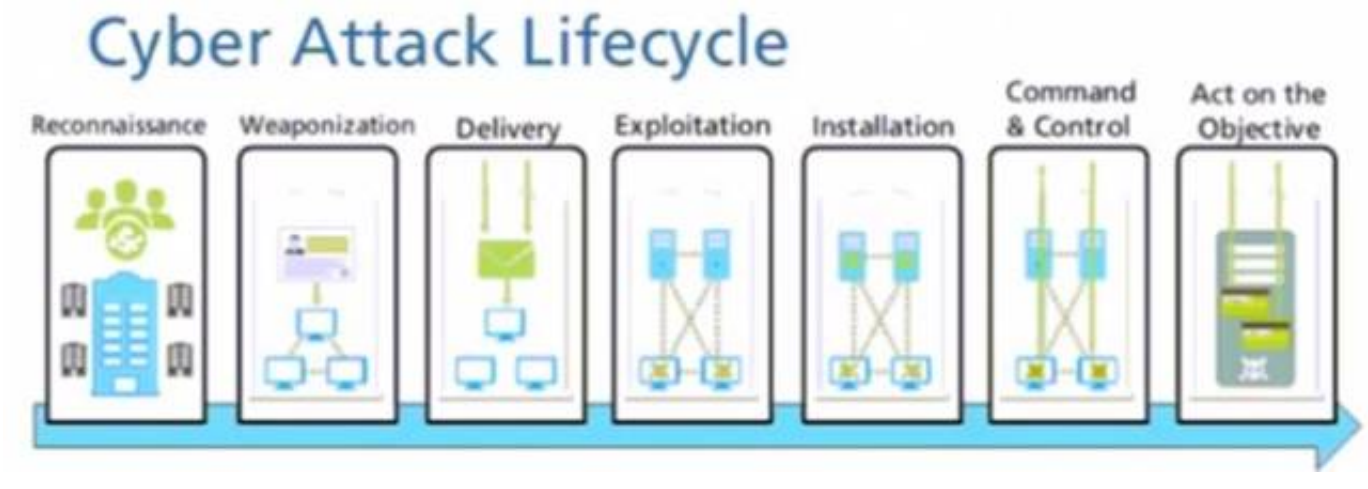
Answer: A

NEW QUESTION 309
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 310
Given the cyber-attack lifecycle diagram identify the stage in which the attacker can run malicious code against a vulnerability in a targeted machine.



Exploitation

A
B. Installation
C. Reconnaissance
D. Act on the Objective

Answer: A

NEW QUESTION 312
Which type firewall configuration contains in-progress configuration changes?

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

Answer: C

NEW QUESTION 315
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 319
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 321
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?

Data Filtering Profile applied to outbound Security policy rules

A
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 322
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 323
An administrator is configuring a NAT rule
At a minimum, which three forms of information are required? (Choose three.)

A. name
B. source zone
C. destination interface
D. destination address
E. destination zone

Answer: BDE

NEW QUESTION 328
Which two firewall components enable you to configure SYN flood protection thresholds? (Choose two.)

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

Answer: BC

Explanation:

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

NEW QUESTION 331
Which firewall feature do you need to configure to query Palo Alto Networks service updates over a data-plane interface instead of the management interface?

A. Data redistribution
B. Dynamic updates
C. SNMP setup
D. Service route

Answer: D

NEW QUESTION 332
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 334
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 339
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 340
An administrator wants to prevent users from submitting corporate credentials in a phishing attack.
Which Security profile should be applied?

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

Answer: B

NEW QUESTION 343
The compliance officer requests that all evasive applications need to be blocked on all perimeter firewalls out to the internet The firewall is configured with two zones;
* 1. trust for internal networks
* 2. untrust to the internet
Based on the capabilities of the Palo Alto Networks NGFW, what are two ways to configure a security policy using App-ID to comply with this request? (Choose two)

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

Answer: AD

NEW QUESTION 345
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 346
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 350
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 353
Which prevention technique will prevent attacks based on packet count?

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

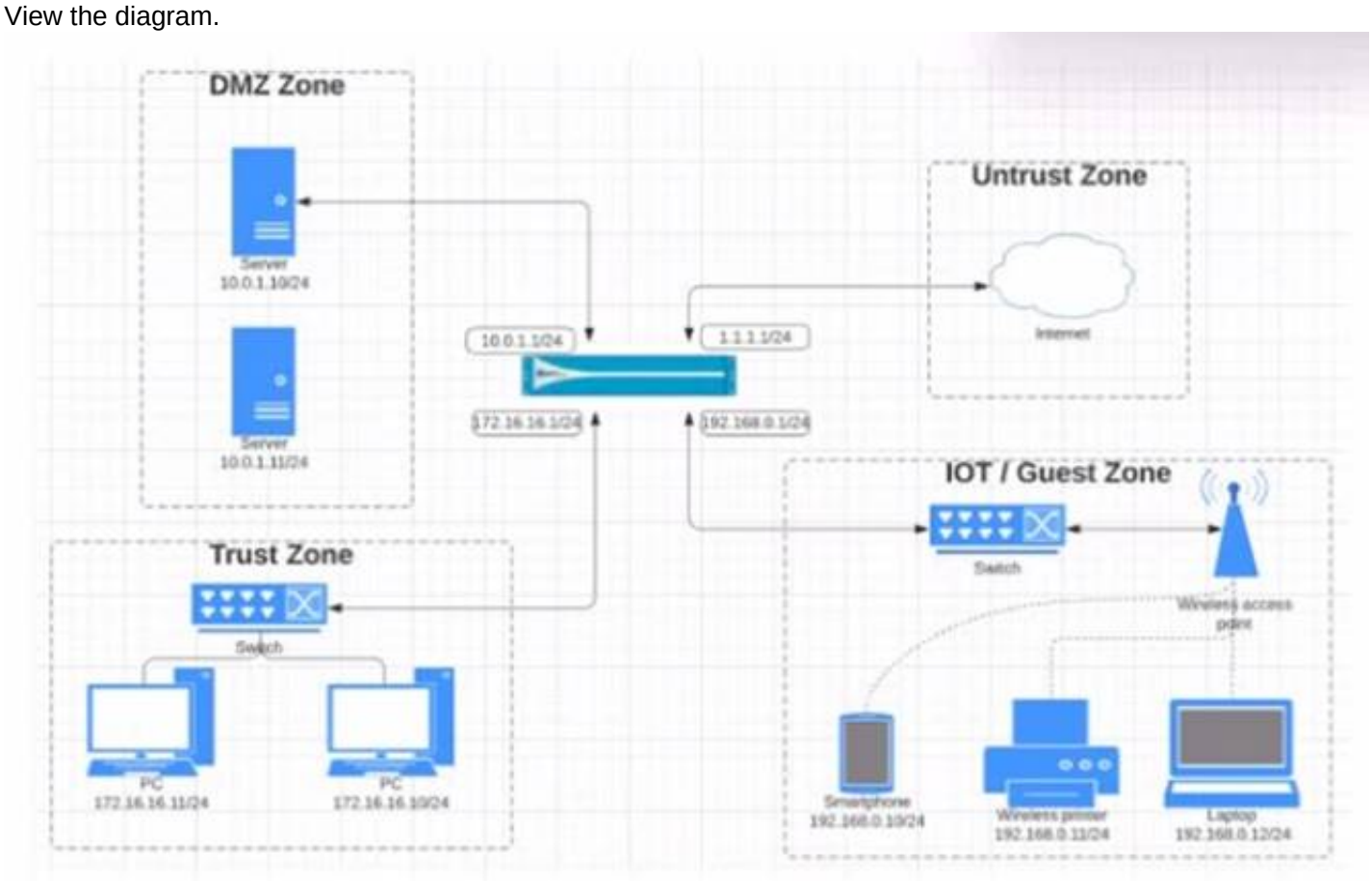
Answer: A

NEW QUESTION 356
Which two matching criteria are used when creating a Security policy involving NAT? (Choose two.)

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

Answer: BD

NEW QUESTION 359
View the diagram.



What is the most restrictive, yet fully functional rule, to allow general Internet and SSH traffic into both the DMZ and Untrust/Internet zones from each of the IOT/Guest and Trust Zones?

A)

B)

C)

D)

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

Answer: C

NEW QUESTION 363
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 364
An administrator would like to determine the default deny action for the application dns- over-https
Which action would yield the information?

A. View the application details in beacon paloaltonetworks.com
B. Check the action for the Security policy matching that traffic
C. Check the action for the decoder in the antivirus profile
D. View the application details in Objects > Applications

Answer: D

Explanation:

NEW QUESTION 365
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 367
Which URL profiling action does not generate a log entry when a user attempts to access that URL?

A. Override
B. Allow
C. Block
D. Continue

Answer: B

NEW QUESTION 368
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 371
An administrator would like to see the traffic that matches the interzone-default rule in the traffic logs.
What is the correct process to enable this logging1?

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

Answer: D

NEW QUESTION 375
.....

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