Exam Questions PCNSA

Palo Alto Networks Certified Network Security Administrator

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

NEW QUESTION 1
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

NEW QUESTION 2
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.

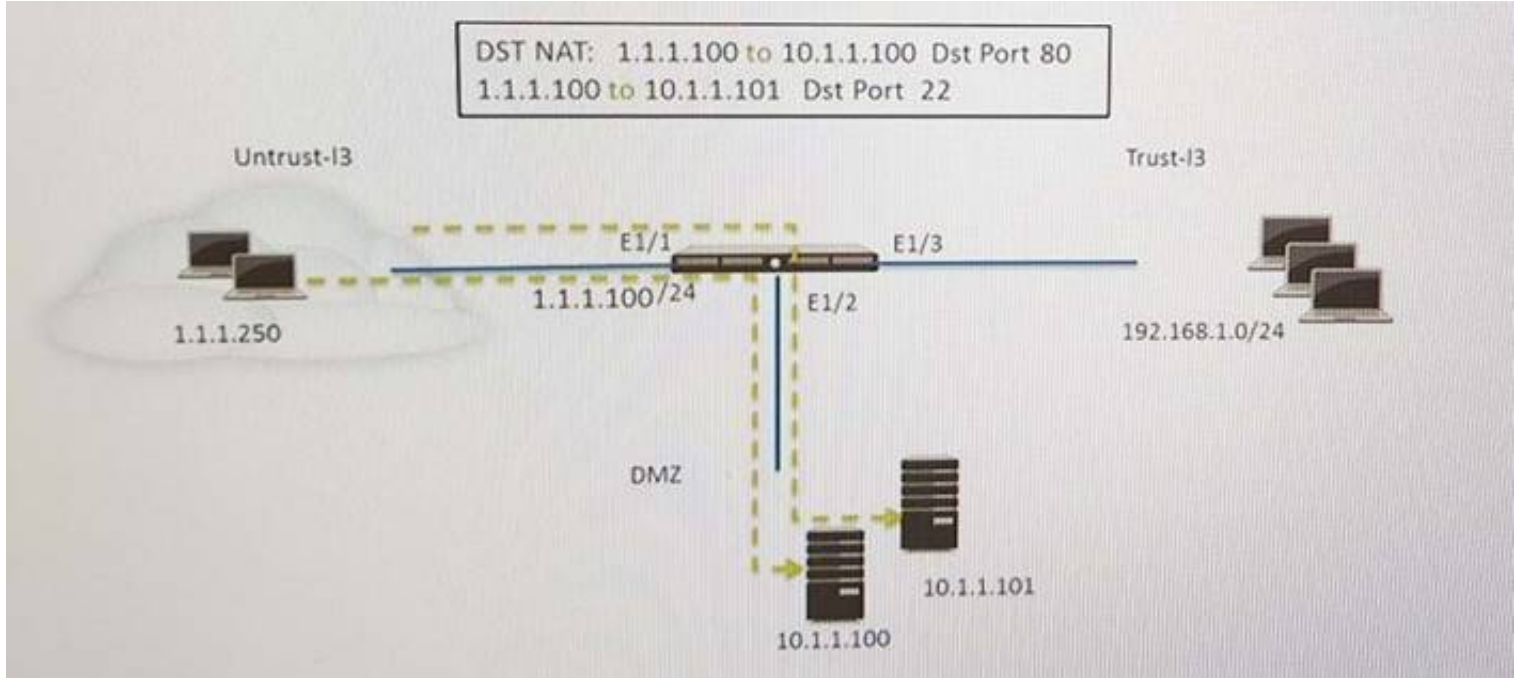
The Panorama web interface resembles the firewall web interface but with additional functions for centralized management.

NEW QUESTION 3
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 4
Refer to the exhibit. An administrator is using DNAT to map two servers to a single public IP address. Traffic will be steered to the specific server based on the application, where Host A (10.1.1.100) receives HTTP traffic and Host B (10.1.1.101) receives SSH traffic.

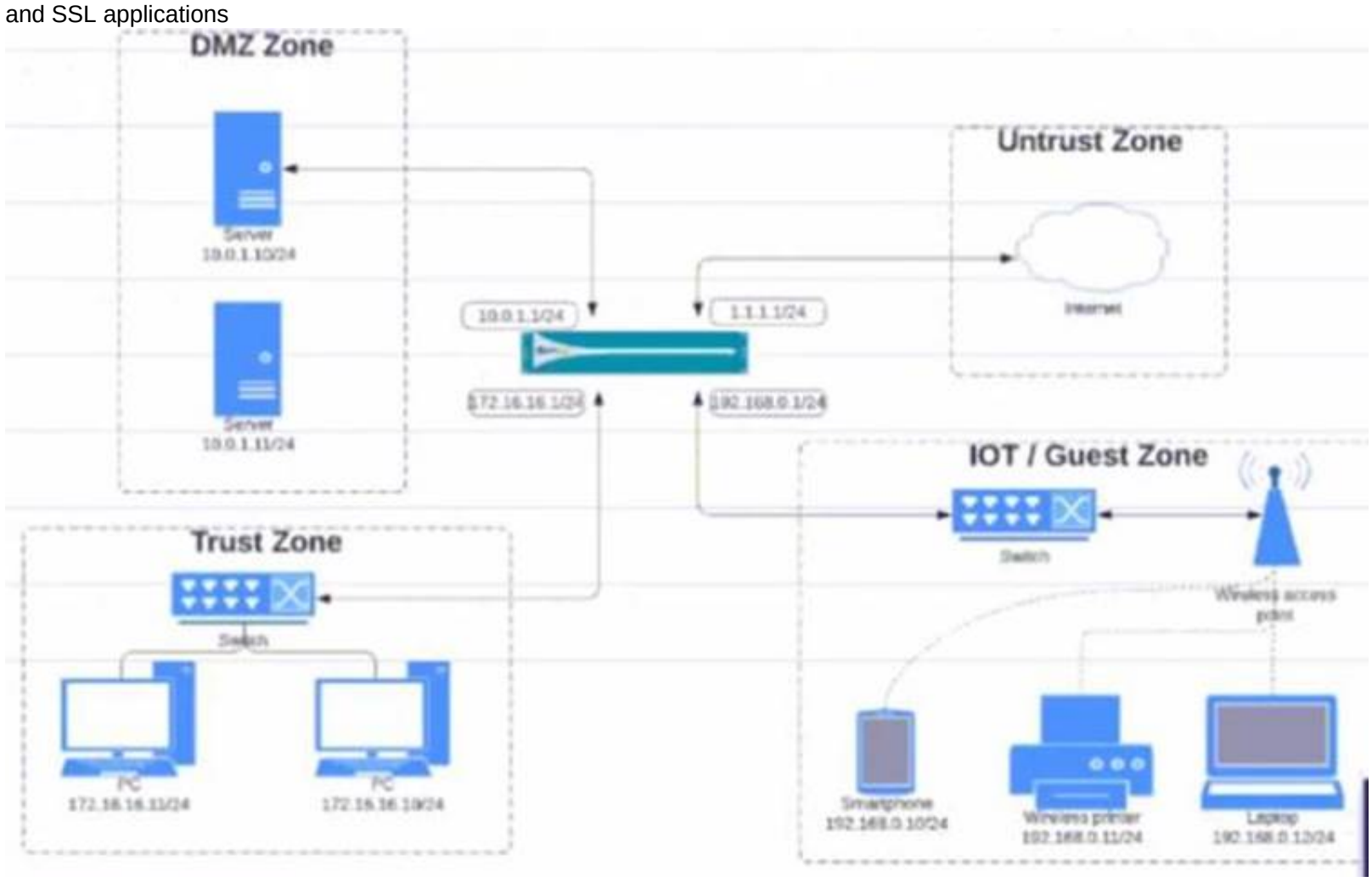


Which two Security policy rules will accomplish this configuration? (Choose two.)

A. Untrust (Any) to DMZ (1.1.1.100), ssh - Allow
B. Untrust (Any) to Untrust (10.1.1.1), web-browsing -Allow
C. Untrust (Any) to Untrust (10.1.1.1), ssh -Allow
D. Untrust (Any)to DMZ (10.1.1.100. 10.1.1.101), ssh, web-browsing-Allow
E. Untrust (Any) to DMZ (1.1.1.100), web-browsing - Allow

Answer: AE

NEW QUESTION 5
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)

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

D)

NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS
01-A	none	universal	IOT-Guest	10.0.1.0/24	any	any	DMZ	1.1.1.0/
			Trust	172.16.16.0/12			Untrust	192.168

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

Answer: C

NEW QUESTION 6
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 7
Access to which feature requires the PAN-OS Filtering license?

A. PAN-DB database
B. DNS Security
C. Custom URL categories
D. URL external dynamic lists

Answer: A

NEW QUESTION 8
Which two statements are true for the DNS security service introduced in PAN-OS version 10.0?

A. It functions like PAN-DB and requires activation through the app portal.
B. It removes the 100K limit for DNS entries for the downloaded DNS updates.
C. IT eliminates the need for dynamic DNS updates.
D. IT is automatically enabled and configured.

Answer: AB

NEW QUESTION 9
The firewall sends employees an application block page when they try to access Youtube. Which Security policy rule is blocking the youtube application?

			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. intrazone-default
B. Deny Google
C. allowed-security services
D. interzone-default

Answer: D

NEW QUESTION 10
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 14
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 19
You must configure which firewall feature to enable a data-plane interface to submit DNS queries on behalf of the control plane?

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

Answer: A

NEW QUESTION 22
All users from the internal zone must be allowed only Telnet access to a server in the DMZ zone. Complete the two empty fields in the Security Policy rules that permits only this type of access.
Source Zone: Internal
Destination Zone: DMZ Zone
Application: _____?
Service: _____?
Action: allow
Choose two.

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

Answer: BC

NEW QUESTION 25
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 27
Which type of security rule will match traffic between the Inside zone and Outside zone, within the Inside zone, and within the Outside zone?

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

Answer: D

Explanation:
References:https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClomCAC

NEW QUESTION 31
An administrator configured a Security policy rule with an Antivirus Security profile. The administrator did not change the action (or the profile. If a virus gets detected, how wilt the firewall handle the traffic?

A. It allows the traffic because the profile was not set to explicitly deny the traffic.
B. It drops the traffic because the profile was not set to explicitly allow the traffic.
C. It uses the default action assigned to the virus signature.
D. It allows the traffic but generates an entry in the Threat logs.

Answer: B

NEW QUESTION 34
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

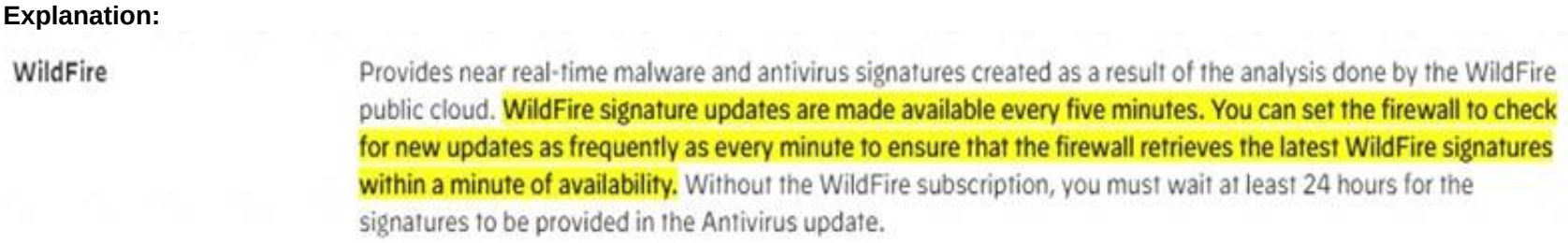
Answer: D

NEW QUESTION 37
What in the minimum frequency for which you can configure the firewall too check for new wildfire antivirus signatures?

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

Answer: B

Explanation:



NEW QUESTION 40
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 41
Which license must an administrator acquire prior to downloading Antivirus updates for use with the firewall?

A. URL filtering
B. Antivirus
C. WildFire
D. Threat Prevention

Answer: D

NEW QUESTION 46
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 47
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-profi

NEW QUESTION 52
Which file is used to save the running configuration with a Palo Alto Networks firewall?

A. running-config.xml
B. run-config.xml
C. running-configuration.xml
D. run-configuratin.xml

Answer: A

NEW QUESTION 57
What are two valid selections within an Antivirus profile? (Choose two.)

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

Answer: BC

NEW QUESTION 59
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

NEW QUESTION 63
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 67
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 69
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 71
During the App-ID update process, what should you click on to confirm whether an existing policy rule is affected by an App-ID update?

A. check now
B. review policies
C. test policy match
D. download

Answer: B

NEW QUESTION 72
What is the maximum volume of concurrent administrative account sessions?

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

Answer: C

NEW QUESTION 77
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 78
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 83
Which Security policy action will message a user's browser thai their web session has been terminated?

A. Reset server
B. Deny
C. Drop
D. Reset client

Answer: B

NEW QUESTION 87
Which statement is true regarding NAT rules?

A. Static NAT rules have precedence over other forms of NAT.
B. Translation of the IP address and port occurs before security processing.
C. NAT rules are processed in order from top to bottom.
D. Firewall supports NAT on Layer 3 interfaces only.

Answer: C

Explanation:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/networking/nat/nat-policy-rules/nat-policy-overvie

NEW QUESTION 90
An administrator needs to allow users to use their own office applications. How should the administrator configure the firewall to allow multiple applications in a dynamic environment?

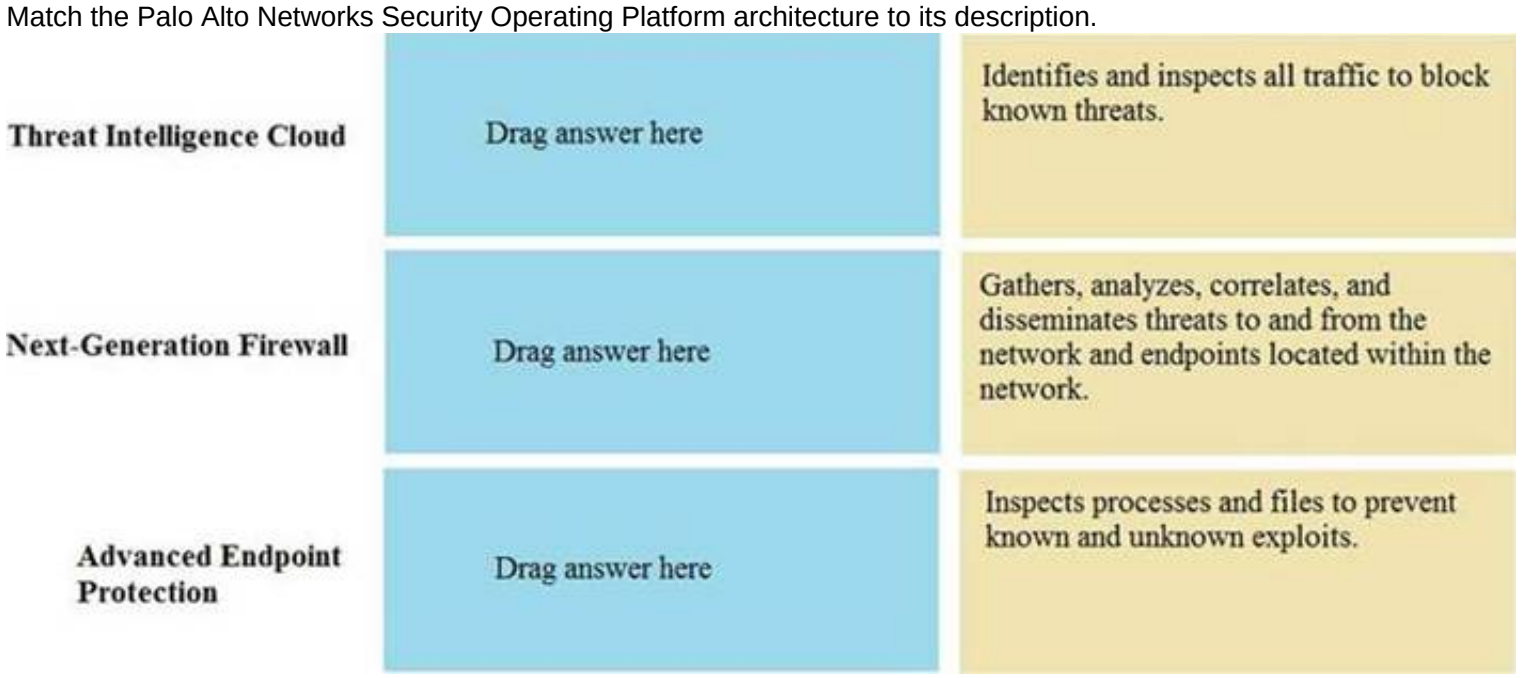
A. Create an Application Filter and name it Office Programs, the filter it on the business-systems category, office-programs subcategory

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 business-systems category
D. Create an Application Group and add Office 365, Evernote, Google Docs, and Libre Office

Answer: A

Explanation:
An application filter is an object that dynamically groups applications based on application attributes that you define, including category, subcategory, technology, risk factor, and characteristic. This is useful when you want to safely enable access to applications that you do not explicitly sanction, but that you want users to be able to access. For example, you may want to enable employees to choose their own office programs (such as Evernote, Google Docs, or Microsoft Office 365) for business use. To safely enable these types of applications, you could create an application filter that matches on the Category business-systems and the Subcategory office-programs. As new applications office programs emerge and new App-IDs get created, these new applications will automatically match the filter you defined; you will not have to make any additional changes to your policy rulebase to safely enable any application that matches the attributes you defined for the filter.
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/app-id/use-application-objects-in
-policy/create-an-application-filter.html

NEW QUESTION 95
Match the Palo Alto Networks Security Operating Platform architecture to its description.



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 96
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

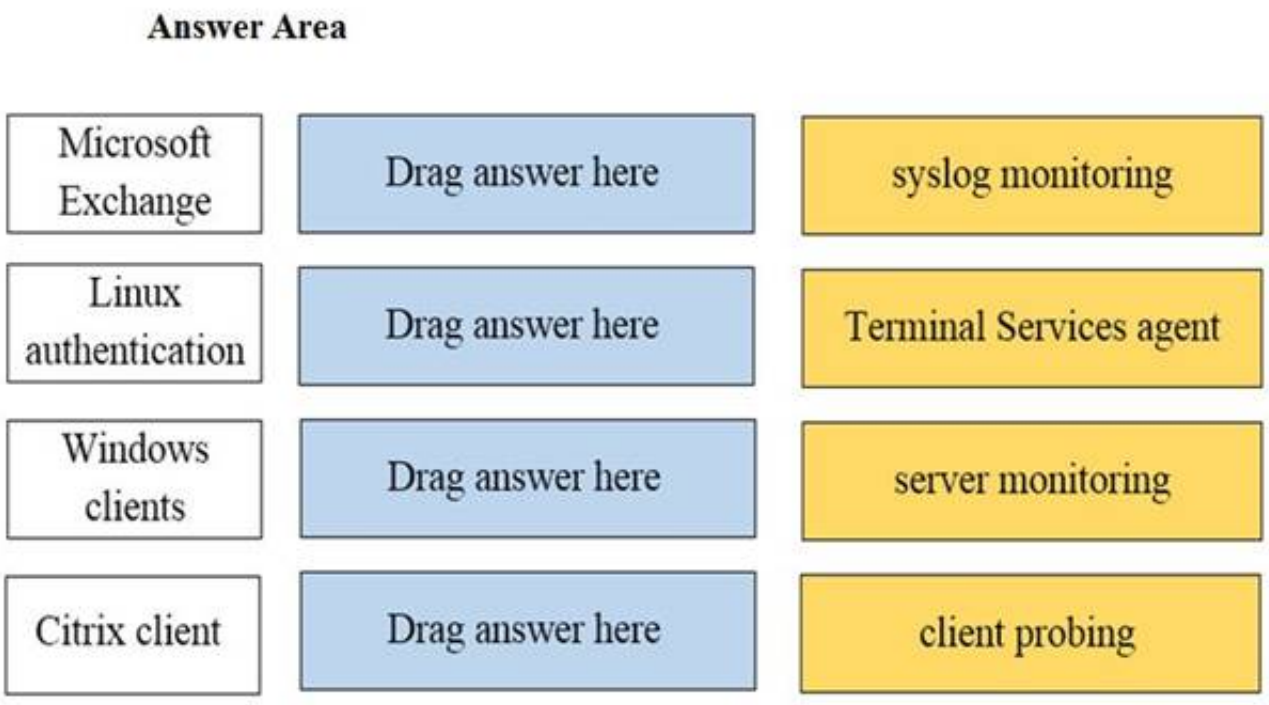
Answer: C

NEW QUESTION 101
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 105
Match the network device with the correct User-ID technology.



A. Mastered
B. Not Mastered

Answer: A

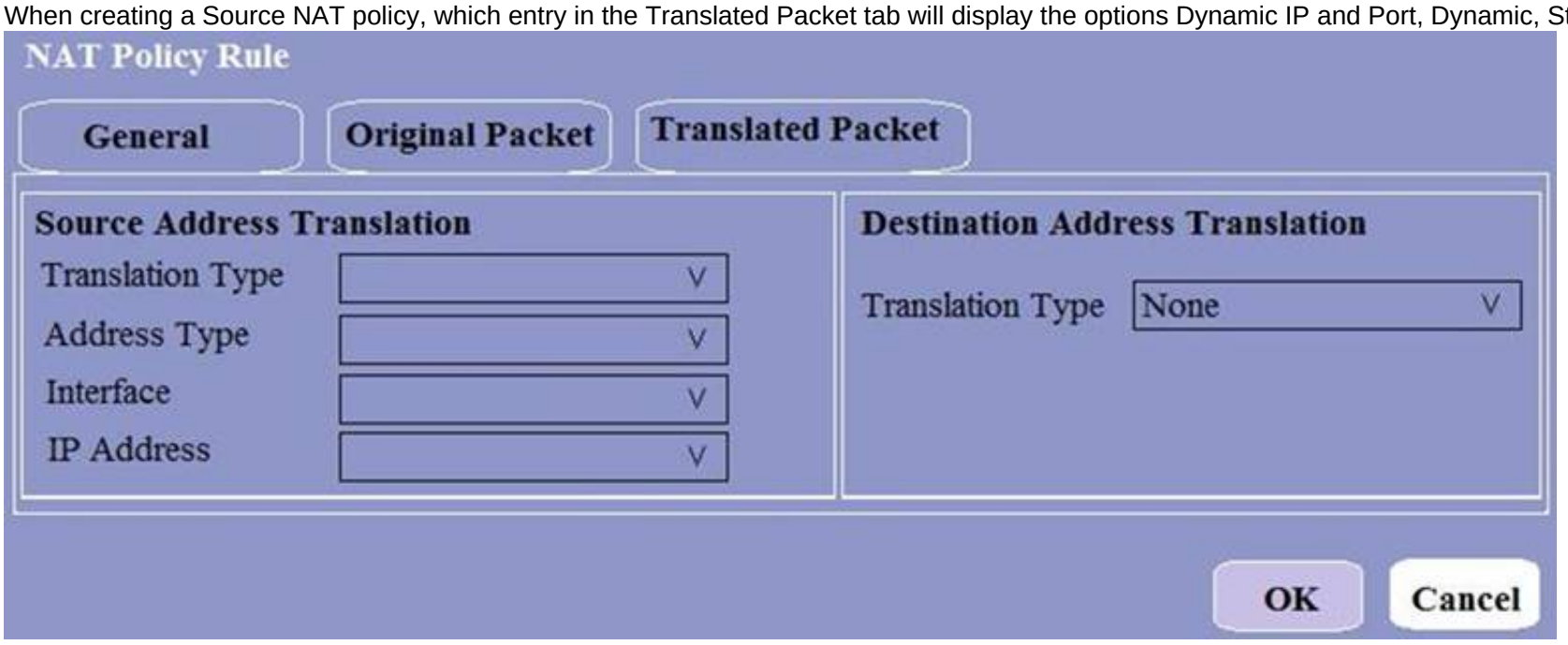
Explanation:
Microsoft Exchange – Server monitoring Linux authentication – syslog monitoring Windows Client – client probing
Citrix client – Terminal Services agent

NEW QUESTION 110
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

NEW QUESTION 113
When creating a Source NAT policy, which entry in the Translated Packet tab will display the options Dynamic IP and Port, Dynamic, Static IP, and None?



A. Translation Type
B. Interface
C. Address Type
D. IP Address

Answer: A

NEW QUESTION 118
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 121
Which plane on a Palo alto networks firewall provides configuration logging and reporting functions on a separate processor?

A. data
B. network processing
C. management
D. security processing

Answer: C

NEW QUESTION 123
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 128
What can be used as match criteria for creating a dynamic address group?

A. Usernames
B. IP addresses
C. Tags
D. MAC addresses

Answer: C

NEW QUESTION 133
Which protocol used to map username to user groups when user-ID is configured?

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

Answer: D

NEW QUESTION 138
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

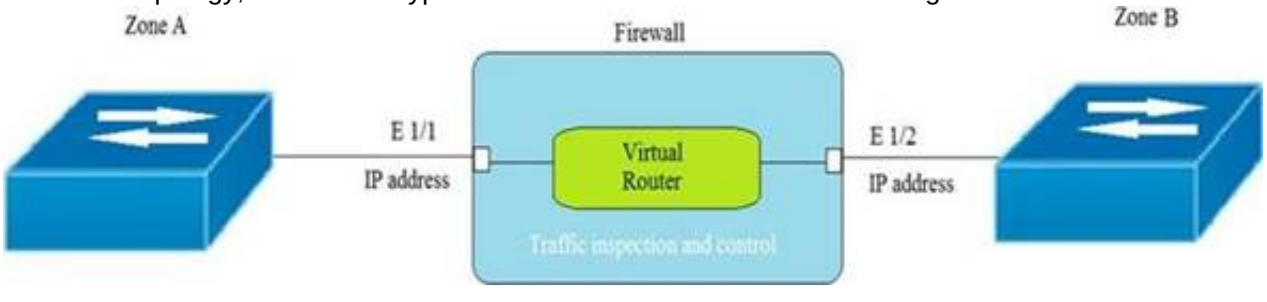
Answer: D

NEW QUESTION 139
Which Security profile would you apply to identify infected hosts on the protected network uwall user database?

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

Answer: A

NEW QUESTION 141
Given the topology, which zone type should zone A and zone B to be configured with?



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

Answer: A

NEW QUESTION 146
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

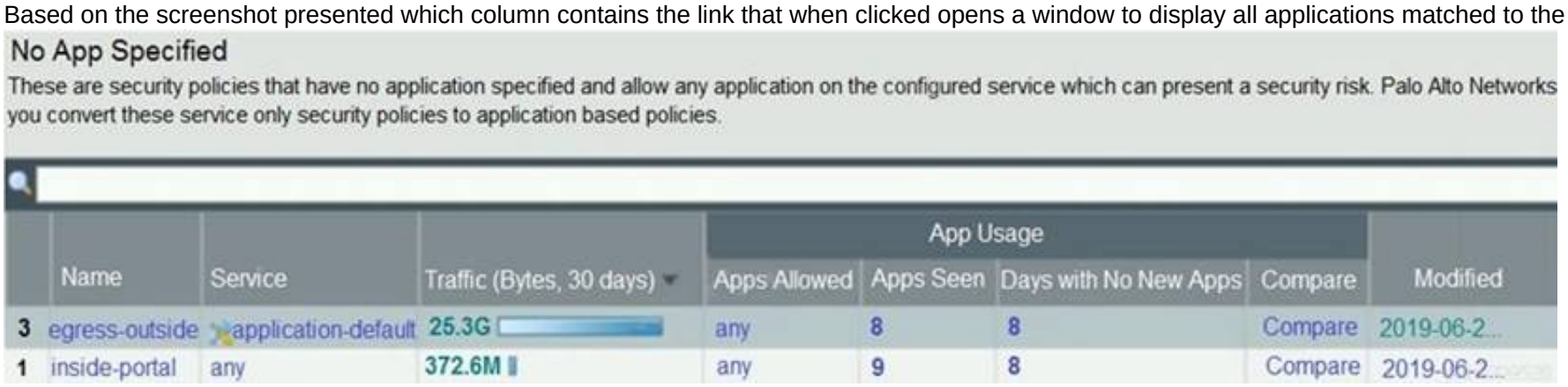
NEW QUESTION 149
What allows a security administrator to preview the Security policy rules that match new application signatures?

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

NEW QUESTION 154
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 156
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 158
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 161
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 164
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 167
What is the main function of Policy Optimizer?

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

Answer: D

NEW QUESTION 171
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 176
What is the minimum timeframe that can be set on the firewall to check for new WildFire signatures?

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

Answer: D

Explanation:
Because new WildFire signatures are now available every five minutes, it is a best practice to use this setting to ensure the firewall retrieves these signatures within a minute of availability.

NEW QUESTION 180
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 183
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 184
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 187
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 191
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 196
Which two settings allow you to restrict access to the management interface? (Choose two)

A. enabling the Content-ID filter
B. administrative management services
C. restricting HTTP and telnet using App-ID
D. permitted IP addresses

Answer: AC

NEW QUESTION 198
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 200
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 201
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 206
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 211
Which interface does not require a MAC or IP address?

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

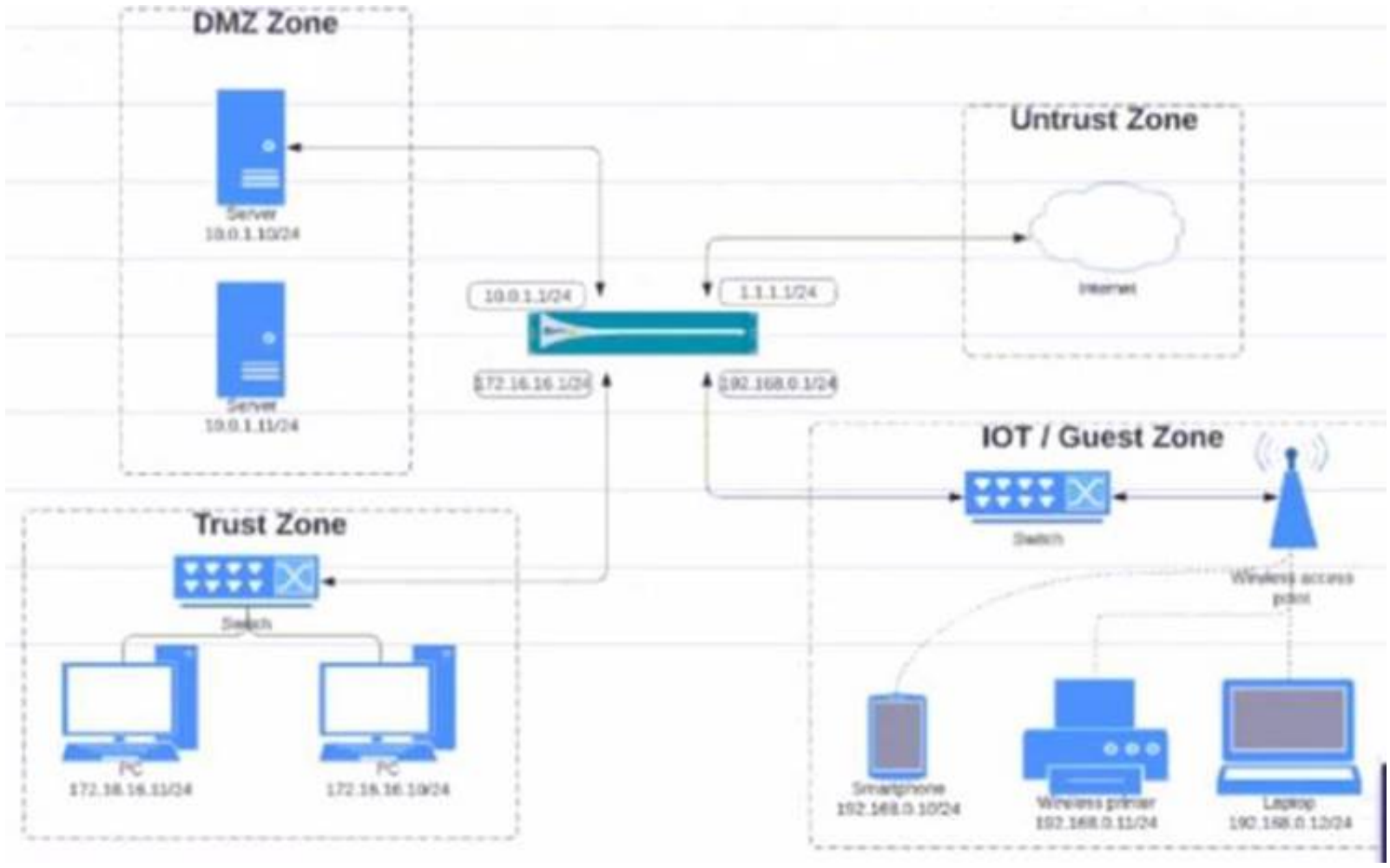
Answer: A

NEW QUESTION 215
Which interface type can use virtual routers and routing protocols?

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

Answer: B

NEW QUESTION 220
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)

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)

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

D)

NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS
01-A	none	universal	IOT-Guest	10.0.1.0/24	any	any	DMZ	1.1.1.0/
			Trust	172.16.16.0/22			Untrust	192.168

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

Answer: C

NEW QUESTION 223
Which type of profile must be applied to the Security policy rule to protect against buffer overflows illegal code execution and other attempts to exploit system flaws?

A. anti-spyware

B. URL filtering
C. vulnerability protection
D. file blocking

Answer: C

NEW QUESTION 224
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 asecurity-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 containssource-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 anydestination-Ip-address
E. In addition to option c, an additional rule from zone OUTSIDE to USERS for application SSH from any source-IP-address to any destination-IP-address is required to allow the return-traffic from theSSH-servers to reach the server-admin

Answer: B

NEW QUESTION 228
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 232
Which type firewall configuration contains in-progress configuration changes?

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

Answer: C

NEW QUESTION 235
Which security policy rule would be needed to match traffic that passes between the Outside zone and Inside zone, but does not match traffic that passes within the zones?

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

Answer: B

NEW QUESTION 238
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	ethernet1/3	198.54.12.97	443	web-browsing	allow	threat	3.3k	from-policy	default	2.7k	541	traffic

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

Answer: D

NEW QUESTION 242
Which feature would be useful for preventing traffic from hosting providers that place few restrictions on content, whose services are frequently used by attackers to distribute illegal or unethical material?

A. Palo Alto Networks Bulletproof IP Addresses

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

Answer: A

Explanation:
To block hosts that use bulletproof hosts to provide malicious, illegal, and/or unethical content, use the bulletproof IP address list in policy.
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-new-features/content-inspection-features/edl-for-bulletpro

NEW QUESTION 247
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual PCNSA Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the PCNSA Product From:

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

Money Back Guarantee

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