Exam Questions PCNSA

Palo Alto Networks Certified Network Security Administrator

https://www.2passeasy.com/dumps/PCNSA/

NEW QUESTION 1
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 2
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 3
Which five Zero Trust concepts does a Palo Alto Networks firewall apply to achieve an integrated approach to prevent threats? (Choose five.)

A. User identification
B. Filtration protection
C. Vulnerability protection
D. Antivirus
E. Application identification
F. Anti-spyware

Answer: ACDEF

NEW QUESTION 4
Which type security policy rule would match traffic flowing between the inside zone and outside zone within the inside zone and within the outside zone?

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

Answer: B

NEW QUESTION 5
Which type of address object is www.paloaltonetworks.com?

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

Answer: D

NEW QUESTION 6
In which profile should you configure the DNS Security feature?

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

Answer: B

NEW QUESTION 7
Which administrator type utilizes predefined roles for a local administrator account?

A. Superuser
B. Role-based
C. Dynamic
D. Device administrator

Answer: C

NEW QUESTION 8
Which administrator receives a global notification for a new malware that infects hosts. The infection will result in the infected host attempting to contact and command-and-control (C2) server.
Which security profile components will detect and prevent this threat after the firewall`s signature database has been updated?

A. antivirus profile applied to outbound security policies
B. data filtering profile applied to inbound security policies
C. data filtering profile applied to outbound security policies
D. vulnerability profile applied to inbound security policies

Answer: C

NEW QUESTION 9
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 10
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 10
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 14
What are three valid information sources that can be used when tagging users to dynamic user groups? (Choose three.)

A. Blometric scanning results from iOS devices
B. Firewall logs
C. Custom API scripts
D. Security Information and Event Management Systems (SIEMS), such as Splun
E. DNS Security service

Answer: BCE

NEW QUESTION 17
Which dynamic update type includes updated anti-spyware signatures?

A. Applications and Threats
B. GlobalProtect Data File
C. Antivirus
D. PAN-DB

Answer: A

NEW QUESTION 22
All users from the internal zone must be allowed only HTTP access to a server in the DMZ zone.
Complete the empty field in the Security policy using an application object to permit only this type of access. Source Zone: Internal Destination Zone: DMZ Zone Application:
Service: application-default - Action: allow

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

Answer: B

NEW QUESTION 26
Which update option is not available to administrators?

A. New Spyware Notifications
B. New URLs
C. New Application Signatures
D. New Malicious Domains
E. New Antivirus Signatures

Answer: B

NEW QUESTION 31
A network administrator is required to use a dynamic routing protocol for network connectivity.
Which three dynamic routing protocols are supported by the NGFW Virtual Router for this purpose? (Choose three.)

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

Answer: ABE

NEW QUESTION 34
When is the content inspection performed in the packet flow process?

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

Answer: A

NEW QUESTION 39
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-f

NEW QUESTION 43
Which two Palo Alto Networks security management tools provide a consolidated creation of policies, centralized management and centralized threat intelligence. (Choose two.)

A. GlobalProtect
B. Panorama
C. Aperture
D. AutoFocus

Answer: BD

NEW QUESTION 45
The Palo Alto Networks NGFW was configured with a single virtual router named VR-1 What changes are required on VR-1 to route traffic between two interfaces on the NGFW?

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

Answer: D

NEW QUESTION 46
Selecting the option to revert firewall changes will replace what settings?

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

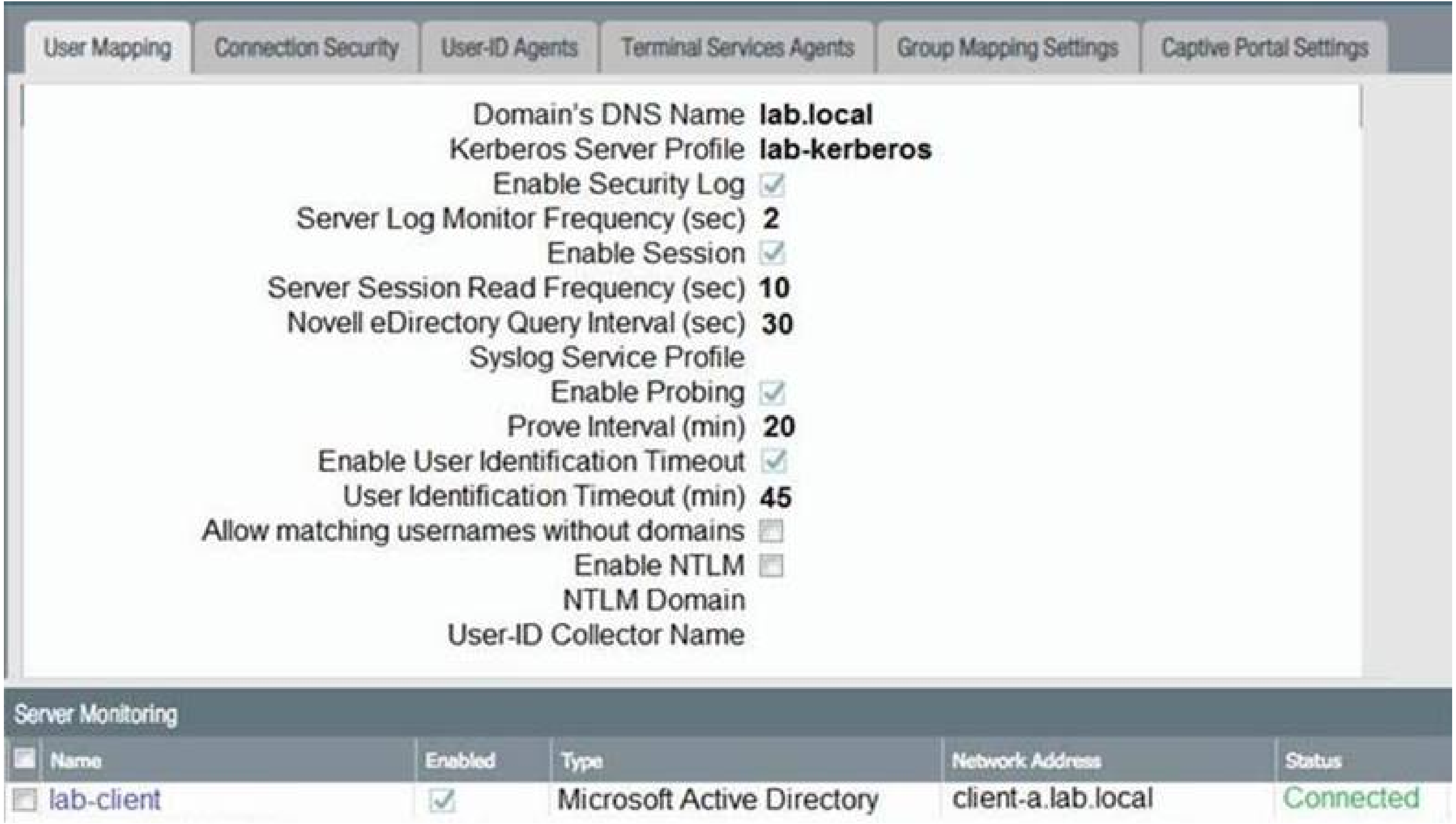
Answer: A

NEW QUESTION 51
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 55
Based on the graphic which statement accurately describes the output shown in the server monitoring panel?



Domain's DNS Name lab.local
Kerberos Server Profile lab-kerberos
Enable Security Log ☑
Server Log Monitor Frequency (sec) 2
Enable Session ☑
Server Session Read Frequency (sec) 10
Novell eDirectory Query Interval (sec) 30
Syslog Service Profile
Enable Probing ☑
Prove Interval (min) 20
Enable User Identification Timeout ☑
User Identification Timeout (min) 45
Allow matching usernames without domains □
Enable NTLM □
NTLM Domain
User-ID Collector Name

Server Monitoring

□ Name	Enabled	Type	Network Address	Status
□ lab-client	☑	Microsoft Active Directory	client-a.lab.local	Connected

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

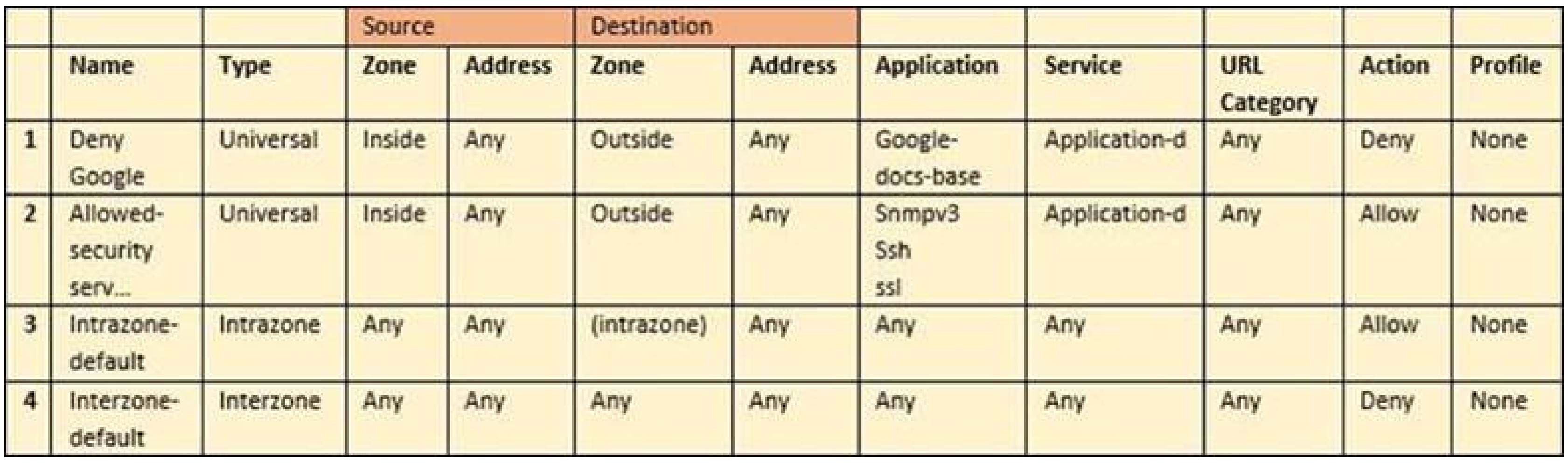
Answer: A

NEW QUESTION 56
What action will inform end users when their access to Internet content is being restricted?

A. Create a custom 'URL Category' object with notifications enabled.
B. Publish monitoring data for Security policy deny logs.
C. Ensure that the 'site access" setting for all URL sites is set to 'alert'.
D. Enable 'Response Pages' on the interface providing Internet access.

Answer: D

NEW QUESTION 58
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. any port
B. same port as ssl and snmpv3
C. the default port
D. only ephemeral ports

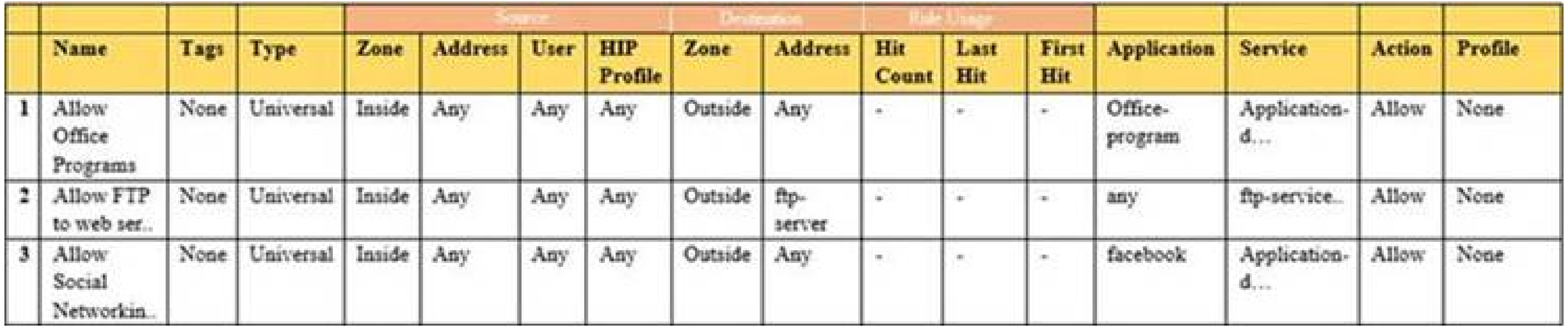
Answer: C

NEW QUESTION 62
Which interface type is used to monitor traffic and cannot be used to perform traffic shaping?

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

Answer: B

NEW QUESTION 67
Given the image, which two options are true about the Security policy rules. (Choose two.)



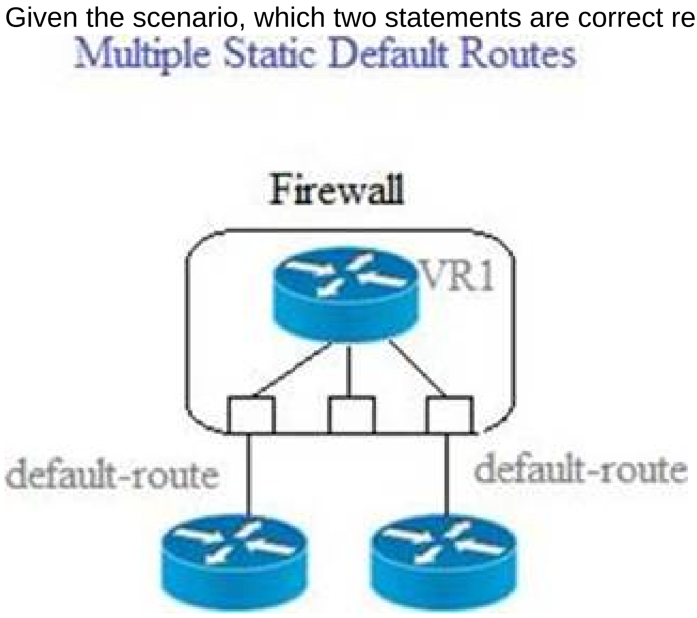
				Source				Destination		Rule Usage						
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Hit Count	Last Hit	First Hit	Application	Service	Action	Profile
1	Allow Office Programs	None	Universal	Inside	Any	Any	Any	Outside	Any	-	-	-	Office-program	Application-d...	Allow	None
2	Allow FTP to web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

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

Answer: AD

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

NEW QUESTION 68
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 70
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 71
Which attribute can a dynamic address group use as a filtering condition to determine its membership?

A. tag
B. wildcard mask
C. IP address
D. subnet mask

Answer: A

Explanation:
Dynamic Address Groups: A dynamic address group populates its members dynamically using looks ups for tags and tag-based filters. Dynamic address groups are very useful if you have an extensive virtual infrastructure where changes in virtual machine location/IP address are frequent. For example, you have a sophisticated failover setup or provision new virtual machines frequently and would like to apply policy to traffic from or to the new machine without modifying the configuration/rules on the firewall.
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface-help/objects/objects-address-groups

NEW QUESTION 74
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

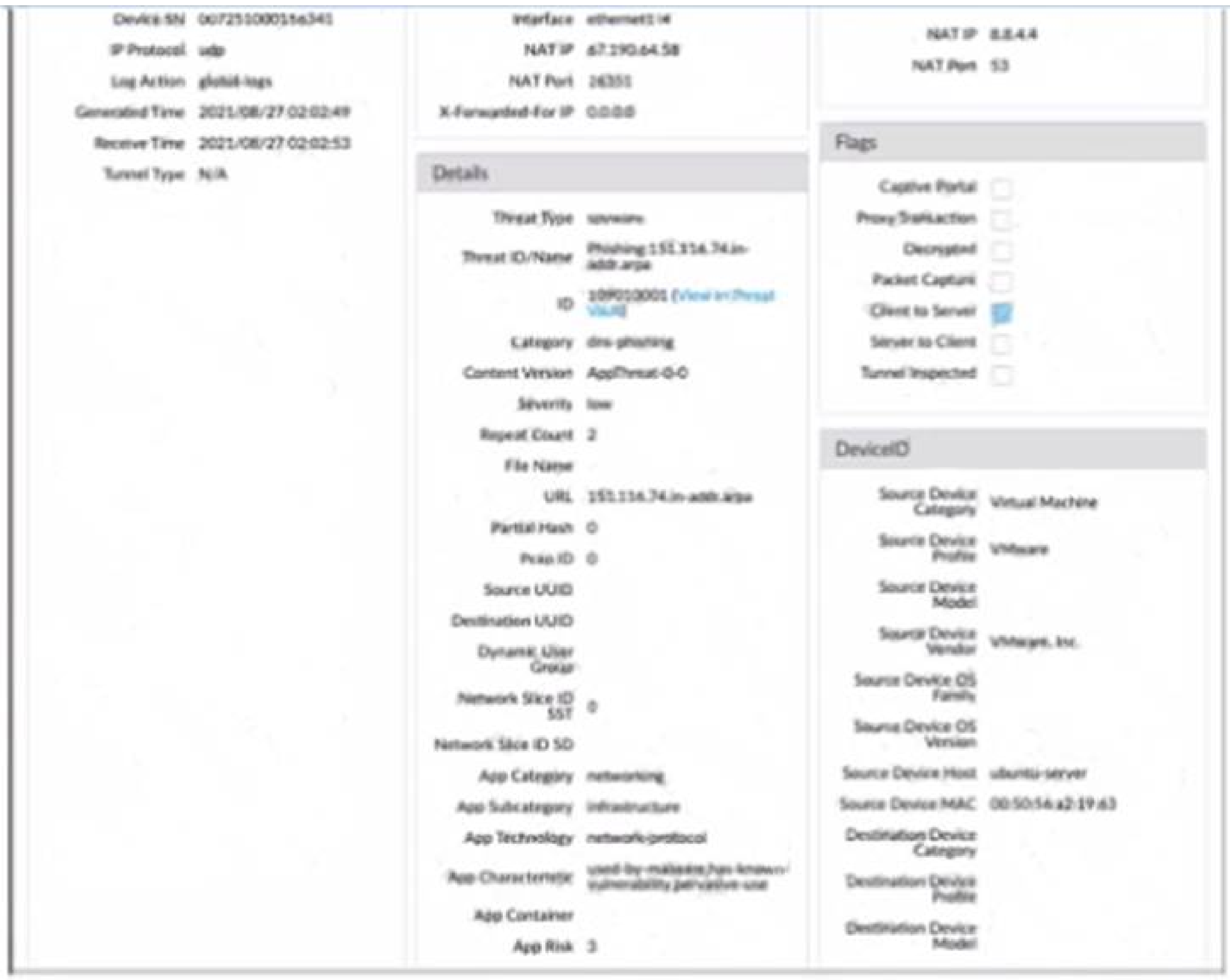
Answer: B

NEW QUESTION 78
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 83
Given the detailed log information above, what was the result of the firewall traffic inspection?



Device SN 007251000156341
IP Protocol udp
Log Action global-logs
Generated Time 2021/08/27 02:02:49
Receive Time 2021/08/27 02:02:53
Tunnel Type N/A

Interface ethernet1/4
NAT IP 67.190.64.58
NAT Port 26351
X-Forwarded-For IP 0.0.0.0

Details

Threat Type spyware
Threat ID/Name Phishing 151.114.74.in-addr.arpa
ID 109010001 (View in Threat Vault)
Category dns-phishing
Content Version AppThreat-0-0
Severity low
Repeat Count 2
File Name
URL 151.114.74.in-addr.arpa
Partial Hash 0
Pcap ID 0
Source UUID
Destination UUID
Dynamic User Group
Network Slice ID SST 0
Network Slice ID SD
App Category networking
App Subcategory infrastructure
App Technology network-protocol
App Characteristic used-by-malware,has-known-vulnerability,pervasive-use
App Container
App Risk 3

NAT IP 8.8.4.4
NAT Port 53

Flags

Captive Portal □
Proxy Transaction □
Decrypted □
Packet Capture □
Client to Server ☑
Server to Client □
Tunnel Inspected □

DeviceID

Source Device Category Virtual Machine
Source Device Profile VMware
Source Device Model
Source Device Vendor VMware, Inc.
Source Device OS Family
Source Device OS Version
Source Device Host ubuntu-server
Source Device MAC 00:50:56:a2:19:63
Destination Device Category
Destination Device Profile
Destination Device Model

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

Answer: C

NEW QUESTION 86
Your company occupies one floor in a single building you have two active directory domain controllers on a single networks the firewall s management plane is only slightly utilized.
Which user-ID agent sufficient in your network?

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

Answer: D

NEW QUESTION 89
What is the maximum volume of concurrent administrative account sessions?

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

Answer: C

NEW QUESTION 94
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

NEW QUESTION 98
Which built-in IP address EDL would be useful for preventing traffic from IP addresses that are verified as unsafe based on WildFire analysis Unit 42 research and data gathered from telemetry?

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

Answer: D

Explanation:
Palo Alto Networks Known Malicious IP Addresses
—Contains IP addresses that are verified malicious based on WildFire analysis, Unit 42 research, and data gathered from telemetry (Share ThreatIntelligence with Palo Alto Networks). Attackers use these IP addresses almost exclusively to distribute malware, initiate command-and-control activity, and launch attacks.
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/policy/use-an-external-dynamic-list-in-policy/built-

NEW QUESTION 103
Why should a company have a File Blocking profile that is attached to a Security policy?

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

Answer: A

NEW QUESTION 105
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 109
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 112
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 117
Prior to a maintenance-window activity, the administrator would like to make a backup of only the running configuration to an external location. What command in Device > Setup > Operations would provide the most operationally efficient way to achieve this outcome?

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

Answer: A

Explanation:
Export Named Configuration Snapshot This option exports the current running configuration, a candidate configuration snapshot, or a previously imported configuration (candidate or running). The firewall exports the configuration as an XML file with the specified name. You can save the snapshot in any network location. These exports often are used as backups. These XML files also can be used as templates for building other firewall configurations.

NEW QUESTION 119
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 121
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

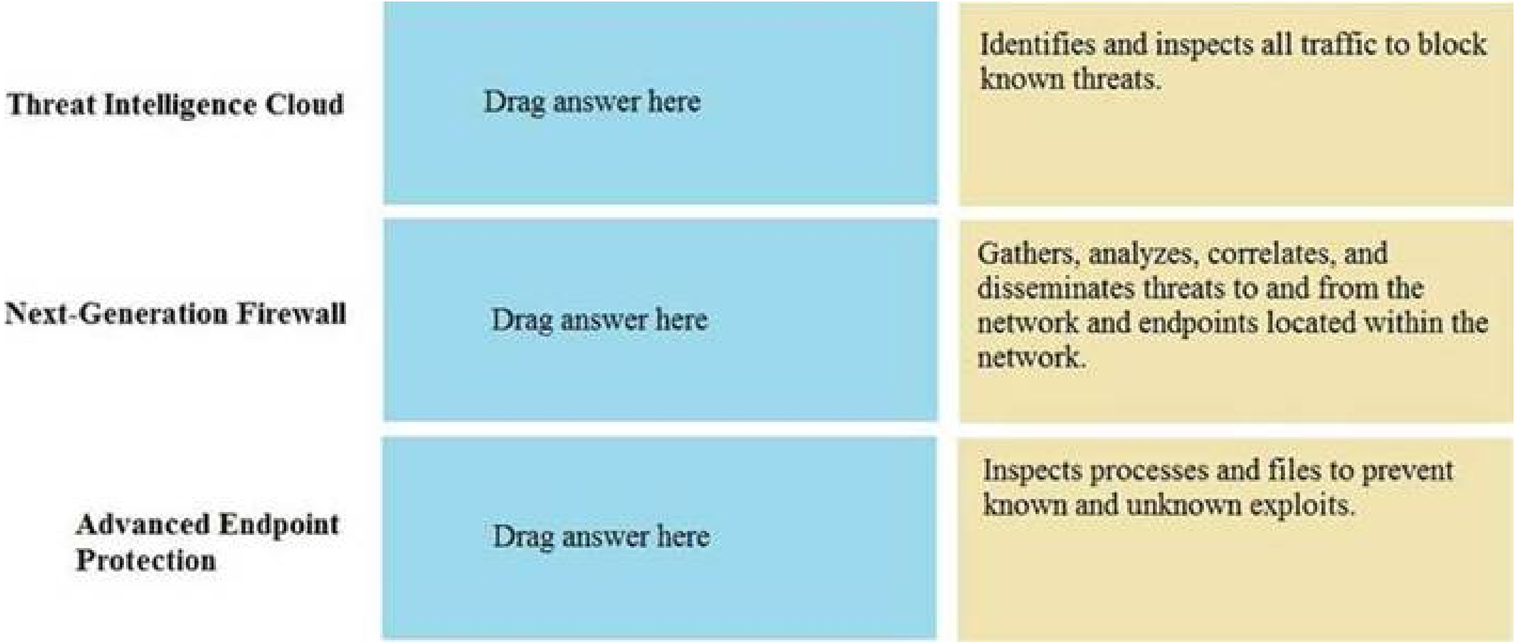
Answer: B

NEW QUESTION 124
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 128
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 130
What two authentication methods on the Palo Alto Networks firewalls support authentication and authorization for role-based access control? (Choose two.)

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

Answer: AB

NEW QUESTION 132
Which statement is true about Panorama managed devices?

A. Panorama automatically removes local configuration locks after a commit from Panorama
B. Local configuration locks prohibit Security policy changes for a Panorama managed device
C. Security policy rules configured on local firewalls always take precedence
D. Local configuration locks can be manually unlocked from Panorama

Answer: D

NEW QUESTION 135
What are the requirements for using Palo Alto Networks EDL Hosting Sen/ice?

A. any supported Palo Alto Networks firewall or Prisma Access firewall
B. an additional subscription free of charge
C. a firewall device running with a minimum version of PAN-OS 10.1
D. an additional paid subscription

Answer: A

NEW QUESTION 136
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

NEW QUESTION 141
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 145
How does an administrator schedule an Applications and Threats dynamic update while delaying installation of the update for a certain amount of time?

A. Disable automatic updates during weekdays
B. Automatically “download and install” but with the “disable new applications” option used
C. Automatically “download only” and then install Applications and Threats later, after the administrator approves the update
D. Configure the option for “Threshold”

Answer: D

NEW QUESTION 148
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

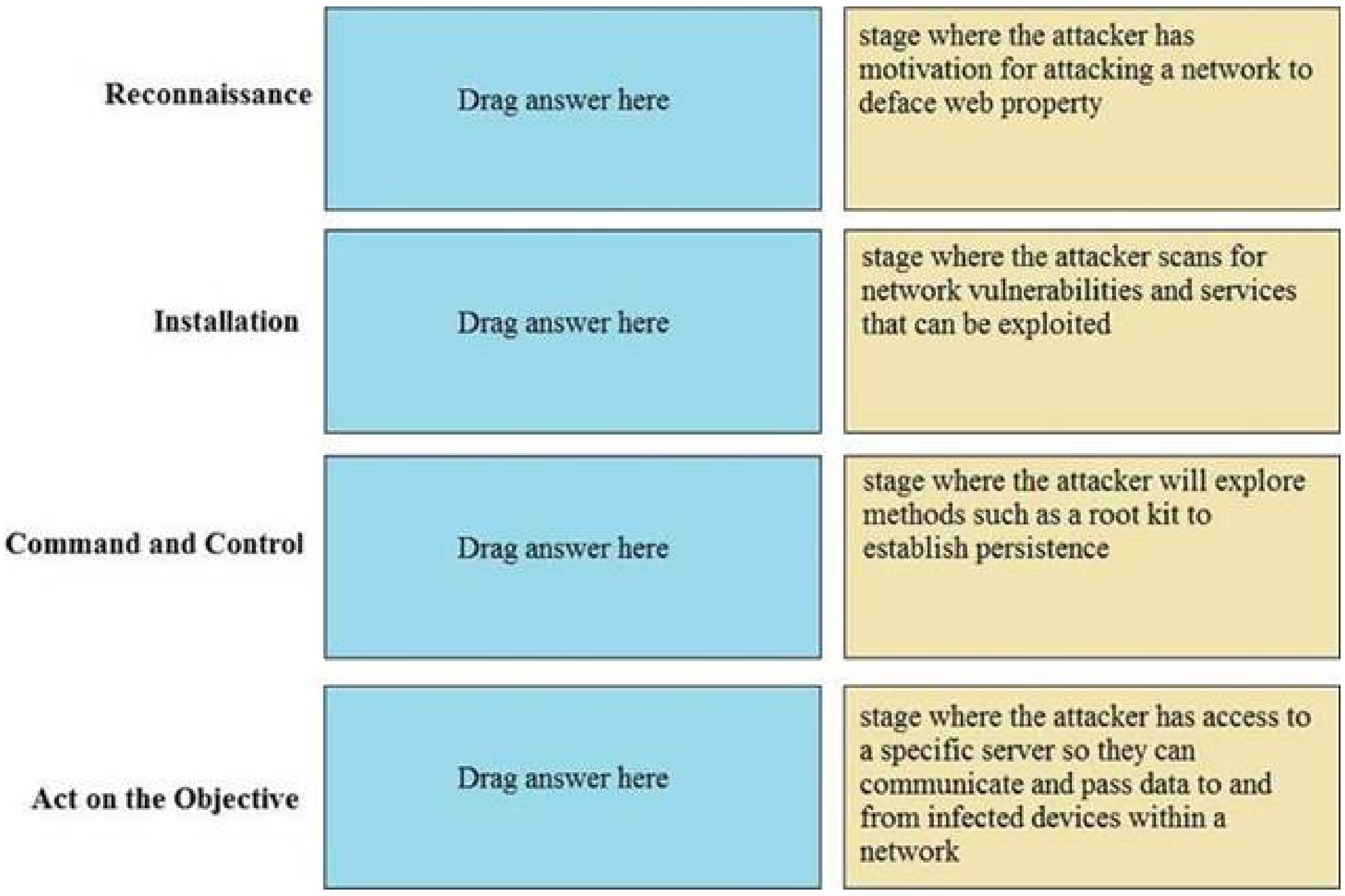
Answer: B

NEW QUESTION 149
Which statement best describes a common use of Policy Optimizer?

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

Answer: C

NEW QUESTION 154
Match the Cyber-Attack Lifecycle stage to its correct description.



Reconnaissance | Drag answer here | stage where the attacker has motivation for attacking a network to deface web property

Installation | Drag answer here | stage where the attacker scans for network vulnerabilities and services that can be exploited

Command and Control | Drag answer here | stage where the attacker will explore methods such as a root kit to establish persistence

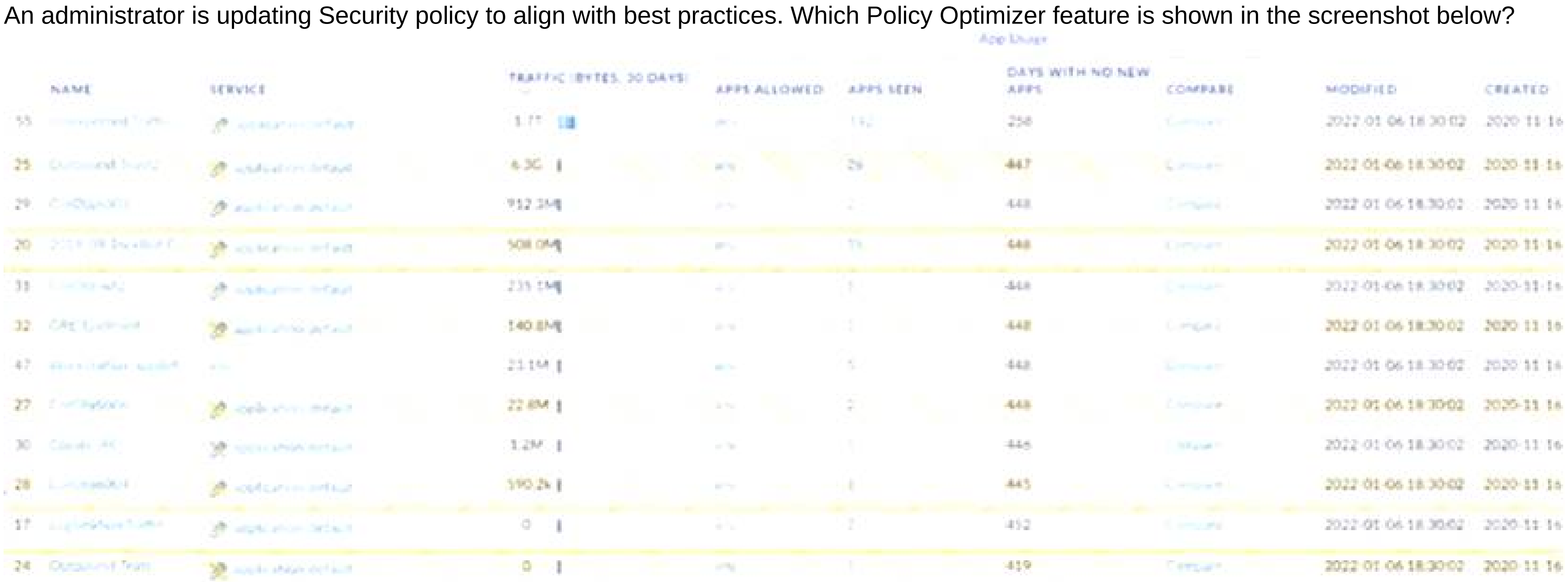
Act on the Objective | Drag answer here | stage where the attacker has access to a specific server so they can communicate and pass data to and from infected devices within a network

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 158
An administrator is updating Security policy to align with best practices. Which Policy Optimizer feature is shown in the screenshot below?



				App Usage					
	NAME	SERVICE	TRAFFIC (BYTES, 30 DAYS)	APPS ALLOWED	APPS SEEN	DAYS WITH NO NEW APPS	COMPARE	MODIFIED	CREATED
55	[illegible]	application-default	1.7T	[illegible]	152	258	Compare	2022-01-06 18:30:02	2020-11-16
25	[illegible]	application-default	6.3G	[illegible]	29	447	Compare	2022-01-06 18:30:02	2020-11-16
29	[illegible]	application-default	912.3M	[illegible]	2	448	Compare	2022-01-06 18:30:02	2020-11-16
20	[illegible]	application-default	508.0M	[illegible]	75	448	Compare	2022-01-06 18:30:02	2020-11-16
31	[illegible]	application-default	235.1M	[illegible]	1	448	Compare	2022-01-06 18:30:02	2020-11-16
32	[illegible]	application-default	140.8M	[illegible]	1	448	Compare	2022-01-06 18:30:02	2020-11-16
47	[illegible]	any	21.1M	[illegible]	5	448	Compare	2022-01-06 18:30:02	2020-11-16
27	[illegible]	application-default	22.8M	[illegible]	2	448	Compare	2022-01-06 18:30:02	2020-11-16
30	[illegible]	application-default	1.2M	[illegible]	1	446	Compare	2022-01-06 18:30:02	2020-11-16
28	[illegible]	application-default	590.2k	[illegible]	1	445	Compare	2022-01-06 18:30:02	2020-11-16
17	[illegible]	application-default	0	[illegible]	2	452	Compare	2022-01-06 18:30:02	2020-11-16
24	Outbound Trust	application-default	0	[illegible]	1	419	Compare	2022-01-06 18:30:02	2020-11-16

A. Rules without App Controls
B. New App Viewer
C. Rule Usage
D. Unused Unused Apps

Answer: C

NEW QUESTION 161
Selecting the option to revert firewall changes will replace what settings?

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

Answer: C

NEW QUESTION 166

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 170
Which three interface deployment methods can be used to block traffic flowing through the Palo Alto Networks firewall? (Choose three.)

A. Layer 2
B. Virtual Wire
C. Tap
D. Layer 3
E. HA

Answer: BDE

NEW QUESTION 171
Which stage of the cyber-attack lifecycle makes it important to provide ongoing education to users on spear phishing links, unknown emails, and risky websites?

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

Answer: B

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

- Gain full visibility into all traffic, including SSL, and block high-risk applications. Extend those protections to remote and mobile devices.
- Protect against perimeter breaches by blocking malicious or risky websites through URL filtering.
- Block known exploits, malware and inbound command-and-control communications using multiple threat prevention disciplines, including IPS, anti-malware, anti-CnC, DNS monitoring and sinkholing, and file and content blocking.
- Detect unknown malware and automatically deliver protections globally to thwart new attacks.
- Provide ongoing education to users on spear phishing links, unknown emails, risky websites, etc.

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

NEW QUESTION 173
You receive notification about a new malware that infects hosts An infection results in the infected host attempting to contact a command-and-control server Which Security Profile when applied to outbound Security policy rules detects and prevents this threat from establishing a command-and-control connection?

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

Answer: D

Explanation:
Anti-Spyware Security Profiles block spyware on compromised hosts from trying to communicate with external command-and-control (C2) servers, thus enabling you to detect malicious traffic leaving the network from infected clients.

NEW QUESTION 177
Which User-ID mapping method should be used for an environment with clients that do not authenticate to Windows Active Directory?

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

Answer: C

Explanation:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/user-id/map-ip-addresses-to-users/map-ip-addres

NEW QUESTION 180
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

NEW QUESTION 183
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 184
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 187
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

NEW QUESTION 190
What is the purpose of the automated commit recovery feature?

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

Answer: C

NEW QUESTION 191
To use Active Directory to authenticate administrators, which server profile is required in the authentication profile?

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

Answer: C

NEW QUESTION 193
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 197
According to the best practices for mission critical devices, what is the recommended interval for antivirus updates?

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

Answer: C

NEW QUESTION 199
The NetSec Manager asked to create a new firewall Local Administrator profile with customized privileges named NewAdmin. This new administrator has to

authenticate without inserting any username or password to access the WebUI.
What steps should the administrator follow to create the New_Admin Administrator profile?

A. * 1. Select the "Use only client certificate authentication" check box.* 2. Set Role to Role Based.* 3. Issue to the Client a Certificate with Common Name = NewAdmin
B. * 1. Select the "Use only client certificate authentication" check box.* 2. Set Role to Dynamic.* 3. Issue to the Client a Certificate with Certificate Name = NewAdmin
C. * 1. Set the Authentication profile to Local.* 2. Select the "Use only client certificate authentication" check box.* 3. Set Role to Role Based.
D. * 1. Select the "Use only client certificate authentication" check box.* 2. Set Role to Dynamic.* 3. Issue to the Client a Certificate with Common Name = New Admin

Answer: B

NEW QUESTION 204
What is a recommended consideration when deploying content updates to the firewall from Panorama?

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

Answer: D

NEW QUESTION 207
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 210
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 214
Which interface does not require a MAC or IP address?

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

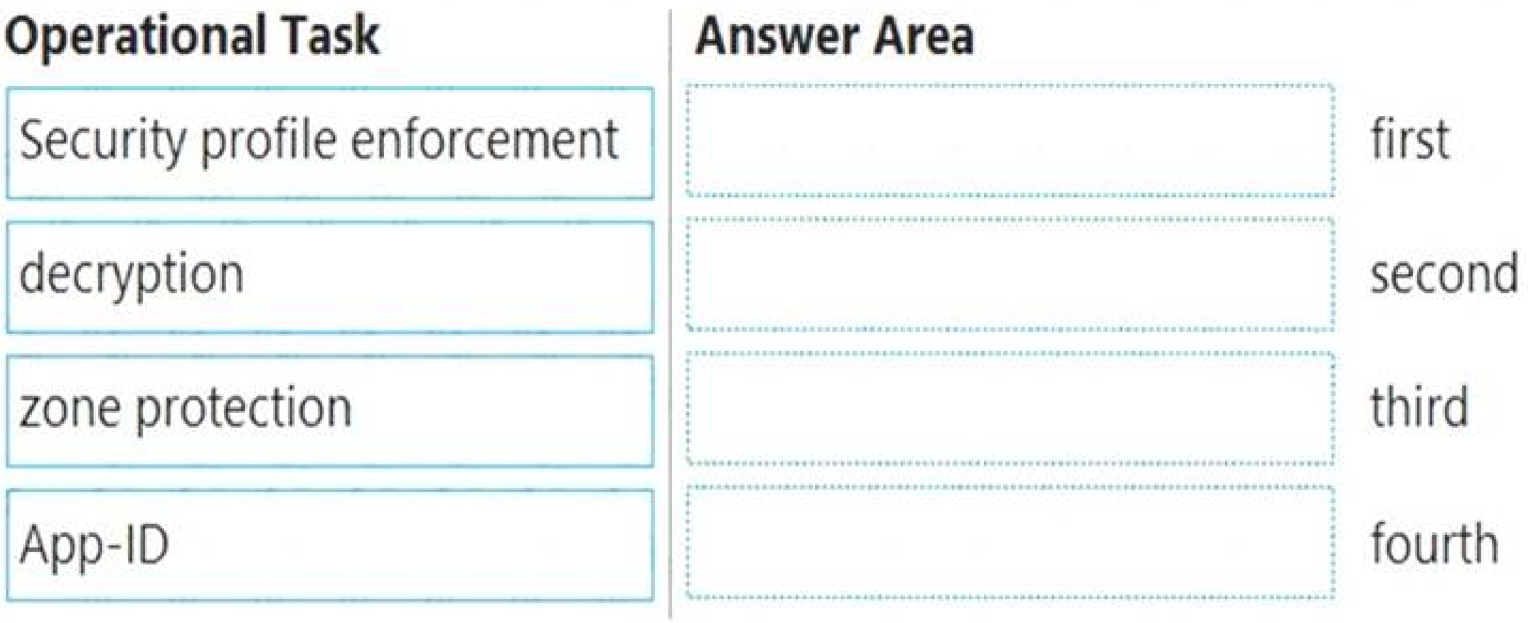
Answer: A

NEW QUESTION 217
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 218
Place the steps in the correct packet-processing order of operations.



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

A. Mastered
B. Not Mastered

Answer: A

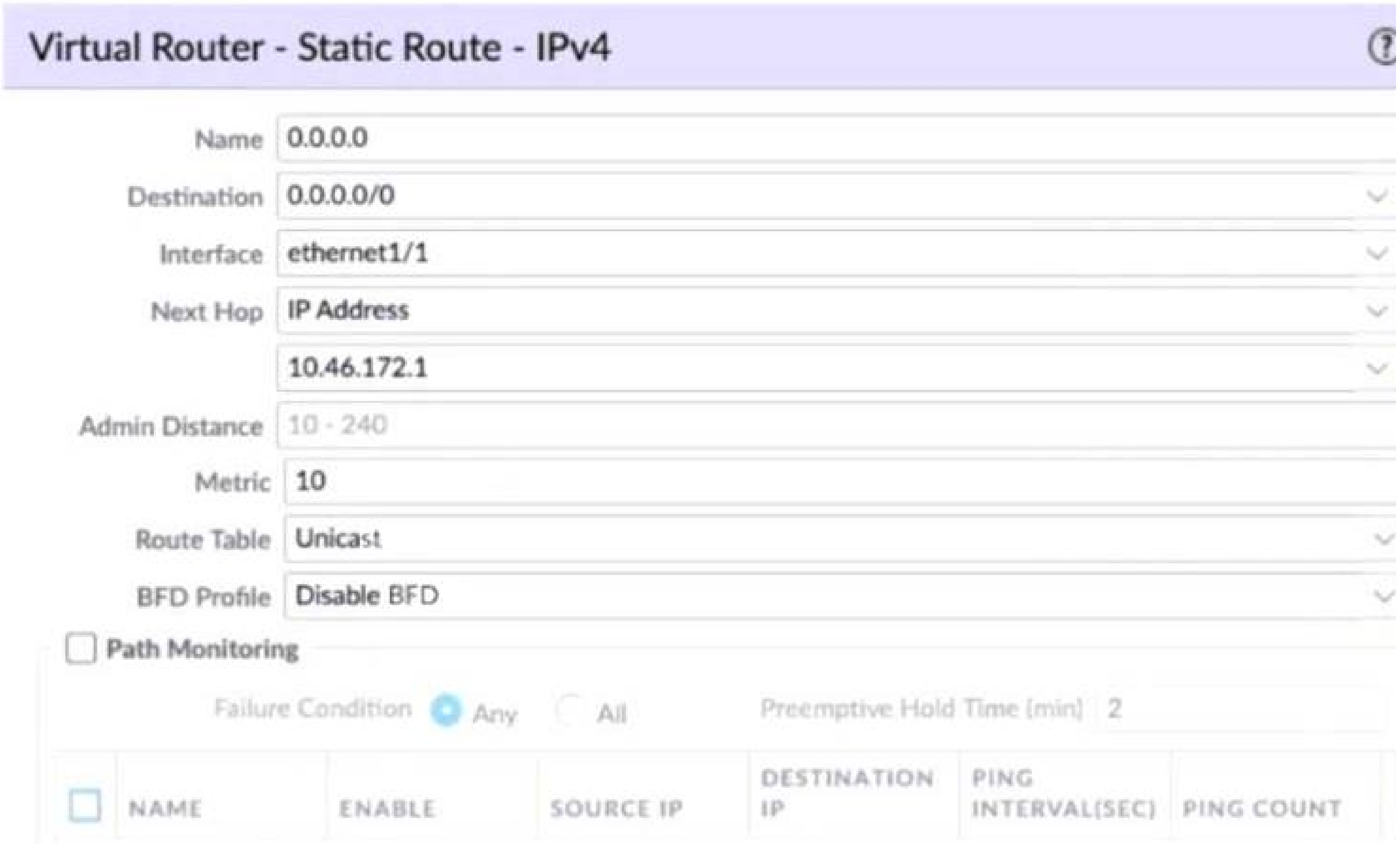
Explanation:
Text, application, table Description automatically generated with medium confidence

NEW QUESTION 221
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 226
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

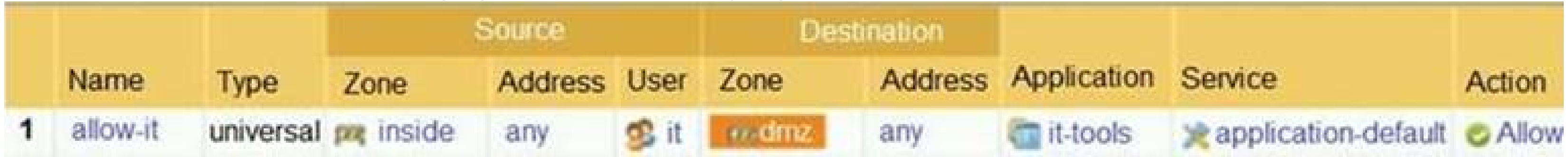
NEW QUESTION 230
Which Palo Alto Networks firewall security platform provides network security for mobile endpoints by inspecting traffic deployed as internet gateways?

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 233
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

NEW QUESTION 234
Which object would an administrator create to block access to all high-risk applications?

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

Answer: B

NEW QUESTION 237
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

NEW QUESTION 242
Which type firewall configuration contains in-progress configuration changes?

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

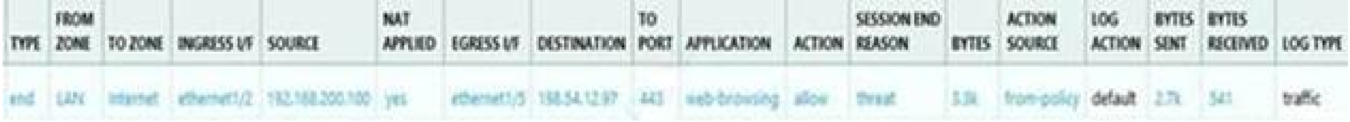
Answer: C

NEW QUESTION 246
Which interface type is part of a Layer 3 zone with a Palo Alto Networks firewall?

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

Answer: C

NEW QUESTION 249
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	188.54.12.97	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 254
You need to allow users to access the office–suite application of their choice. How should you configure the firewall to allow access to any office-suite application?

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

Answer: C

NEW QUESTION 258
Which two components are utilized within the Single-Pass Parallel Processing architecture on a Palo Alto Networks Firewall? (Choose two.)

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

Answer: BD

NEW QUESTION 260
What is a prerequisite before enabling an administrative account which relies on a local firewall user database?

A. Configure an authentication policy
B. Configure an authentication sequence
C. Configure an authentication profile
D. Isolate the management interface on a dedicated management VLAN

Answer: C

NEW QUESTION 264
......