ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

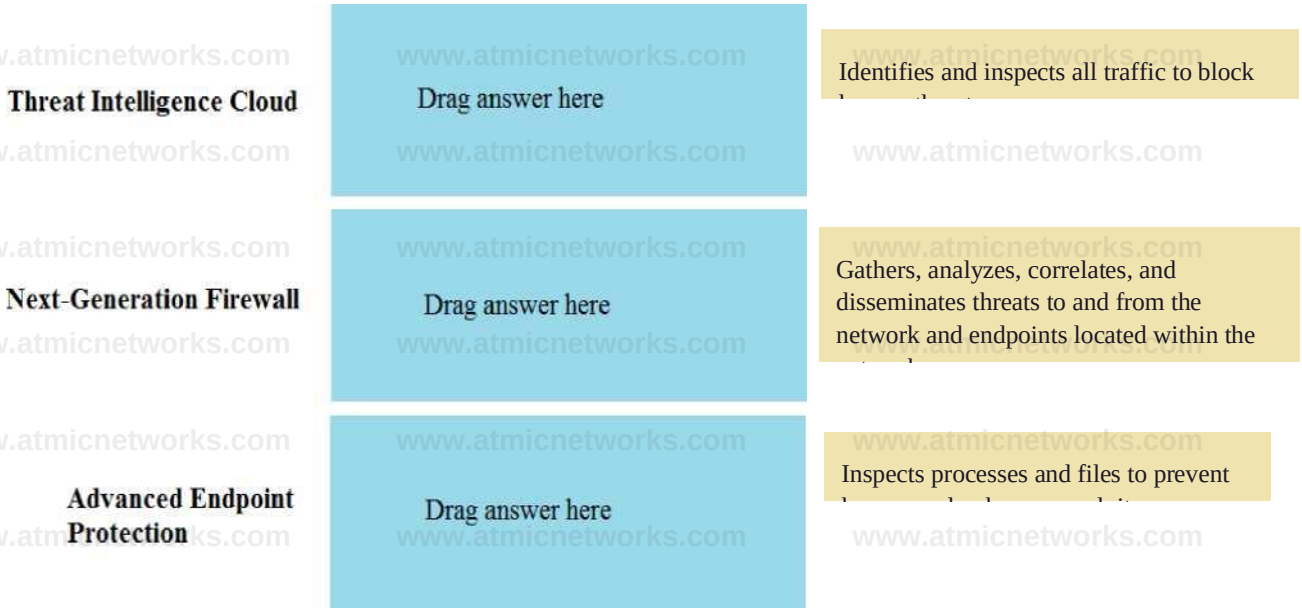
www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

Question: 1

DRAG DROP

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



Answer:

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

Question: 2

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

Explanation:

Question: 3

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

Question: 4

How many zones can an interface be assigned with a Palo Alto Networks firewall?

A. two

B. three

C. four

D. one

Answer: D

Explanation:

Reference:

Question: 5

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

Palo Alto Networks User-ID Agent Setup

Enable Security Log \/ Sewer Log Monitor Frequency (sec) **15** Enable Session V Sewer Session Read Frequency (sec) **10** Novell eDirectow Query Intewal (sec) **30** Syslog Sewice Profile Enable Probing Probe Interval (min) **20** Enable User Identification Timeout V User Identification Timeout (min) **45** Allow matching usernames without domains

Enable NTLM NTLM Domain User-ID Collector Name

A. Enable Security Log

B. Server Log Monitor Frequency (sec)

C. Enable Session

D. Enable Probing

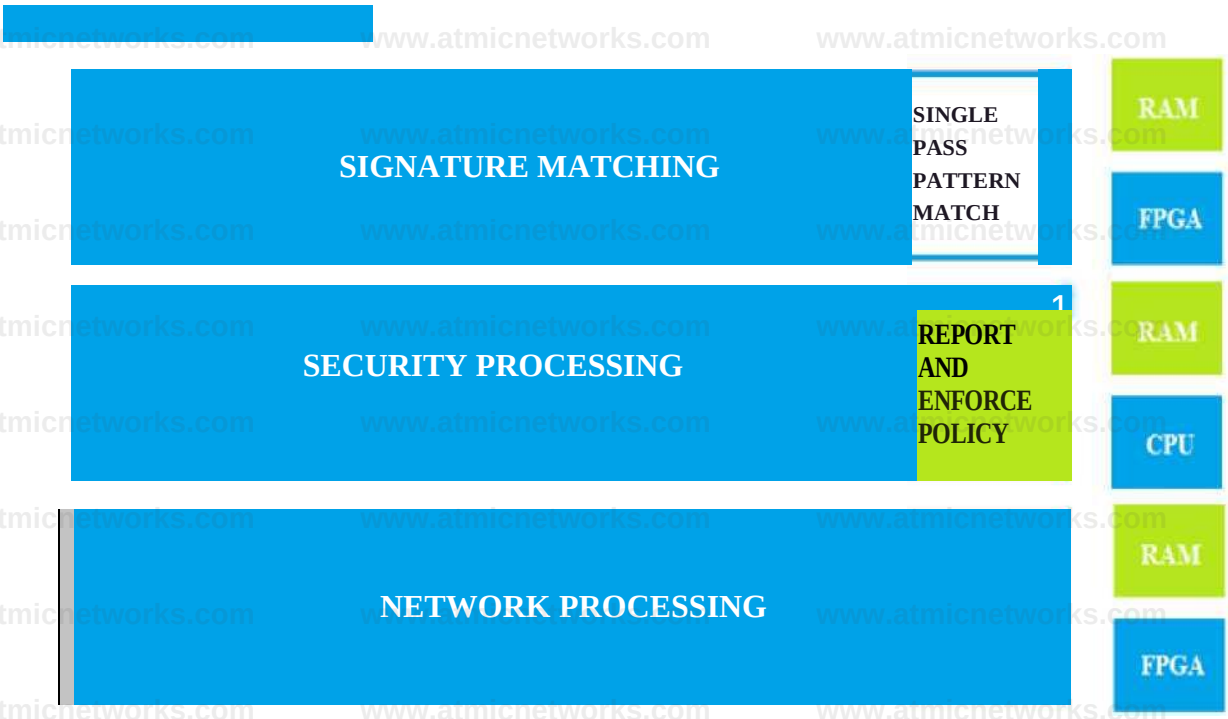
Answer: B,C

Explanation:

Reference:

Question: 6

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



A. Signature Matching

B. Network Processing

C. Security Processing

D. Security Matching

Answer: A

Explanation:

Question: 7

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

Question: 8

Actions can be set for which two items in a URL filtering security profile? (Choose two.)

A. Block List

B. Custom URL Categories

C. PAN-DB URL Categories

D. Allow List

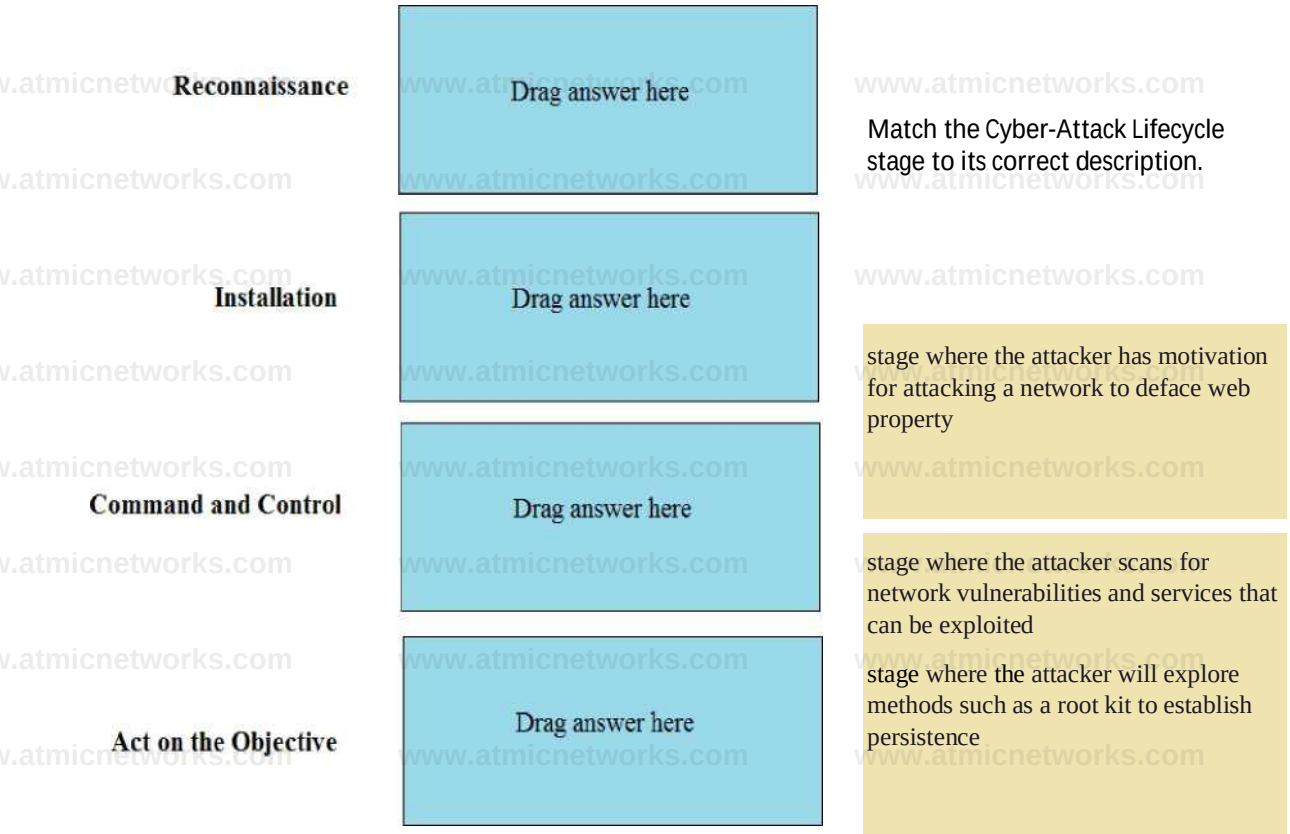
Answer: A,D

Explanation:

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

Question: 9

DRAG DROP



Answer:

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

Question: 10

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: A,D

Explanation:

Question: 11

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

A. Windows session monitoring via a domain controller

B. passive server monitoring using the Windows-based agent

C. Captive Portal

D. passive server monitoring using a PAN-OS integrated User-ID agent

Answer: C

Explanation:

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

Question: 12

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

Question: 13

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

Explanation:

Question: 14

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

Explanation:

Question: 15

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

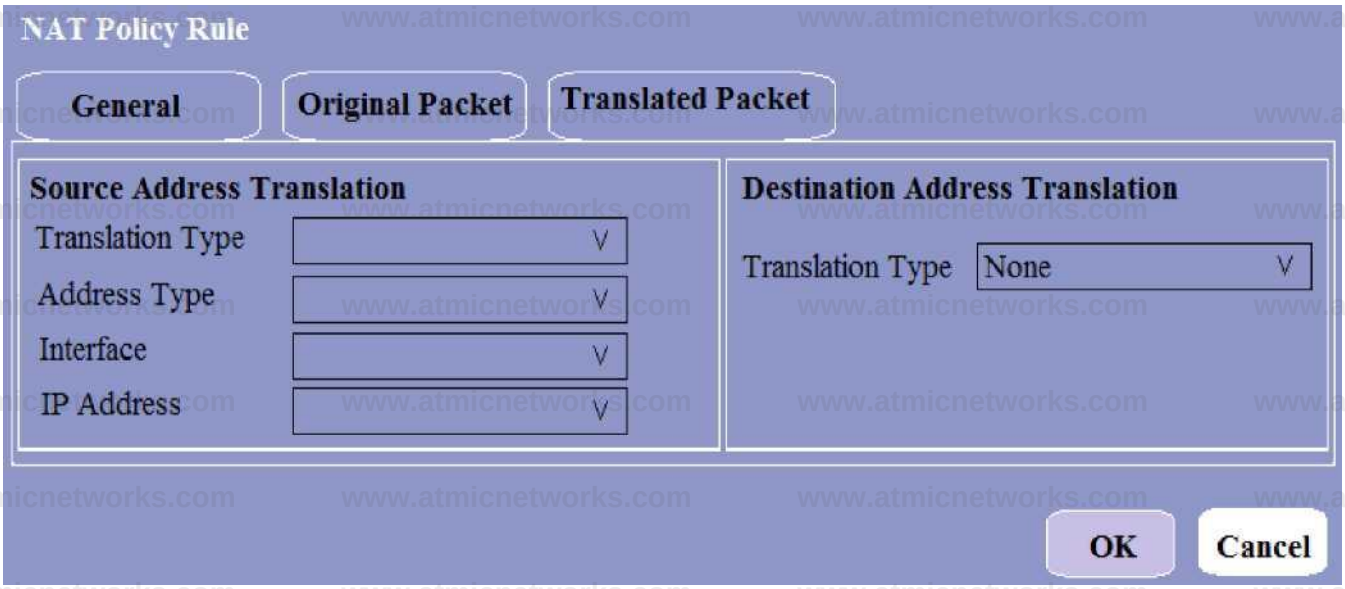
Answer: B

Explanation:

Security profiles are objects added to policy rules that are configured with an action of allow.

Question: 16

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

Explanation:

Question: 17

Which interface does not require a MAC or IP address?

A. Virtual Wire

B. Layer3

C. Layer2

D. Loopback

Answer: A

Explanation:

Question: 18

A company moved its old port-based firewall to a new Palo Alto Networks NGFW 60 days ago. Which utility should the company use to identify out-of-date or unused rules on the firewall?

A. Rule Usage Filter > No App Specified

B. Rule Usage Filter >Hit Count > Unused in 30 days

C. Rule Usage Filter > Unused Apps

D. Rule Usage Filter > Hit Count > Unused in 90 days

Answer: D

Explanation:

Question: 19

DRAG DROP

Order the steps needed to create a new security zone with a Palo Alto Networks firewall.

Step 1	Drag answer here	Select Zones from the list of available items
Step 2	Drag answer here	Assign interfaces as needed
Step 3	Drag answer here	Select Network tab
Step 4	Drag answer here	Specify Zone Name
Step 5	Drag answer here	Select Add
Step 6	Drag answer here	Specify Zone Type

Answer:

Explanation:

Step 1 – Select network tab

Step 2 – Select zones from the list of available items

Step 3 – Select Add

Step 4 – Specify Zone Name

Step 5 – Specify Zone Type

Step 6 – Assign interfaces as needed

Question: 20

What are two differences between an implicit dependency and an explicit dependency in App-ID? (Choose two.)

A. An implicit dependency does not require the dependent application to be added in the security policy

B. An implicit dependency requires the dependent application to be added in the security policy

C. An explicit dependency does not require the dependent application to be added in the security policy

D. An explicit dependency requires the dependent application to be added in the security policy

Answer: A,D

Explanation:

Question: 21

Recently changes were made to the firewall to optimize the policies and the security team wants to see if those changes are helping.

What is the quickest way to reset the hit counter to zero in all the security policy rules?

A. At the CLI enter the command reset rules and press Enter

B. Highlight a rule and use the Reset Rule Hit Counter > Selected Rules for each rule

C. Reboot the firewall

D. Use the Reset Rule Hit Counter > All Rules option

Answer: D

Explanation:

Reference:

Question: 22

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

A. facebook

B. facebook-chat

C. facebook-base

D. facebook-email

Answer: B,C

Explanation:

Question: 23

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

A. Windows-based agent deployed on the internal network

B. PAN-OS integrated agent deployed on the internal network

C. Citrix terminal server deployed on the internal network

D. Windows-based agent deployed on each of the WAN Links

Answer: A

Explanation:

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

Question: 24

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

Explanation:

Question: 25

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: B,D

Explanation:

Reference:

Question: 26

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

Explanation:

Question: 27

Identify the correct order to configure the PAN-OS integrated USER-ID agent.

3. add the service account to monitor the server(s)

2. define the address of the servers to be monitored on the firewall

4. commit the configuration, and verify agent connection status

1. create a service account on the Domain Controller with sufficient permissions to execute the UserID agent

A. 2-3-4-1

B. 1-4-3-2

C. 3-1-2-4

D. 1-3-2-4

Answer: D

Explanation:

Question: 28

Users from the internal zone need to be allowed to Telnet into a server in the DMZ zone.

Complete the security policy to ensure only Telnet is allowed.

Security Policy: Source Zone: Internal to DMZ Zone services "Application defaults", and action = Allow

A. Destination IP: 192.168.1.123/24

B. Application = 'Telnet'

C. Log Forwarding

D. USER-ID = 'Allow users in Trusted'

Answer: B

Explanation:

Question: 29

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:

Question: 30

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

A. Threat Prevention License

B. Threat Implementation License

C. Threat Environment License

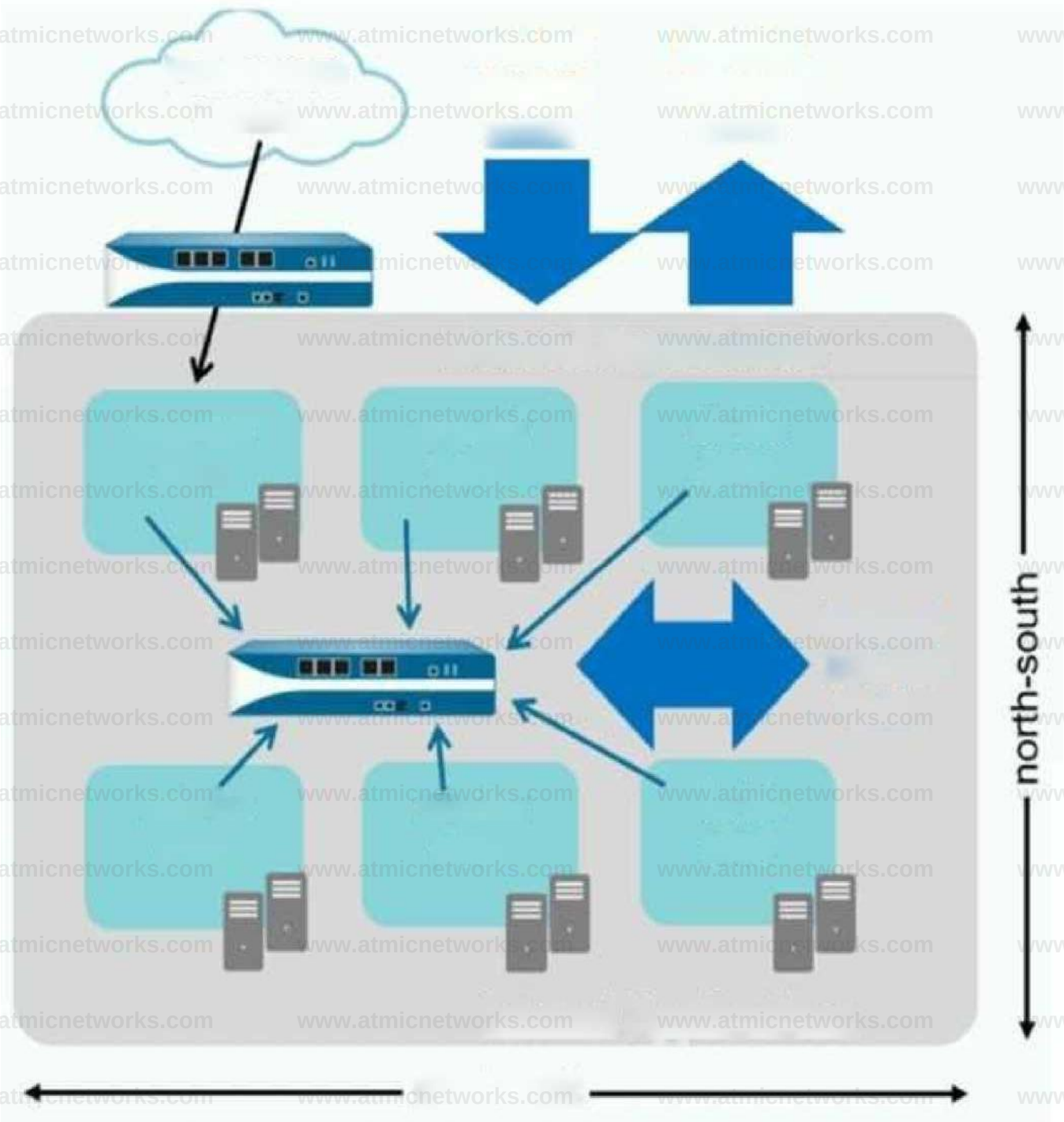
D. Threat Protection License

Answer: A

Explanation:

Question: 31

An administrator notices that protection is needed for traffic within the network due to malicious lateral movement activity. Based on the image shown, which traffic would the administrator need to monitor and block to mitigate the malicious activity?



A. branch office traffic

B. north-south traffic

C. perimeter traffic

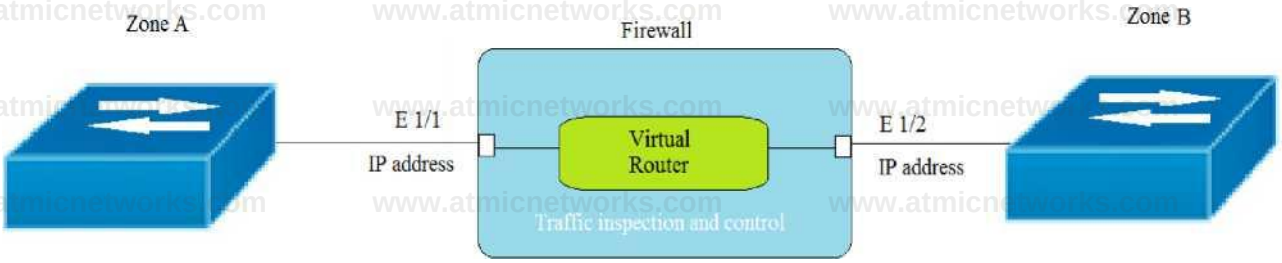
D. east-west traffic

Answer: D

Explanation:

Question: 32

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

Explanation:

Question: 33

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

Explanation:

Question: 34

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

Explanation:

Question: 35

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

A. Root

B. Dynamic

C. Role-based

D. Superuser

Answer: C

Explanation:

Question: 36

Which administrator type utilizes predefined roles for a local administrator account?

A. Superuser

B. Role-based

C. Dynamic

D. Device administrator

Answer: C

Explanation:

Reference:

Question: 37

Which two security profile types can be attached to a security policy? (Choose two.)

A. antivirus

B. DDoS protection

C. threat

D. vulnerability

Answer: A,D

Explanation:

Reference:

Question: 38

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:

Reference:

Question: 39

Which user mapping method could be used to discover user IDs in an environment with multiple Windows domain controllers?

A. Active Directory monitoring
B. Windows session monitoring
C. Windows client probing
D. domain controller monitoring

Answer: A

Explanation:

Question: 40

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: B,C,E

Explanation:

Question: 41

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

	Name	Tigs	Type	Zone	Address	User	HIP Profile	Zone	Address	Hit Count	Last Hit	First Hit	Application	Service	Action	Profile
)	Allow Office Programs	None	Universal	Inside	Any	Any	■Any	Outside	Any				Officeprogram	Application- d..	Allow	None
2	Allow FTP to web ser..	None	Universal	Inside	Any	Any	■Any	Outside	ftp. server				any	ftp-senice..	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: A,D

Explanation:

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

Question: 42

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:

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

Question: 43

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

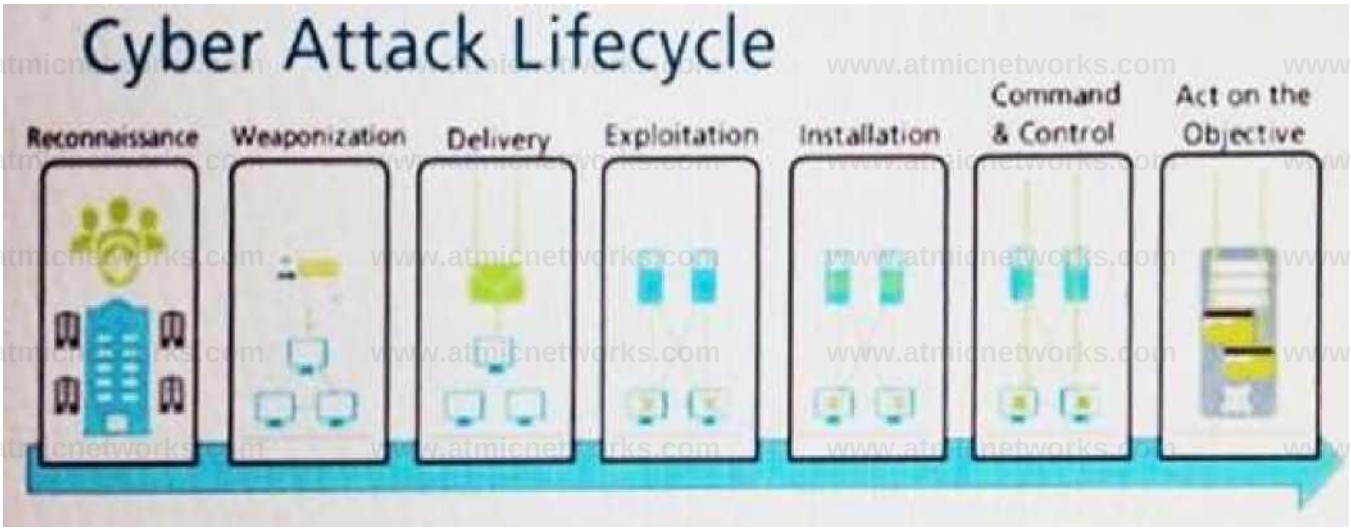
Answer: A

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.

Question: 45

Given the Cyber-Attack Lifecycle diagram, identify the stage in which the attacker can initiate malicious code against a targeted machine.



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

Answer: A

Explanation:

Question: 46

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

Explanation:

Question: 47

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: A,B

Explanation:

Question: 48

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: B,D

Explanation:

Question: 49

Which statement is true regarding a Prevention Posture Assessment?

A. The Security Policy Adoption Heatmap component filters the information by device groups, serial numbers, zones, areas of architecture, and other categories
B. It provides a set of questionnaires that help uncover security risk prevention gaps across all areas of network and security architecture
C. It provides a percentage of adoption for each assessment area
D. It performs over 200 security checks on Panorama/firewall for the assessment

Answer: B

Explanation:

Question: 50

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: A,C,D,E,F

Explanation:

Question: 51

The PowerBall Lottery has reached a high payout amount and a company has decided to help employee morale by allowing employees to check the number, but doesn't want to unblock the gambling URL category.

Which two methods will allow the employees to get to the PowerBall Lottery site without the company unlocking the gambling URL category? (Choose two.)

A. Add all the URLs from the gambling category except powerball.com to the block list and then set the action for the gambling category to allow.

B. Manually remove powerball.com from the gambling URL category.

C. Add *.powerball.com to the allow list

D. Create a custom URL category called PowerBall and add *.powerball.com to the category and set the action to allow.

Answer: C,D

Explanation:

Question: 52

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

Explanation:

Question: 53

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:

Question: 54

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

Explanation:

Question: 55

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 securityrule 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 created. 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

D. 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 the SSH-servers to reach the server-admin

Answer: B

Explanation:

Question: 56

How often does WildFire release dynamic updates?

A. every 5 minutes

B. every 15 minutes

C. every 60 minutes

D. every 30 minutes

Answer: A

Explanation:

Reference:

Question: 57

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.

Question: 58

A network has 10 domain controllers, multiple WAN links, and a network infrastructure with bandwidth needed to support mission-critical applications. Given the scenario, which type of User-ID agent is considered a best practice by Palo Alto Networks?

A. Windows-based agent on a domain controller

B. Captive Portal

C. Citrix terminal server with adequate data-plane resources

D. PAN-OS integrated agent

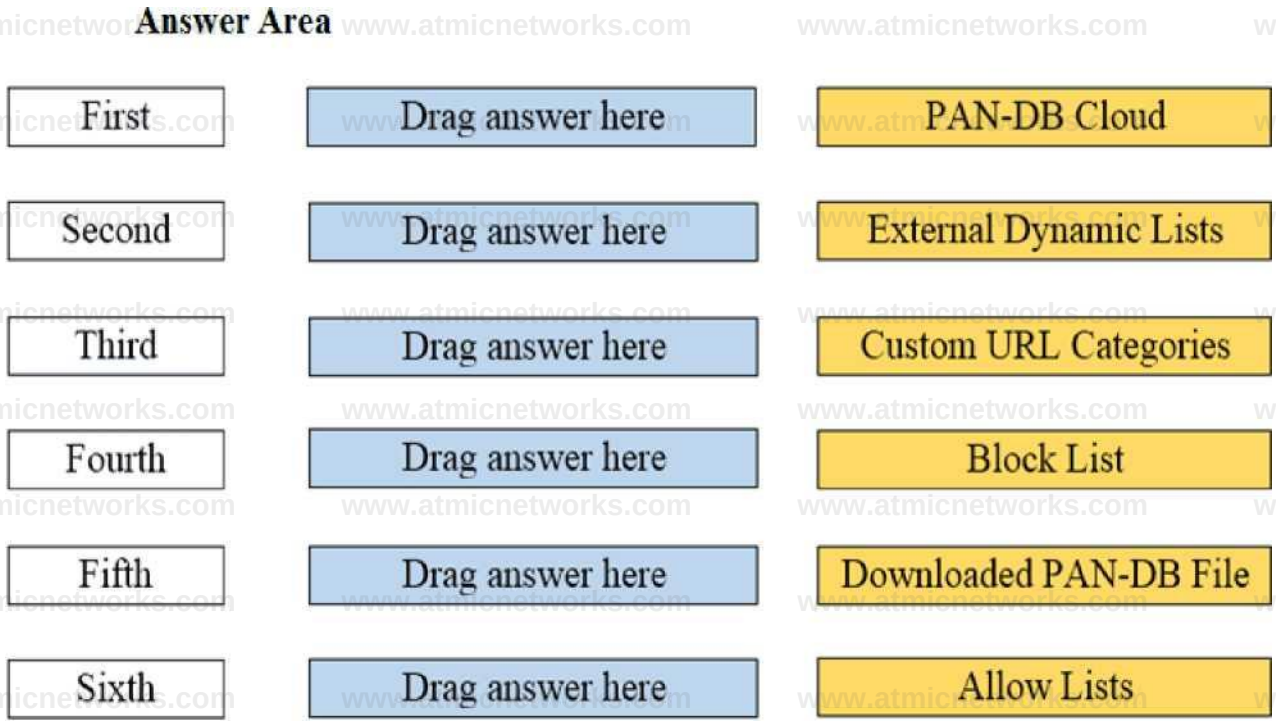
Answer: A

Explanation:

Question: 59

DRAG DROP

Arrange the correct order that the URL classifications are processed within the system.



Answer:

Explanation:

First – Block List
Second – Allow List
Third – Custom URL Categories
Fourth – External Dynamic Lists
Fifth – Downloaded PAN-DB Files
Sixth - PAN-DB Cloud

Question: 60

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

Explanation:

Reference:

Question: 61

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

Explanation:

Question: 62

Which interface type can use virtual routers and routing protocols?

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

Answer: B

Explanation:

Question: 63

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

Explanation:

Reference:

Answer: B

Question: 64

An internal host wants to connect to servers of the internet through using source NAT.

Which policy is required to enable source NAT on the firewall?

A. NAT policy with source zone and destination zone specified
B. post-NAT policy with external source and any destination address
C. NAT policy with no source of destination zone selected
D. pre-NAT policy with external source and any destination address

Answer: A

Explanation:

Question: 65

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

Explanation:

Question: 66

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

Question: 67

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: B,D

Explanation:

Question: 68

Which path is used to save and load a configuration with a Palo Alto Networks firewall?

A. Device>Setup>Services

B. Device>Setup>Management

C. Device>Setup>Operations

D. Device>Setup>Interfaces

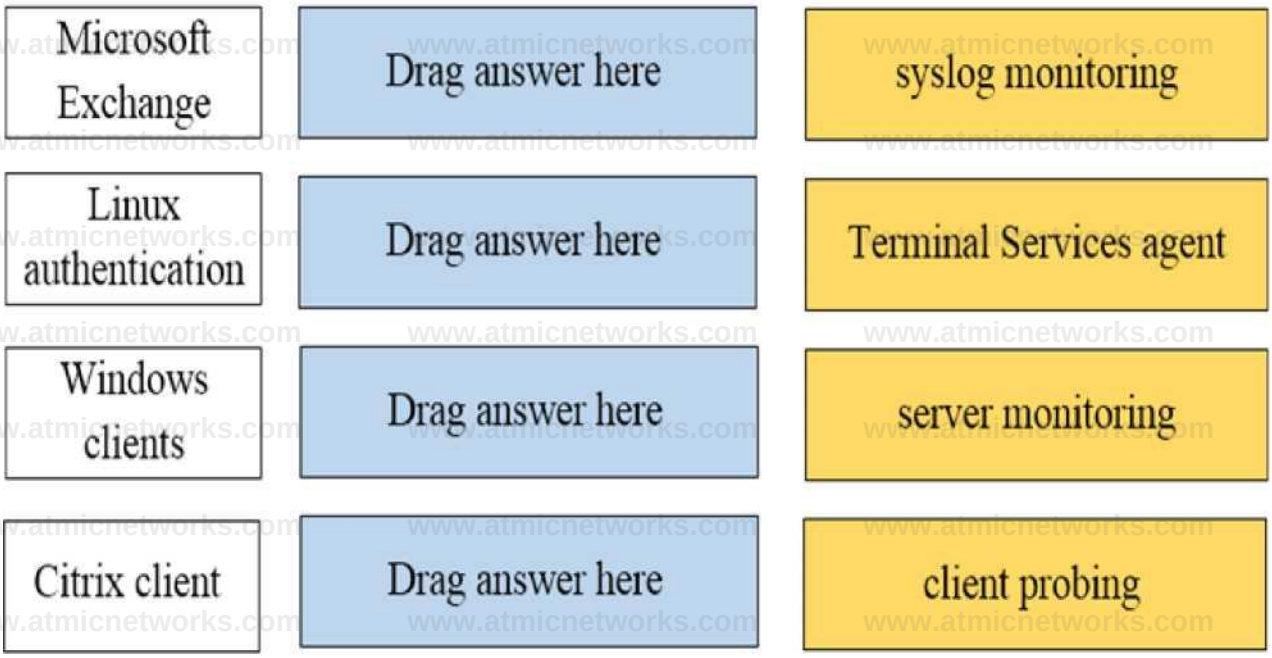
Answer: C

Question: 69

DRAG DROP

Match the network device with the correct User-ID technology.

Answer Area



Answer:

Explanation:

Microsoft Exchange – Server monitoring

Linux authentication – syslog monitoring

Windows Client – client probing

Citrix client – Terminal Services agent

Question: 70

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:

Reference:

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

Question: 71

How is the hit count reset on a rule?

A. select a security policy rule, right click Hit Count > Reset

B. with a dataplane reboot

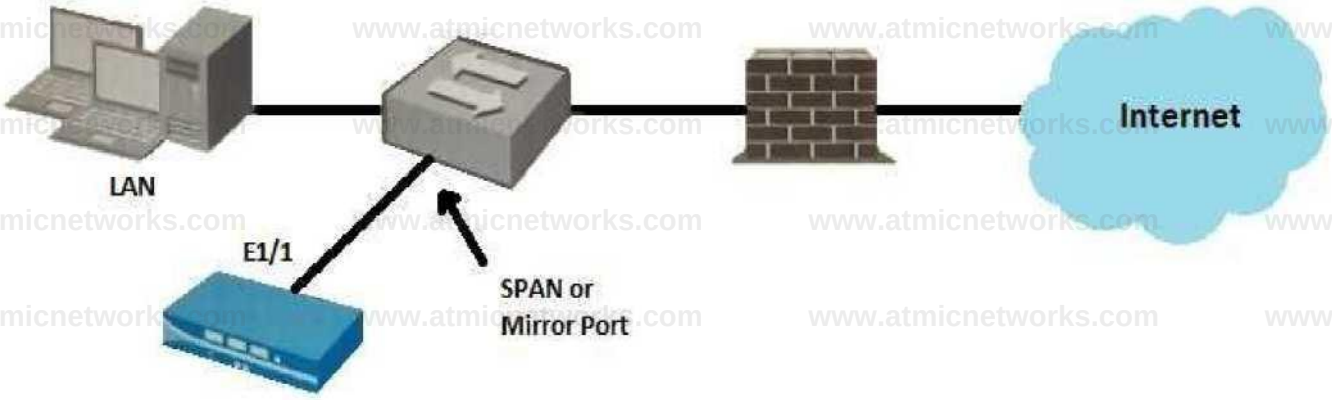
C. Device > Setup > Logging and Reporting Settings > Reset Hit Count

D. in the CLI, type command reset hitcount <POLICY-NAME>

Answer: A

Explanation:

Question: 72



Given the topology, which zone type should interface E1/1 be configured with?

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

Explanation:

Answer: A

Question: 73

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

Explanation:

Question: 74

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

Explanation:

Answer: B

Question: 75

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

	Name	Type	Zone	Address Zone	Address	Application	Service	Action
1	iiwde-poitsl	universal	ph| inside	any	m outside	^203 011:	J zu any	any	$ Allow
2	in!?ir3!*in5KiHInv	universal	pt inside	any	BSE	any	3 ftp 3 uh 3 ssl QwtUxnw'mg	• default
3	egress-outs xi*	universal	Pt inside	any	PU outside	any	any any	^f» aptM cation ■default 0 Abort
4	ogrca^ ^fSrae-Gonfenf id	unrrCf&l'	narde		outoide	any		app/GObon ■diefauf MD* f
5	canget-s rrulatec tratti;	universal	1 '** danger1	any	/ danger |	any	any	IP appiication- defauti ©Allow
6	i'll f 320 ^v<WadII $	intrazone	any	any	(intrazana)	any	wy	any © Allow
7	inltazone-defaili ^	intrazone	any	any	any	any	any	any Q Deny

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

Answer: B

Explanation:

Question: 76

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: B,D

Explanation:

Question: 77

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?

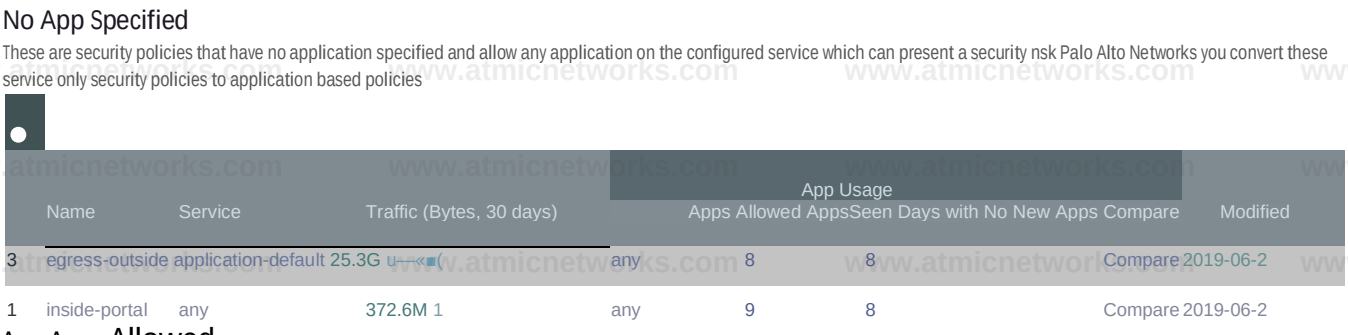
A. global
B. universal
C. intrazone
D. interzone

Answer: B

Explanation:

Question: 78

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

Explanation:

Question: 79

In a security policy what is the quickest way to rest all policy rule hit counters to zero?

A. Use the CLI enter the command reset rules all
B. Highlight each rule and use the Reset Rule Hit Counter > Selected Rules.
C. use the Reset Rule Hit Counter > All Rules option.
D. Reboot the firewall.

Answer: C

Explanation:

Question: 80

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:

WildFire	**Provides near real-time malware and antivirus signatures created as a result of the analysis done by the WildFire public cloud. WildFire signature updates are made available every five minutes. You can set the firewall to check for new updates as frequently as every minute to ensure that the firewall retrieves the latest WildFire signatures within a minute of availability. Without the WildFire subscription, you must wait at least 24 hours for the signatures to be provided in the Antivirus update.**

Question: 81

What do dynamic user groups you to do?

A. create a QoS policy that provides auto-remediation for anomalous user behavior and malicious activity
B. create a policy that provides auto-sizing for anomalous user behavior and malicious activity
C. create a policy that provides auto-remediation for anomalous user behavior and malicious activity
D. create a dynamic list of firewall administrators

Answer: C

Explanation:

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/user-id-features/dynamic-

user-

groups#:~:text=Dynamic%20user%20groups%20help%20you,activity%20while%20maintaining%20us er%20visibility.

Question: 82

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

Explanation:

Question: 83

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:

Explanation/Reference:

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

Question: 84

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

Question: 85

Which Palo Alto network security operating platform component provides consolidated policy creation and centralized management?

A. Prisma SaaS

B. Panorama

C. AutoFocus

D. GlobalProtect

Answer: B

Explanation:

Question: 86

Which type firewall configuration contains in-progress configuration changes?

A. backup

B. running

C. candidate

D. committed

Answer: C

Explanation:

Question: 87

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

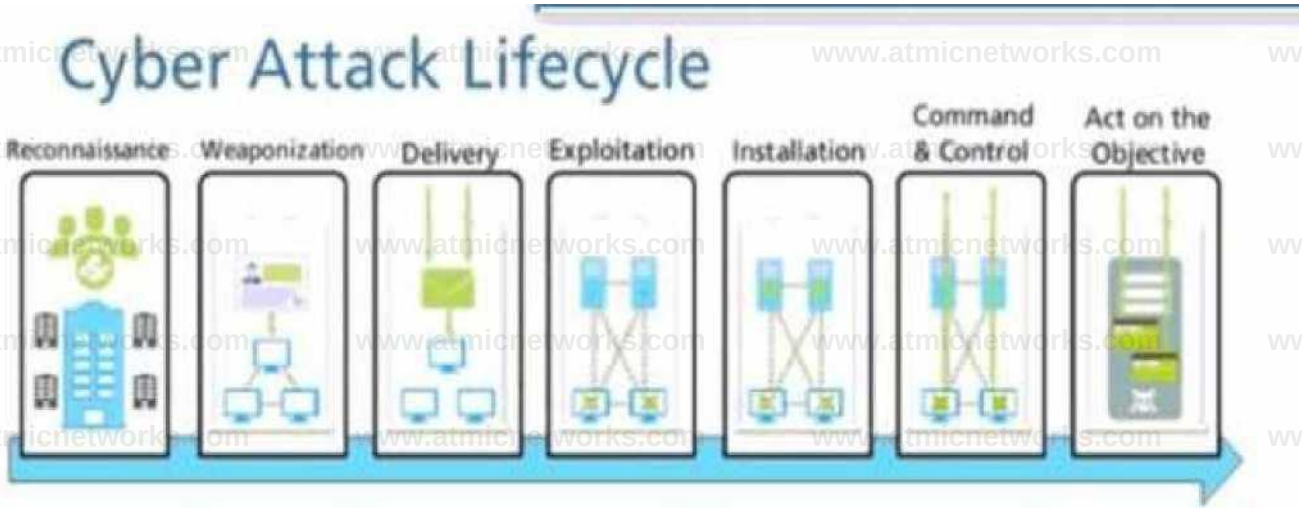
D. Review Policies

Answer: D

Explanation:

Question: 88

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



A. delivery

B. command and control

C. explotation

D. reinsurance

E. installation

Answer: A

Explanation:

Question: 89

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

Explanation:

Question: 90

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

Explanation:

Question: 91

How do you reset the hit count on a security policy rule?

A. First disable and then re-enable the rule.

B. Reboot the data-plane.

C. Select a Security policy rule, and then select Hit Count > Reset.

D. Type the CLI command reset hitcount <POLICY-NAME>.

Answer: C

Explanation:

Question: 92

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

A. SAML

B. RADIUS

C. TACACS+

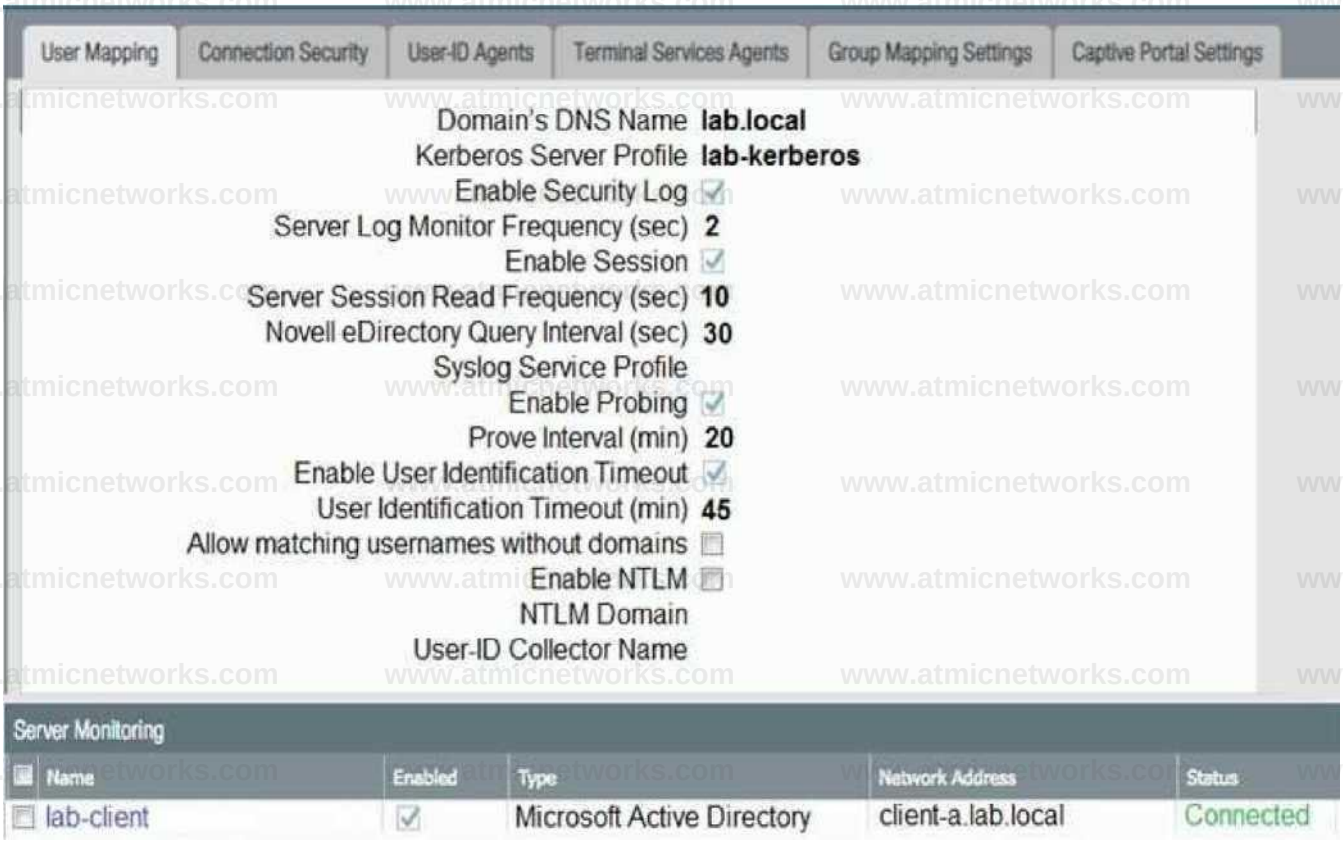
D. LDAP

Answer: D

Explanation:

Question: 93

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

Explanation:

Question: 94

Which three configuration settings are required on a Palo Alto networks firewall management interface?

A. default gateway

B. netmask

C. IP address

D. hostname

E. auto-negotiation

Answer: A,B,C

Explanation:

Explanation/Reference:

Reference:

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClN7CAK

Question: 95

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

Explanation:

Question: 96

Which statements is true regarding a Heatmap report?

A. When guided by authorized sales engineer, it helps determine te areas of greatest security risk.

B. It provides a percentage of adoption for each assessment area.

C. It runs only on firewall.

D. It provides a set of questionnaires that help uncover security risk prevention gaps across all areas of network and security architecture.

Answer: B

Explanation:

Reference: https://live.paloaltonetworks.com/t5/best-practice-assessment-blogs/the-best-practice- assessment-bpa-tool-for-ngfw-and-panorama/ba-p/248343

Question: 97

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

Explanation:

Question: 98

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: A,B

Explanation:

Question: 99

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: B,C,E

Explanation:

Question: 100

Based on the screenshot what is the purpose of the included groups?

	Name	Type	Zone	Address	User	Zone	Address	Application	Service	Action
1	allow-it	universal	R inside	any	^ it		any	it-tools	X application-default	& Allow

A. They are only groups visible based on the firewall's credentials.

B. They are used to map usernames to group names.

C. They contain only the users you allow to manage the firewall.

D. They are groups that are imported from RADIUS authentication servers.

Answer: B

Explanation:

Reference:

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/user-id/map-users-to-groups.html

Question: 101

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

Explanation:

Question: 102

Which operations are allowed when working with App-ID application tags?

A. Predefined tags may be deleted.

B. Predefined tags may be augmented by custom tags.

C. Predefined tags may be modified.

D. Predefined tags may be updated by WildFire dynamic updates.

Answer: B

Explanation:

Question: 103

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

Explanation:

Question: 104

In which profile should you configure the DNS Security feature?

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

Answer: B

Explanation:

Explanation/Reference:

Reference:

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

Question: 105

Access to which feature requires PAN-OS Filtering licens?

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

Answer: A

Explanation:

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

Question: 106

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

Explanation:

Question: 107

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

Question: 108

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

Question: 109

Four configuration choices are listed, and each could be used to block access to a specific URL. If you configured each choices to block the sameURL then which choice would be the last to block access to the URL?

A. EDL in URL Filtering Profile.
B. Custom URL category in Security Policy rule.
C. Custom URL category in URL Filtering Profile.
D. PAN-DB URL category in URL Filtering Profile.

Answer: D

Explanation:

The precedence is from the top down; First Match Wins: 1) Block list: Manually entered blocked URLs Objects - 2) Allow list: Manually entered allowed URLs Objects - 3) Custom URL Categories - 4) Cached Cached: URLs learned from External Dynamic Lists (EDLs) - 5) Pre-Defined Categories: PAN- DB or Brightcloud categories.

Question: 110

The CFO found a malware infected USB drive in the parking lot, which when inserted infected their corporate laptop the malware contacted a known command-and-control server which exfiltrating corporate data. Which Security profile feature could have been used to prevent the communications with the command-and-control server?

A. Create a Data Filtering Profile and enable its DNS sinkhole feature.
B. Create an Antivirus Profile and enable its DNS sinkhole feature.
C. Create an Anti-Spyware Profile and enable its DNS sinkhole feature.
D. Create a URL Filtering Profile and block the DNS sinkhole URL category.

Answer: C

Explanation:

Question: 111

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: A,D

Explanation:

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

Question: 112

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

Question: 113

Which action results in the firewall blocking network traffic with out notifying the sender?

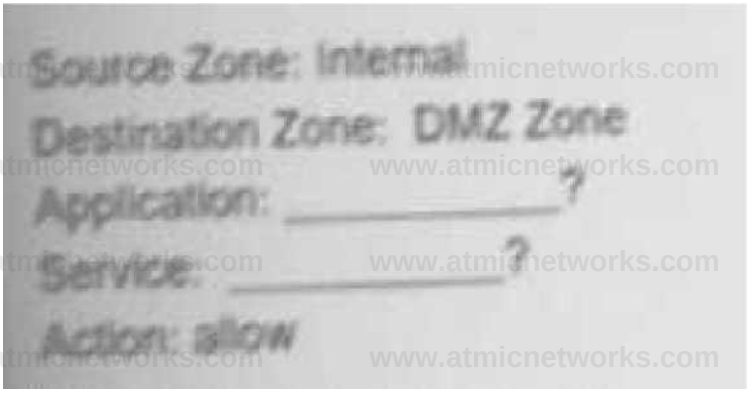
A. Drop
B. Deny
C. Reset Server
D. Reset Client

Explanation:

Answer: B

Question: 114

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



Choose two.

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

Answer: B,C

Explanation:

Question: 115

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

Question: 116

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: C,D

Explanation:

Question: 117

Which type of administrator account cannot be used to authenticate user traffic flowing through the firewall's

data plane?

A. Kerberos user

B. SAML user

C. local database user

D. local user

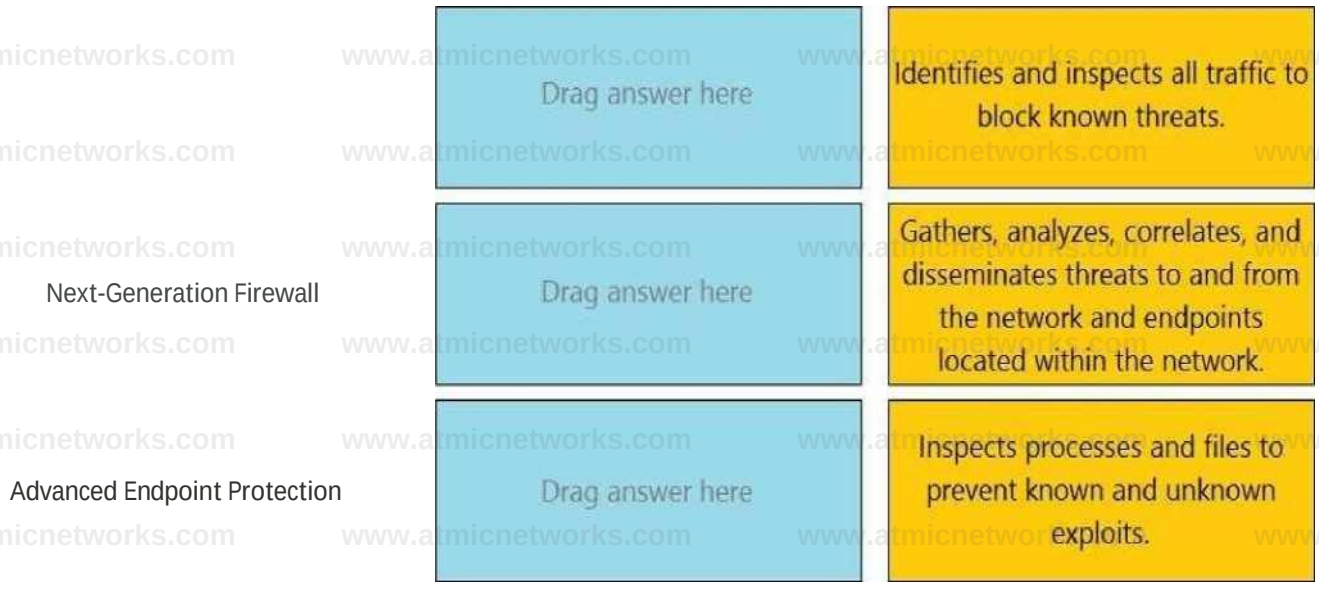
Explanation:

Answer: B

Question: 118

DRAG DROP

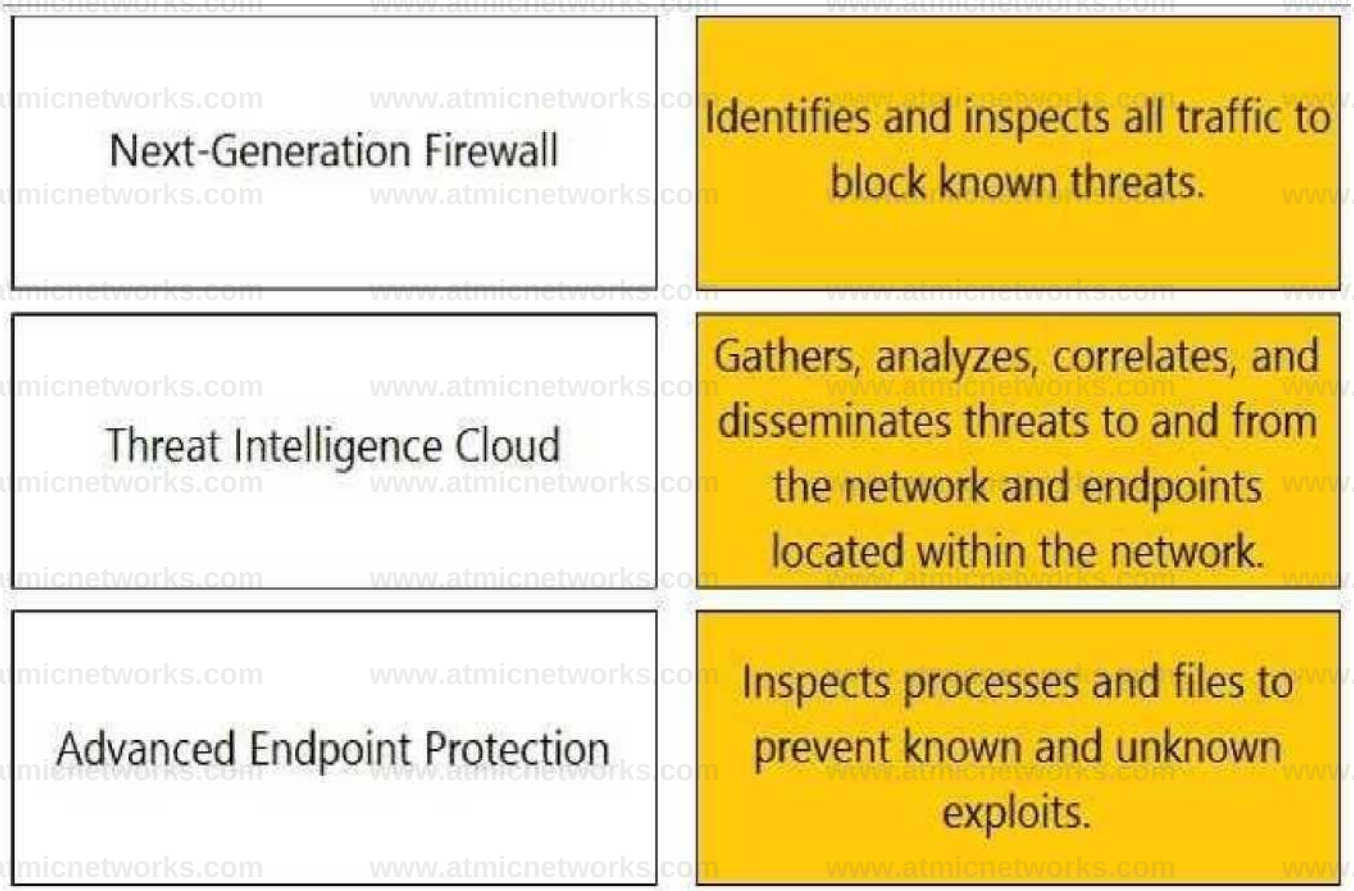
Match each feature to the DoS Protection Policy or the DoS Protection Profile.



Answer:

Explanation:

Threat Intelligence Cloud



Question: 119

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

Explanation:

Reference: https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/getting-started/activate-licenses-andsubscriptions.html

Question: 120

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?

A. Data Filtering Profile applied to outbound Security policy rules

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

Explanation:

Question: 121

Which Security profile can you apply to protect against malware such as worms and Trojans?

A. data filtering

B. antivirus

C. vulnerability protection

D. anti-spyware

Answer: B

Explanation:

Reference:

https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/security-profiles#:~:text=Antivirus%20profiles%20protect%20against%20viruses,as%20well%20as%20spyware%20downloads

Question: 122

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: A,C

Explanation:

Question: 123

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

Explanation:

Explanation/Reference:

Reference:

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

Question: 124

An administrator would like to override the default deny action for a given application and instead would like to block the traffic and send the ICMP code "communication with the destination is administratively prohibited"

Which security policy action causes this?

A. Drop

B. Drop, send ICMP Unreachable

C. Reset both

D. Reset server

Answer: B

Explanation:

Question: 125

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

Explanation:

Question: 126

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

A. interzone

B. intrazone

C. universal

D. shadowed

Answer: A,C

Explanation:

Question: 127

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

Explanation:

Explanation

Explanation/Reference:

Reference:

https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/administer-panorama/manage- locks-forrestricting-configuration-changes.html

Question: 128

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

A. Doing so limits the templates that receive the policy rules

B. Doing so provides audit information prior to making changes for selected policy rules

C. You can specify the firewalls m a device group to which to push policy rules

D. You specify the location as pre can - or post-rules to push policy rules

Answer: C

Explanation:

Question: 129

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

Explanation:

Question: 130

What is the correct process tor creating a custom URL category?

A. Objects > Security Profiles > URL Category > Add
B. Objects > Custom Objects > URL Filtering > Add
C. Objects > Security Profiles > URL Filtering > Add
D. Objects > Custom Objects > URL Category > Add

Answer: D

Explanation:

Question: 131

Which tab would an administrator click to create an address object?

A. Device

B. Policies

C. Monitor

D. Objects

Answer: D

Explanation:

Question: 132

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

Explanation:

Question: 133

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:

Question: 134

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

Explanation:

Question: 135

DRAG DROP

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

Answer:

Explanation:

Answer Area

installation	stage where the attacker scans for network vi exploited
Command and control	stage where the attacker will explore methodi persistence
	stage where the attacker has access to a spe and pass data lo and from infected devices w

Question: 136

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

Explanation:

Question: 137

Which objects would be useful for combining several services that are often defined together?

A. shared service objects

B. service groups

C. application groups

D. application filters

Answer: B

Explanation:

Reference:

https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface-help/objects/objects- services.html

Question: 138

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

Explanation:

Question: 139

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

Explanation:

Question: 140

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

Explanation:

Question: 141

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

Explanation:

Question: 142

An administrator wishes to follow best practices for logging traffic that traverses the firewall

Which log setting is correct?

A. Disable all logging

B. Enable Log at Session End

C. Enable Log at Session Start

D. Enable Log at both Session Start and End

Answer: B

Explanation:

Explanation

Explanation/Reference:

Reference:

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

Question: 143

Assume that traffic matches a Security policy rule but the attached Security Profiles is configured to block matching traffic

Which statement accurately describes how the firewall will apply an action to matching traffic?

A. If it is an allowed rule, then the Security Profile action is applied last

B. If it is a block rule then the Security policy rule action is applied last

C. If it is an allow rule then the Security policy rule is applied last

D. If it is a block rule then Security Profile action is applied last

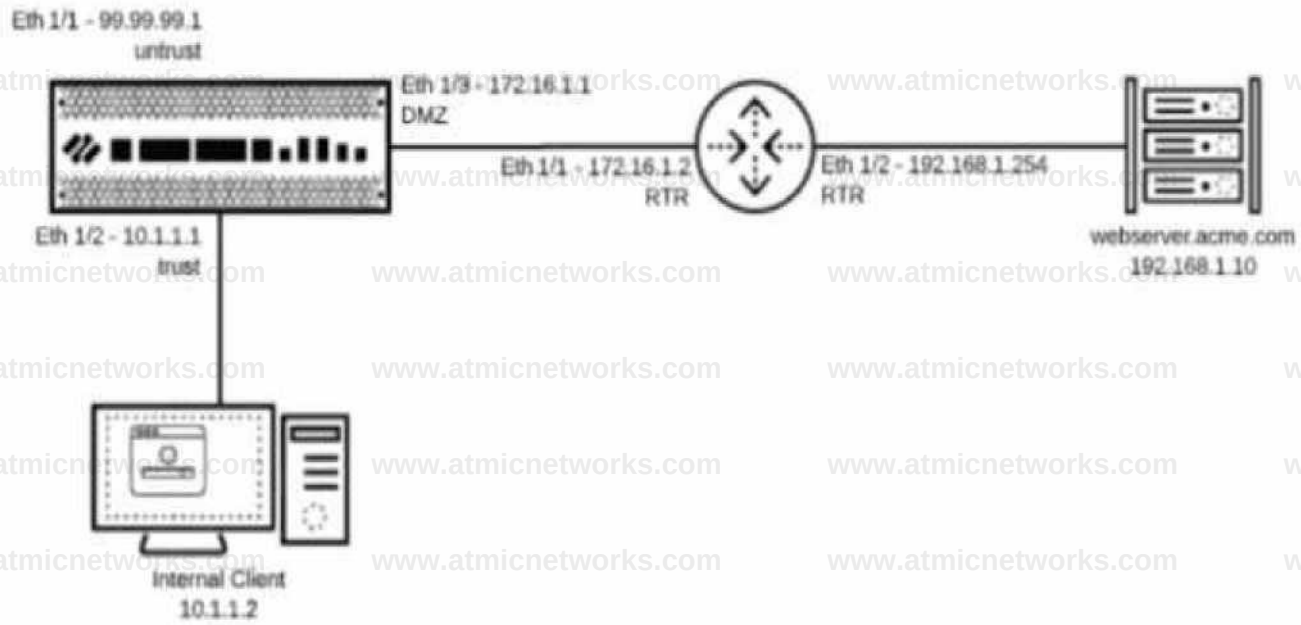
Answer: A

Explanation:

Question: 144

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

Explanation:

Question: 145

An administrator wants to prevent access to media content websites that are risky

Which two URL categories should be combined in a custom URL category to accomplish this goal? (Choose two)

A. streaming-media

B. high-risk

C. recreation-and-hobbies

D. known-risk

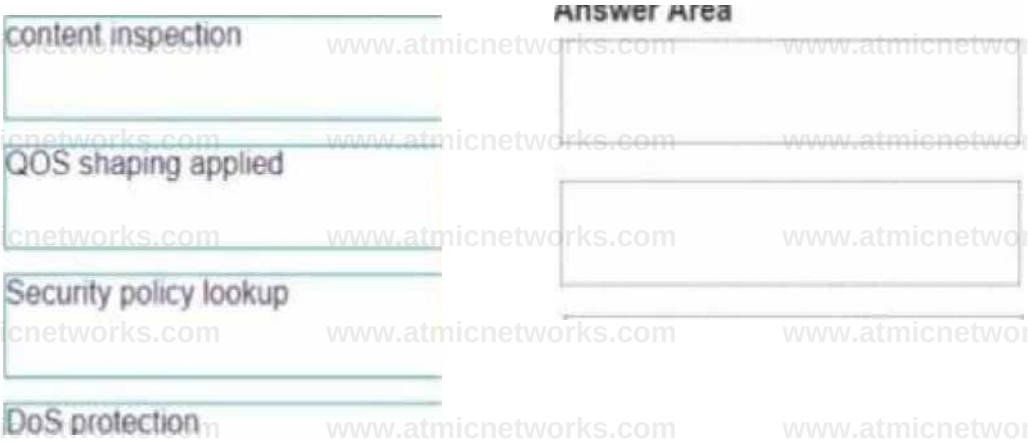
Answer: A,C

Explanation:

Question: 146

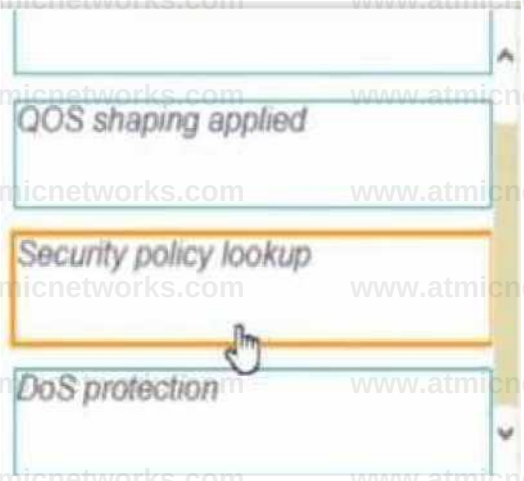
DRAG DROP

Place the following steps in the packet processing order of operations from first to last.



Answer:

Explanation:



Answer Area jwuttiy
pvitiy nxmup

content inspection

QOS shaping applied

third

four

tt

Question: 147

A Security Profile can block or allow traffic at which point?

A. after it is matched to a Security policy rule that allows traffic

B. on either the data plane or the management plane

C. after it is matched to a Security policy rule that allows or blocks traffic

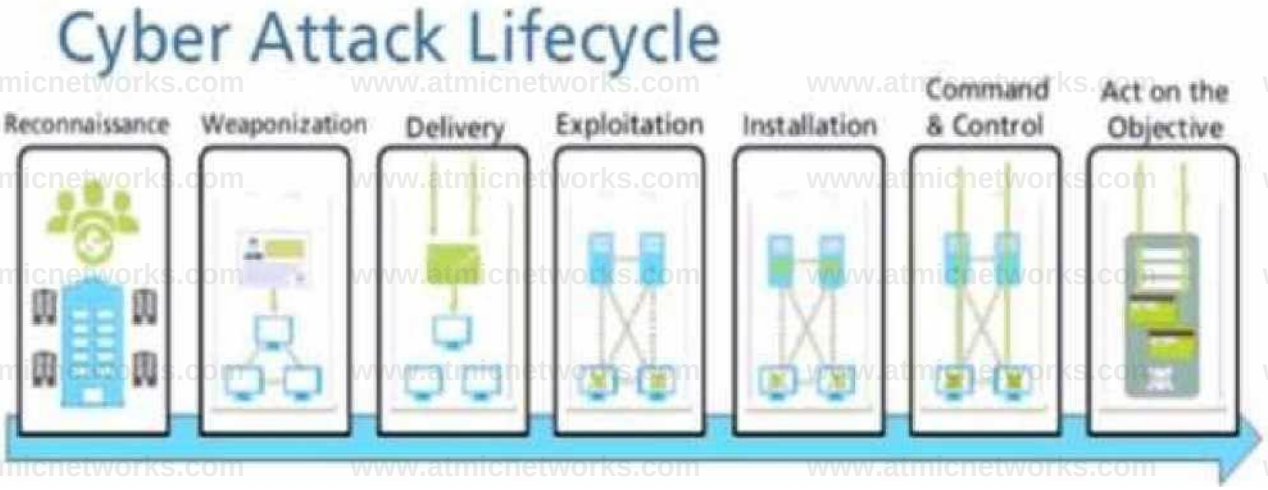
D. before it is matched to a Security policy rule

Answer: A

Explanation:

Question: 148

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



A. Exploitation

B. Installation

C. Reconnaissance

D. Act on the Objective

Answer: A

Explanation:

Question: 149

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

Explanation:

Question: 150

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: A,B,D

Explanation:

Question: 151

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 0000/0 v

Interface ethcrnctl/1 v

Next Hop IP Address

10.46.172.1

Admin Distance 10 ■ 240

Metric 10

Route Table Unicast BFD Profile Disable BFD v

I J Path Monitoring

1 NAME ENABLE SOURCE IP IP INTERVALISEC) PING COUNT

A. default route

B. OSPF

C. BGP

D. static route

Answer: A

Explanation:

Question: 152

Based on the screenshot what is the purpose of the group in User labelled "it"

A. Allows users to access IT applications on all ports

B. Allows users in group "DMZ" lo access IT applications

C. Allows "any" users to access servers in the DMZ zone

D. Allows users in group "it" to access IT applications

Answer: D

Explanation:

Question: 153

Which dynamic update type includes updated anti-spyware signatures?

A. Applications and Threats

B. GlobalProtect Data File

C. Antivirus

D. PAN-DB

Answer: A

Explanation:

Question: 154

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

A. override

B. allow

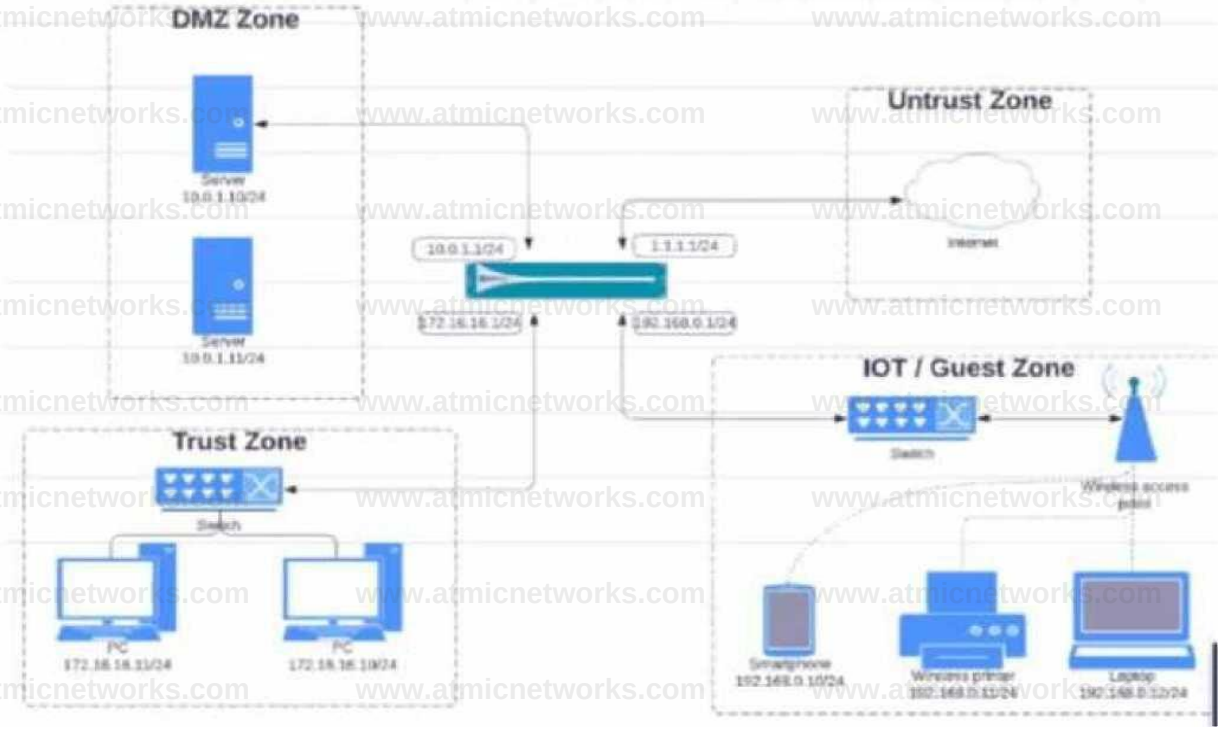
C. block

D. continue

Answer: B

Explanation:

Question: 155

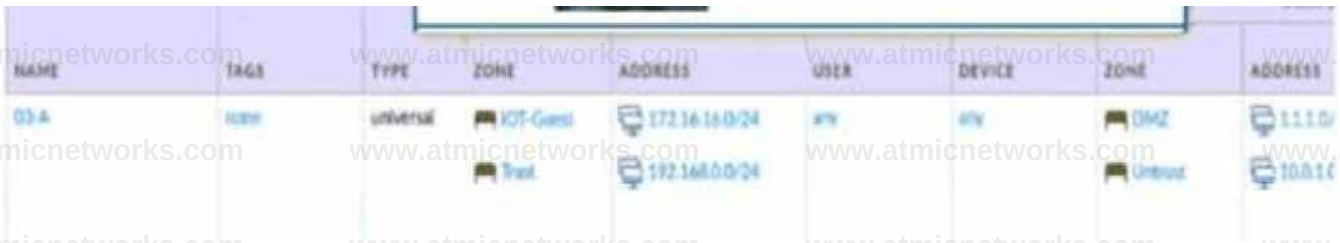


Given the network diagram, traffic should be permitted for both Trusted and Guest users to access general Internet and DMZ servers using SSH. web-browsing and SSL applications

Which policy achieves the desired results?

A)

B)



C)

NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS
G2-A	none	universal	IOT-Guest	172.16.18.0/24	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
G1-A	none	universal	IOT-Guest	10.0.10/24	any	any	DMZ	3.3.18/
			Trust	172.16.16.0/12			Untrust	192.168

A. Option

B. Option

C. Option

D. Option

Answer: C

Explanation:

Question: 156

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

Explanation:

Question: 157

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

Explanation:

Reference: https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface- help/objects/objects-security-profiles-vulnerability-protection.html

Vulnerability Protection Security Profiles protect against threats entering the network. For example, Vulnerability Protection Security Profiles protect against buffer overflows, illegal code execution, and other attempts to exploit system vulnerabilities. The default Vulnerability Protection Security Profile protects clients and servers from all known critical-, high-, and medium-severity threats. You also can create exceptions that enable you to change the response to a specific signature.

Question: 158

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

Explanation:

Question: 159

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:

Explanation/Reference:

Reference:

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

Question: 160

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

Explanation:

Question: 161

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

Explanation:

Question: 162

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

Explanation:

Question: 163

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

A. URL traffic

B. vulnerability protection

C. anti-spyware

D. antivirus

Answer: C

Explanation:

Question: 164

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: B,C

Explanation:

Explanation

Explanation/Reference:

Reference:

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

Question: 165

What is the main function of Policy Optimizer?

A. reduce load on the management plane by highlighting combinable security rules

B. migrate other firewall vendors' security rules to Palo Alto Networks configuration

C. eliminate "Log at Session Start" security rules

D. convert port-based security rules to application-based security rules

Answer: D

Explanation:

Explanation/Reference:

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

Question: 166

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

Explanation:

Question: 167

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

Question: 168

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

Explanation:

Question: 169

What must be considered with regards to content updates deployed from Panorama?

A. Content update schedulers need to be configured separately per device group.

B. Panorama can only install up to five content versions of the same type for potential rollback scenarios.

C. A PAN-OS upgrade resets all scheduler configurations for content updates.

D. Panorama can only download one content update at a time for content updates of the same type.

Answer: D

Explanation:

Reference: https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/manage-licenses- and-updates/deploy-updates-to-firewalls-log-collectors-and-wildfire-appliances-using- panorama/schedule-a-content-update-using-panorama.html

Question: 170

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

A. pattern based application identification

B. application override policy match

C. session application identified

D. application changed from content inspection

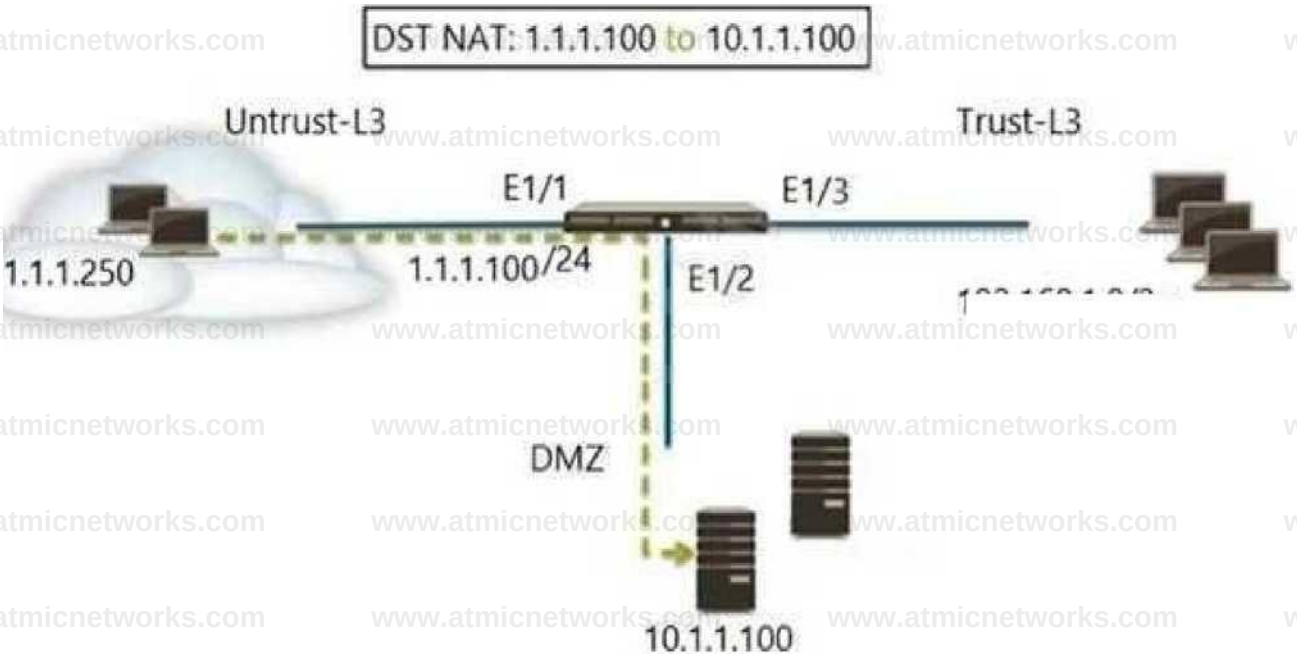
Answer: A,B

Explanation:

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

Question: 171

Refer to the exhibit. A web server in the DMZ is being mapped to a public address through DNAT.



Which Security policy rule will allow traffic to flow to the web server?
A. Untrust (any) to DMZ (10.1.1.100), web browsing -Allow
B. Untrust (any) to Untrust (1.1.1.100), web browsing - Allow
C. Untrust (any) to Untrust (10.1.1.100), web browsing -Allow
D. Untrust (any) to DMZ (1.1.1.100), web browsing - Allow

Answer: D

Explanation:

Reference: https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/networking/nat/nat-configuration-examples/destination-nat-exampleone-to-one-mapping

Question: 172

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=kA10g000000CIQSCA0

Question: 173

What is the purpose of the automated commit recovery feature?

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

Answer: C

Explanation:

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

Question: 174

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

Question: 175

DRAG DROP

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

Answer:

Explanation:

Answer Area

zone protection	first
decryption	second
Security profile enforcement	third
App-ID	fourth

Reference:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIVHCA0

Question: 176

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

Explanation:

Answer: B

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

Question: 177

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

A. authentication

B. decryptionC application override

C. NAT

Answer: A,B

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

Question: 178

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

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

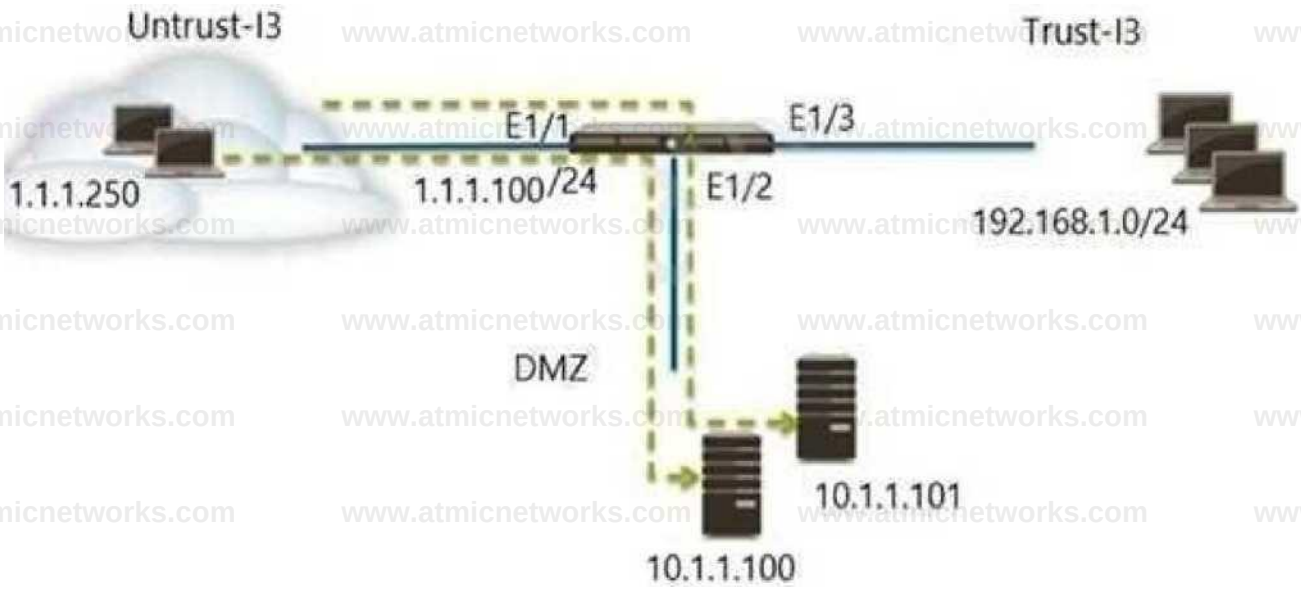
Explanation:

Question: 179

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.

DST NAT: 1.1.1.100 10.1.1.100 Dst Port 80

1.1.1.100 10.1.1,101 Dst Port 22



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: A,E

Explanation:

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 Status window

B. on the Policy Optimizer's Rule Usage page

C. on the Application tab in the Security Policy Rule creation window

D. on the Objects > Applications browser pages

Answer: A,C

Explanation:

Reference: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/app-id/use-application- objects-in-policy/resolve-application-dependencies.html

Question: 181

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

Explanation:

Reference: https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface- help/device/device-response-pages.html

Question: 182

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

Explanation:

Reference: https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/manage-licenses- and-updates/deploy-updates-to-firewalls-log-collectors-and-wildfire-appliances-using- panorama/schedule-a-content-update-using-panorama.html

Question: 183

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

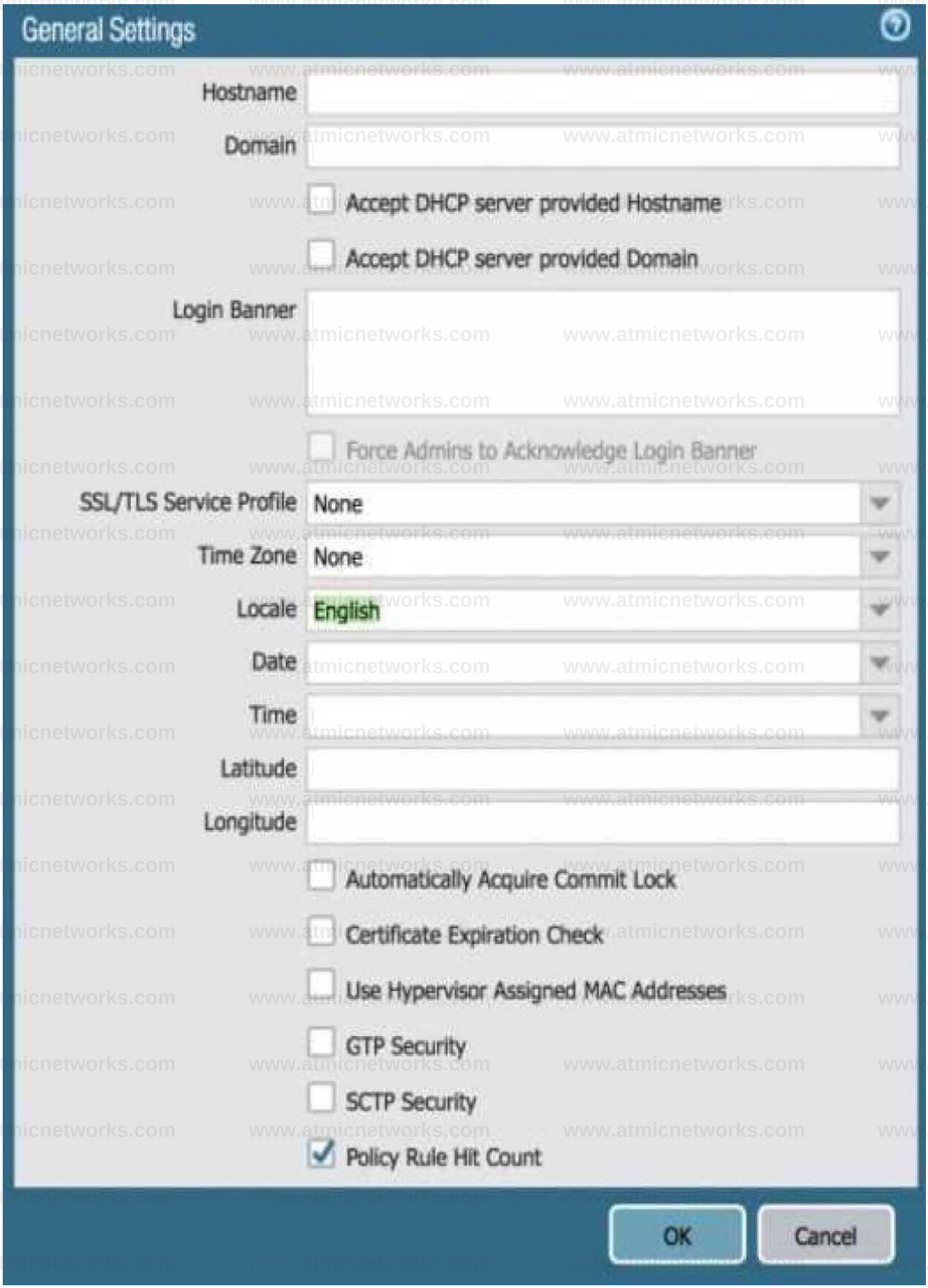
Answer: D

Explanation:

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

Question: 184

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



A. It defines the SSUTLS encryption strength used to protect the management interface.

B. It defines the CA certificate used to verify the client's browser.

C. It defines the certificate to send to the client's browser from the management interface.

D. It defines the firewall's global SSL/TLS timeout values.

Answer: C

Explanation:

Reference:

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClFGCA0

Question: 185

An administrator is troubleshooting an issue with traffic that matches the intrazone-default rule, which is set to default configuration.

What should the administrator do?

A. change the logging action on the rule

B. review the System Log

C. refresh the Traffic Log

D. tune your Traffic Log filter to include the dates

Answer: A

Explanation:

Question: 186

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

Explanation:

Reference:

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClVHCA0

Question: 187

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

A. check now

B. review policies

C. test policy match

D. download

Answer: B

Explanation:

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

Question: 188

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

Question: 189

When HTTPS for management and GlobalProtect are enabled on the same interface, which TCP port is used for management access?

A. 80

B. 8443

C. 4443

D. 443

Answer: C

Explanation:

Reference:

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Cm8SCAS#:~:text=

Details,using%20https%20on%20port%204443

Question: 190

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: A,B

Explanation:

Reference: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/firewall- administration/manage-firewall-administrators/administrative-authentication.html

The administrative accounts are defined on an external SAML, TACACS+, or RADIUS server. The server performs both authentication and authorization. For authorization, you define Vendor-Specific Attributes (VSAs) on the TACACS+ or RADIUS server, or SAML attributes on the SAML server. PAN-OS maps the attributes to administrator roles, access domains, user groups, and virtual systems that you define on the firewall.

Question: 191

Choose the option that correctly completes this statement. A Security Profile can block or allow traffic .

A. on either the data place or the management plane.

B. after it is matched by a security policy rule that allows traffic.

C. before it is matched to a Security policy rule.

D. after it is matched by a security policy rule that allows or blocks traffic.

Answer: B

Explanation:

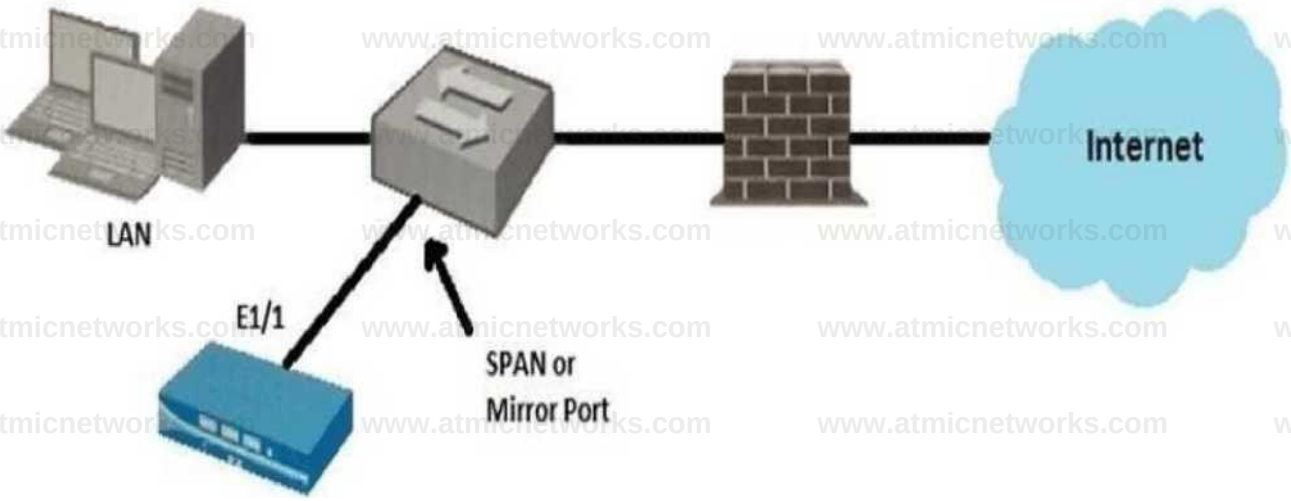
Explanation/Reference:

Reference:

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

After a packet has been allowed by the Security policy, Security Profiles are used to scan packets for threats, vulnerabilities, viruses, spyware, malicious URLs, data exfiltration, and exploitation software.

Question: 192



Given the topology, which zone type should you configure for firewall interface E1/1?

A. Tap

B. Tunnel

C. Virtual Wire

D. Layer3

Answer: A

Explanation:

Question: 193

For the firewall to use Active Directory to authenticate users, which Server Profile is required in the Authentication Profile?

A. TACACS+

B. RADIUS

C. LDAP

D. SAML

Answer: C

Explanation:

Explanation/Reference:

Reference:

https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/authentication/configure-an-authenticationprofile-and-sequence

Question: 194

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

Question: 195

Which license is required to use the Palo Alto Networks built-in IP address EDLs?

A. DNS Security

B. Threat Prevention

C. WildFire

D. SD-Wan

Answer: B

Explanation:

Explanation/Reference:

Reference:

https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/use-an-external-dynamic-list-in- policy/builtin-edls.html#:~:text=With%20an%

Question: 196

Which component is a building block in a Security policy rule?

A. decryption profile

B. destination interface

C. timeout (min)

D. application

Answer: D

Explanation:

Explanation/Reference:

Reference:

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

Question: 197

An administrator would like to use App-ID's deny action for an application and would like that action updated with dynamic updates as new content becomes available.

Which security policy action causes this?

A. Reset server

B. Reset both

C. Deny

D. Drop

Answer: C

Explanation:

Explanation/Reference:

Reference:

https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/firewall-administration/manage- configuration backups/revert-firewall-configuration- changes.html

Question: 198

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

Question: 199

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

Question: 200

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: A,B,C

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

Question: 201

Which action would an administrator take to ensure that a service object will be available only to the selected device group?

A. create the service object in the specific template

B. uncheck the shared option

C. ensure that disable override is selected

D. ensure that disable override is cleared

Answer: D

Explanation:

https://docs.paloaltonetworks.com/panorama/9-0/panorama-admin/manage-firewalls/manage- device-groups/create-objects-for-use-in-shared-or-device-group-policy

Question: 202

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

Question: 203

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, HTTP. 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.

Question: 204

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-bulletproof-isps#:~:text=A%20new%20built%2Din%20external,%2C%20illegal%2C%20and%20unethical%20cont ent.

Question: 205

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

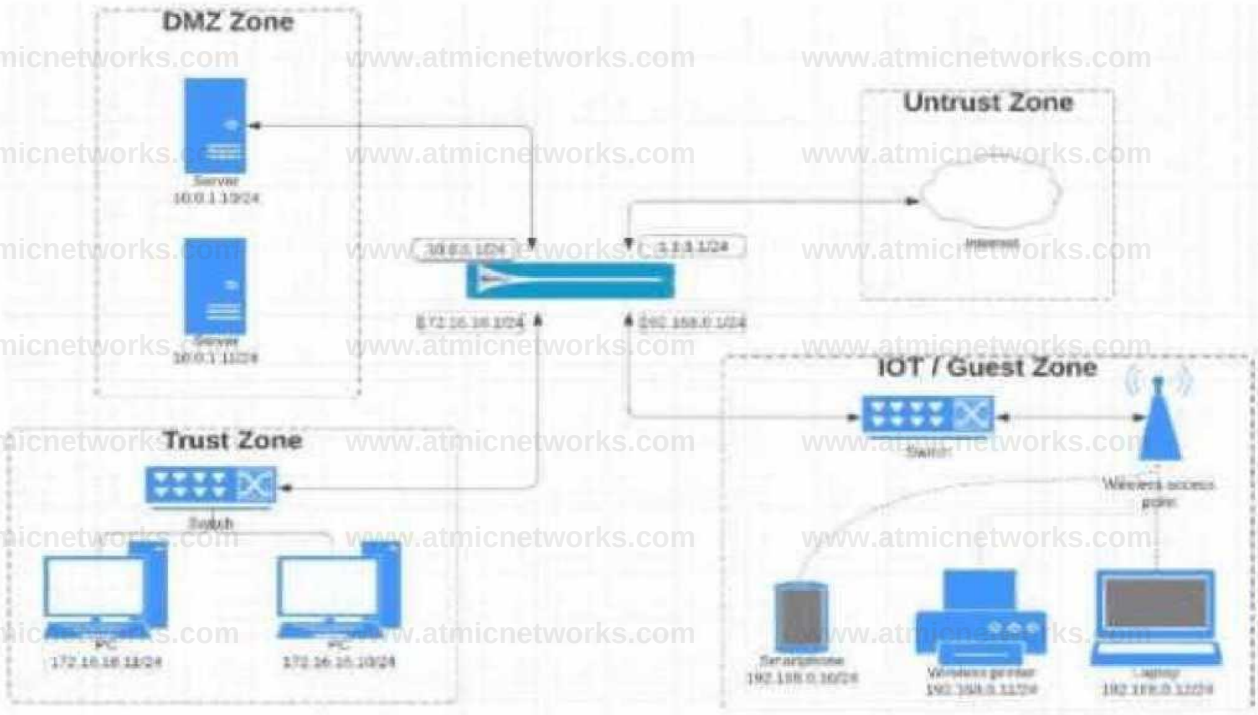
Explanation:

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

Question: 206

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)

ADMIM	UM*	on«t	TOM	A DOM II	MUM a	AWtKAIIOAi	MtWICI	uai r AMGoar	AC MO A
Quu. ^WM	MOM «w MM*		Row R	610015.74	wr	S «<D y .wHira	><RXM>RA*		0AAw

B)

ADMIM	UM*	MVtCI	COM	MV<I	AWKAYIOM	MWXI	um CAYMOOV	ACT KIM
Quan	AW	ROW			□ ^			0 ***••
§'»»		RIWm	QmtMO^M					

C)

ADOaili	UM*	MV1CI	TOM	MKMU>	MVKt	AWUCATIO*	UBVIC1	UAL CAHCOar	ACMOM
^nn*	£0/M	AW	ROW Rwra			U R a<R*~Ri	JtaaftaavaaW		Q AHA*

D)

A. Option A

B. Option B

C. Option C

D. Option D

Answer: C

Explanation:

Question: 207

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

Explanation:

Question: 208

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

Explanation:

Question: 209

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.

Question: 210

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 Threat Intelligence with Palo Alto Networks). Attackers use these IP addresses almost exclusively to distribute malware, initiate command-and-control activity, and launch attacks.

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

Question: 211

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: A,D

Explanation:

Question: 212

What must be configured before setting up Credential Phishing Prevention?

A. Anti Phishing Block Page

B. Threat Prevention

C. Anti Phishing profiles

D. User-ID

Answer: B

Explanation:

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/threat-prevention/prevent- credential-phishing/set-up-credential-phishing-prevention

Question: 213

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

Question: 214

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

Explanation:

Question: 215

An address object of type IP Wildcard Mask can be referenced in which part of the configuration?

A. Security policy rule

B. ACC global filter

C. external dynamic list

D. NAT address pool

Answer: A

Explanation:

You can use an address object of type IP Wildcard Mask only in a Security policy rule.

https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/objects/objects- addresses

IP Wildcard Mask

—Enter an IP wildcard address in the format of an IPv4 address followed by a slash and a mask (which must begin with a zero); for example, 10.182.1.1/0.127.248.0. In the wildcard mask, a zero (0) bit indicates that the bit being compared must match the bit in the IP address that is covered by the 0. A one (1) bit in the mask is a wildcard bit, meaning the bit being compared need not match the bit in the IP address that is covered by the 1. Convert the IP address and the wildcard mask to binary. To illustrate the matching: on binary snippet 0011, a wildcard mask of 1010 results in four matches (0001, 0011, 1001, and 1011).

Question: 216

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:

Question: 217

An administrator needs to create a Security policy rule that matches DNS traffic within the LAN zone, and also needs to match DNS traffic within the DMZ zone The administrator does not want to allow traffic between the DMZ and LAN zones.

Which Security policy rule type should they use?

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

Explanation:

Answer: C

Question: 218

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: A,C,D

Explanation:

Palo Alto Networks firewalls can map IP addresses to usernames using various methods, such as User-ID agents, Captive Portal, GlobalProtect, XML API, and HTTP headers. These methods allow the firewall to enforce security policies based on user identity, rather than just IP address. Some of these methods are:

Using the XML API: The XML API allows external systems to send user mapping information to the firewall using HTTPS requests. The firewall can then use this information to identify the users behind the IP addresses and apply the appropriate policies1.

A user connecting into a GlobalProtect gateway using a GlobalProtect Agent: GlobalProtect provides secure remote access to the network by establishing a VPN tunnel between the user's device and the firewall. When a user connects to a GlobalProtect gateway using a GlobalProtect agent, the firewall can authenticate the user and map the user's IP address to the username1.

Usernames inserted inside HTTP Headers: The firewall can also extract usernames from HTTP headers in web traffic. This method requires the web server or proxy server to insert the username into a custom HTTP header that the firewall can read. The firewall can then use this information to map the IP address to the username1.

Reference: Map IP Addresses to Users, Certifications - Palo Alto Networks, Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0) or Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0).

Question: 219

Which object would an administrator create to enable access to all applications in the officeprograms subcategory?

A. application filter

B. URL category

C. HIP profile

D. application group

Answer: A

Explanation:

Question: 220

An administrator would like to create a URL Filtering log entry when users browse to any gambling website. What combination of Security policy and Security profile actions is correct?

A. Security policy = drop, Gambling category in URL profile = allow

B. Security policy = deny. Gambling category in URL profile = block

C. Security policy = allow, Gambling category in URL profile = alert

D. Security policy = allow. Gambling category in URL profile = allow

Answer: C

Explanation:

Question: 221

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-overview

Question: 222

After making multiple changes to the candidate configuration of a firewall, the administrator would like to start over with a candidate configuration that matches the running configuration.

Which command in Device > Setup > Operations would provide the most operationally efficient way to accomplish this?

A. Import named config snapshot

B. Load named configuration snapshot

C. Revert to running configuration

D. Revert to last saved configuration

Answer: C

Explanation:

Question: 223

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:

Question: 224

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: A,B

Explanation:

Question: 225

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

A. deny

B. drop

C. default

D. block-ip

Answer: B,C

Explanation:

Question: 226

DRAG DROP

Match each rule type with its example

Create a policy with source zones A and S The rule will apph all traffic within zone A and all traffic within zone B. but not to traffic between zones A and B

Create a policy with source zones A and B and destination zc A and B The rule should apply to all traffic within zone A. all t within zone B. all traffic from zone A to zone B. and all traffic t zone B to zone A.

Create a policy with source zones A and B and destination zc A and B The rule would apply to traffic from zone A to zone E from zone B to zone A. but not traffic within zones A or B

Answer:

Explanation:

Answer Area

Create a policy with source zones A and B and destination zones A and B The rule would apply to traffic from zone A to zone B. and from zone B to zone A. but not traffic within zones A or B	Universal
Create a policy with source zones A and B. The rule will apply to all traffic within zone A and all traffic within zone B. but not to traffic between zones A and B.	Intrazone
Create a policy with source zones A and B and destination zones A and B, The rule should apply to all traffic within zone A. all traffic w4hin zone B, all traffic from zone A to zone B, and all traffic from zone B to zone A	Interzone

Question: 227

An administrator wants to create a NAT policy to allow multiple source IP addresses to be translated to the same public IP address. What is the most appropriate NAT policy to achieve this?

A. Dynamic IP and Port

B. Dynamic IP

C. Static IP

D. Destination

Answer: A

Explanation:

Question: 228

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. exclude

B. continue

C. hold

D. override

Answer: D

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.

Question: 229

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

Explanation:

Question: 230

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: A,B,D

Explanation:

Question: 231

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: B,D

Explanation:

Question: 232

What does an application filter help you to do?

A. It dynamically provides application statistics based on network, threat, and blocked activity,

B. It dynamically filters applications based on critical, high, medium, low. or informational severity.

C. It dynamically groups applications based on application attributes such as category and subcategory.

D. It dynamically shapes defined application traffic based on active sessions and bandwidth usage.

Answer: C

Explanation:

Question: 233

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: C

Explanation:

The Revert, Save, and Load operations all work with firewall co nfigurations local to the firewall. The Export operations transfer configurations as XML-formatted files from the firewall to the host running the web interface browser. From your local machine, you can save the files as configuration backups. The Import operations transfer XML configuration files from the host running the web interface browser to the firewall. The XML file can be loaded as the candidate configuration or even be committed to becoming the running configuration. [Palo Alto Networks]

Question: 234

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

Question: 235

An administrator wants to create a No-NAT rule to exempt a flow from the default NAT rule. What is the best way to do this?

A. Create a Security policy rule to allow the traffic.
B. Create a new NAT rule with the correct parameters and leave the translation type as None
C. Create a static NAT rule with an application override.
D. Create a static NAT rule translating to the destination interface.

Answer: B

Explanation:

Question: 236

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: C,D

Explanation:

Question: 237

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

Explanation:

Question: 238

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: B,D,E

Explanation:

Question: 239

Which type of address object is www.paloaltonetworks.com?

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

Answer: D

Explanation:

Question: 240

What are three characteristics of the Palo Alto Networks DNS Security service? (Choose three.)

A. It uses techniques such as DGA.DNS tunneling detection and machine learning.
B. It requires a valid Threat Prevention license.
C. It enables users to access real-time protections using advanced predictive analytics.
D. It requires a valid URL Filtering license.
E. It requires an active subscription to a third-party DNS Security service.

Answer: A,B,C

Explanation:

DNS Security subscription enables users to access real-time protections using advanced predictive analytics. When techniques such as DGA/DNS tunneling detection and machine learning are used, threats hidden within DNS traffic can be proactively identified and shared through an infinitely scalable cloud service. Because the DNS signatures and protections are stored in a cloud-based

architecture, you can access the full database of ever-expanding signatures that have been generated using a multitude of data sources. This list of signatures allows you to defend against an array of threats using DNS in real-time against newly generated malicious domains. To combat future threats, updates to the analysis, detection, and prevention capabilities of the DNS Security service will be available through content releases. To access the DNS Security service, you must have a Threat Prevention license and DNS Security license.

Question: 241

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

Explanation:

Question: 242

An administrator would like to block access to a web server, while also preserving resources and minimizing half-open sockets. What are two security policy actions the administrator can select? (Choose two.)

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

Answer: A,C

Explanation:

Question: 243

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

Explanation:

Question: 244

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: A,B,E

Explanation:

Question: 245

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

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

Explanation:

Question: 246

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: B,D,E

Explanation:

Question: 247

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

Explanation:

Question: 248

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

A. HIP profile

B. Application group

C. URL category

D. Application filter

Answer: C

Explanation:

Question: 249

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

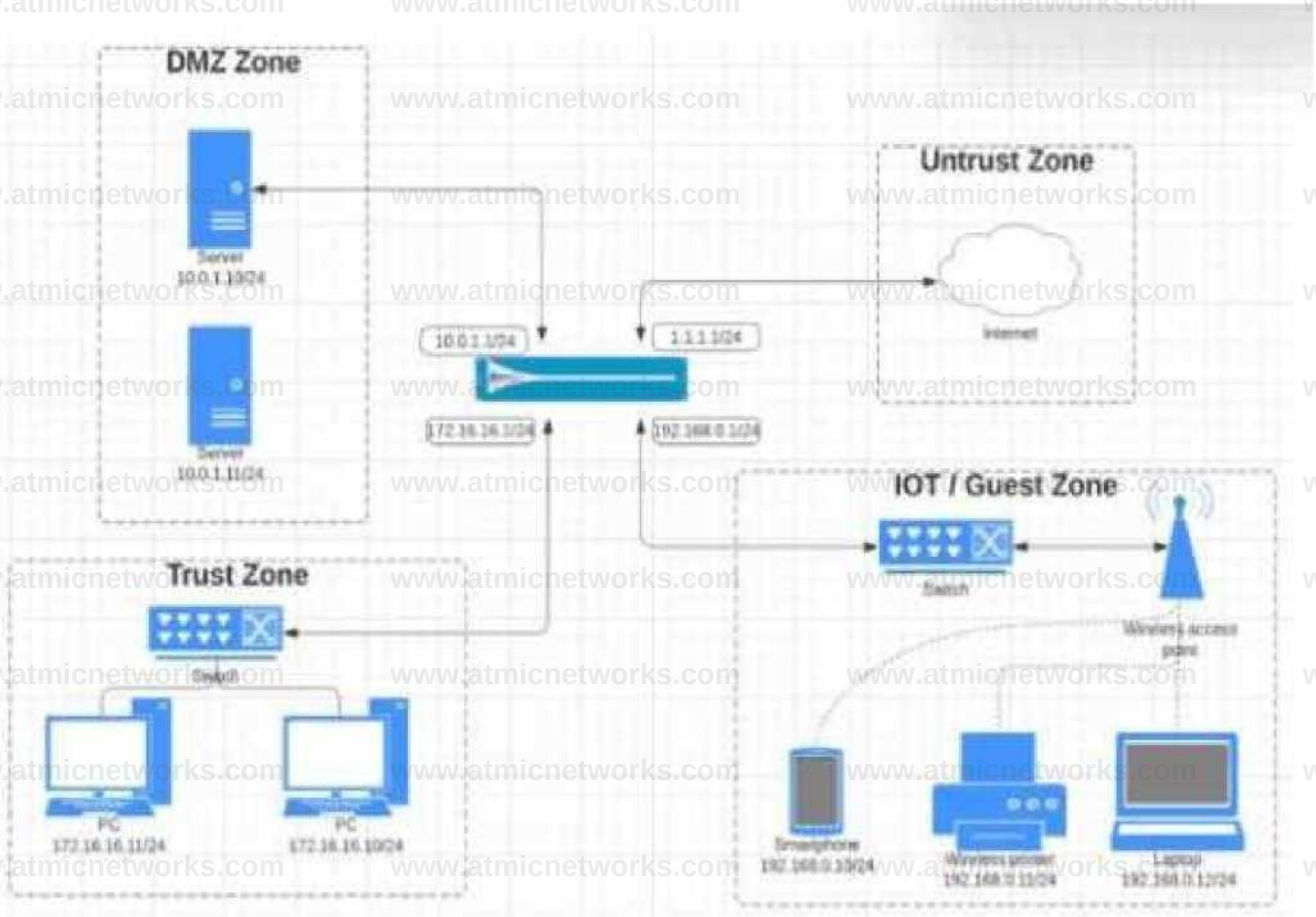
C. Address groups

D. Custom objects

Answer: B

Explanation:

Question: 250



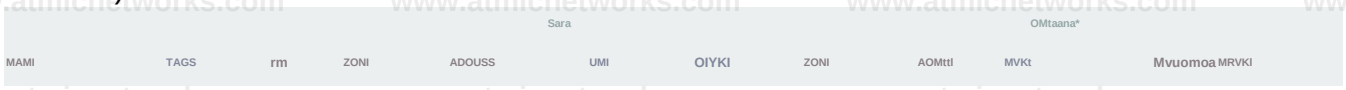
View the diagram. What is the most restrictive, yet fully functional rule, to allow general Internet and SSH traffic into both the DMZ and Untrust/Internet zones from each of the IOT/Guest and Trust Zones?

A)

B)

C)

D)



A. Option

B. Option

C. Option

D. Option

Answer: C

Explanation:

Question: 251

A website is unexpectedly allowed due to miscategorization.

What are two way-s 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.com.Submit for "request change*, identifying the appropriate categorization, and wait for confirmation before testing again.

D. Create a URL category and assign the affected URL.Add a Security policy with a URL category qualifier of the custom URL category below the original policy. Set the policy action to Deny.

Answer: C,D

Explanation:

Question: 252

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

Explanation:

Question: 253

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. Logging on the interzone-default policy is disabled.

B. Traffic is being denied on the interzone-default policy.

C. The Log Forwarding profile is not configured on the policy.

D. The interzone-default policy is disabled by default.

Answer: A

Explanation:

Question: 254

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

Explanation:

Question: 255

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

Explanation:

Question: 256

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 exists. Admins can then manually enable policies they want to keep and delete ones they want to remove.

Answer: C

Explanation:

Question: 257

Which rule type is appropriate for matching traffic occurring within a specified zone?

A. Interzone

B. Universal

C. Intrazone

D. Shadowed

Answer: C

Explanation:

Question: 258

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

Explanation:

Question: 259

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

Explanation:

Question: 260

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

Explanation:

Question: 261

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

Explanation:

Question: 262

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

Explanation:

Question: 263

An administrator has an IP address range in the external dynamic list and wants to create an exception for one specific IP address in this address range.

Which steps should the administrator take?

A. Add the address range to the Manual Exceptions list and exclude the IP address by selecting the entry.

B. Add each IP address in the range as a list entry and then exclude the IP address by adding it to the Manual Exceptions list.

C. Select the address range in the List Entries list. A column will open with the IP addresses. Select the entry to

exclude.

D. Add the specific IP address from the address range to the Manual Exceptions list by using regular expressions to define the entry.

Answer: D

Explanation:

Question: 264

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: B,D

Explanation:

Question: 265

					App«X»V					
	NAME	SERVICE	TRAffK ItYTCS. >0 DAYS)	AW ALLOWED	Am SEEN	DAYS WITH NO NEW Am COMPARE		MODIFIED	CREATED
		£ jptfCJKXjn OrfMt	tn u			258	Ccmpa*	2022 01 06 18 30 02	2020 11 16
25		$ JWttMttM defMI	63G |	All		447	CMOMV	202201 06 183002	2020 11 16
29	CuiOtHWOJ	«P«4k4D<n <MMA	maq			448	Ccnwav	2022 01 06 18 3002	2020 11 16
20	JOl»<»1r<<bB<itl		sot OK	wr		448	COTOMT	2022 01 06 18 3002	2020 11 16
31	CorOtJwfi	# x>d«4Oon cWtluR	2» IM			448	COMM	2022-01-06 18 3002	202041 16
32	GK£ Wirtil	£ MMitnjfMw <Jrf«uR	140 AM	•w		448	COTO**	2022 01 06 18 3002	2020)1 16
47	Wvisuflw JiHide*-		21 IM |			448	CM**!	2022 01 06 18 30.02	2020 11 16
27		W JW>4k 4tfon drf MA	22 8M |			448	Camcor*	2022 0106 18 3002	JOJO li U
30	Cara* IK	W apptronon drtMt	UM |			446	C0WR	2022 01 06 18 30 02	202011 16
28			SWAI			445	Cawt	2022 01 06 18 30 02	202011 16
37	Lof5«*ho*Tt#ff»c	)• MHAutkin <MMA	0 1			452	Cow	2022 01 06 18 3002	2020 11 16
24	Outbound True	uilKjfRri drf *A	0 1			419	CaNparv	2022 01 06 18 3002	2020 11 16

An administrator is updating Security policy to align with best practices.

Which Policy Optimizer feature is shown in the screenshot below?

A. Rules without App Controls

B. New App Viewer

C. Rule Usage

D. Unused Unused Apps

Answer: C

Explanation:

Question: 266

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

A. Reset-client

B. Reset-server

C. Deny

D. Allow

Answer: C

Explanation:

Question: 267

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: B,D

Explanation:

Question: 268

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: B,C,E

Explanation:

Question: 269

What is the maximum volume of concurrent administrative account sessions?

A. Unlimited

B. 2

C. 10

D. 1

Answer: C

Explanation:

Question: 270

In a File Blocking profile, which two actions should be taken to allow file types that support critical apps? (Choose two.)

A. Clone and edit the Strict profile.

B. Use URL filtering to limit categories in which users can transfer files.

C. Set the action to Continue.

D. Edit the Strict profile.

Answer: A,D

Explanation:

Question: 271

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

Explanation:

Question: 272

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

Question: 273

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

Explanation:

Question: 274

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

Question: 275

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

Explanation:

Question: 276

Why does a company need an Antivirus profile?

A. To prevent command-and-control traffic

B. To protect against viruses, worms, and trojans

C. To prevent known exploits

D. To prevent access to malicious web content

Answer: B

Explanation:

Question: 277

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

Explanation:

Question: 278

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

Explanation:

Question: 279

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

Explanation:

Question: 280

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: A

Explanation:

Domain Credential detection is the User Credential Detection method that checks for the submission of a valid corporate username and the associated password within a URL Filtering Security profile. This method requires the Windows User-ID agent and the User-ID credential service to be installed on a read-only domain controller (RODC). The firewall can then detect passwords submitted to web pages and compare them with the domain credentials stored on the RODC. If the firewall detects a match, it can block the request, alert the user, or generate a log entry1. Reference: Configure Credential Detection with the Windows User-ID Agent, Set Up Credential Phishing Prevention, Certifications - Palo Alto Networks, Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0) or [Palo Alto Networks Certified Network Security Administrator (PANOS 10.0)].

Question: 281

Which interface type requires no routing or switching but applies Security or NAT policy rules before passing allowed traffic?

A. Layer 3

B. Virtual Wire

C. Tap

D. Layer 2

Answer: A

Explanation:

Question: 282

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)

Source Zone Trusted
Declination Zone; DMZ
Services: Application-Default
Applications: SSH
Action: Deny

B)

Source Zone. Trusted
Destination Zone: DMZ
Services: SSH
Applications: Any
Action: Allow

C)

Source Zone: Trusted
Destination Zone. DMZ
Services: SSH
Applications: Any
Action: Deny

D)

Source Zone Trusted Destination Zone. DMZ Services: Application-Detank
Applications: SSH Action: Allow

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

Answer: D

Explanation:

Question: 283

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

Explanation:

Question: 284

A network administrator created an intrazone Security policy rule on the firewall. The source zones were set to IT. Finance, and HR.

Which two types of traffic will the rule apply to? (Choose two)

A. traffic between zone IT and zone Finance
B. traffic between zone Finance and zone HR
C. traffic within zone IT
D. traffic within zone HR

Answer: C,D

Explanation:

Question: 285

Which three filter columns are available when setting up an Application Filter? (Choose three.)

A. Parent App
B. Category
C. Risk
D. Standard Ports
E. Subcategory

Answer: B,C,E

Explanation:

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/objects/objects- application-filters

Question: 286

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: A,B,D

Explanation:

Question: 287

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)

D. Learning Spyware analysis

Answer: B

Explanation:

Question: 288

In which section of the PAN-OS GUI does an administrator configure URL Filtering profiles?

A. Policies

B. Network

C. Objects

D. Device

Answer: C

Explanation:

An administrator can configure URL Filtering profiles in the Objects section of the PAN-OS GUI. A URL Filtering profile is a collection of URL filtering controls that you can apply to individual Security policy rules that allow access to the internet1. You can set site access for URL categories, allow or disallow user credential submissions, enable safe search enforcement, and various other settings1.

To create a URL Filtering profile, go to Objects > Security Profiles > URL Filtering and click Add. You can then specify the profile name, description, and settings for each URL category and action2. You can also configure other options such as User Credential Detection, HTTP Header Insertion, and URL Filtering Inline ML2. After creating the profile, you can attach it to a Security policy rule that allows web traffic2.

Question: 289

By default, what is the maximum number of templates that can be added to a template stack?

A. 6

B. 8

C. 10

D. 12

Answer: B

Explanation:

By default, the maximum number of templates that can be added to a template stack is 8. This is the recommended limit for performance reasons, as adding more templates may result in sluggish responses on the user interface. However, starting from PAN-OS 8.1.10 and 9.0.4, you can use a debug command to increase the maximum number of templates per stack to 16. This command requires a commit operation to take effect.

A template stack is a collection of templates that you can use to push common settings to multiple firewalls or Panorama managed collectors. A template contains the network and device settings that you want to share across devices, such as interfaces, zones, virtual routers, DNS, NTP, and login banners. You can create multiple templates for different device groups or locations and add them to a template stack in a hierarchical order. The settings in the lower templates override the settings in the higher templates if there are any conflicts. You can then assign a template stack to one or more devices and push the configuration changes.

Question: 290

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.

Reference:

1: Security Profile: Anti-Spyware - Palo Alto Networks

Question: 291

Which two DNS policy actions in the anti-spyware security profile can prevent hacking attacks through DNS queries to malicious domains? (Choose two.)

A. Deny
B. Sinkhole
C. Override
D. Block

Answer: B,D

Explanation:

A DNS policy action is a setting in an Anti-Spyware security profile that defines how the firewall handles DNS queries to malicious domains. A malicious domain is a domain name that is associated with a known threat, such as malware, phishing, or botnet1.

There are four possible DNS policy actions: alert, allow, block, and sinkhole1.

The alert action logs the DNS query and allows it to proceed to the intended destination. This action does not prevent hacking attacks, but only notifies the administrator of the potential threat1.

The allow action allows the DNS query to proceed to the intended destination without logging it. This action does not prevent hacking attacks, but only bypasses the DNS security inspection2.

The block action blocks the DNS query and sends a response to the client with an NXDOMAIN (nonexistent domain) error code. This action prevents hacking attacks by preventing the client from resolving the malicious domain1.

The sinkhole action redirects the DNS query to a predefined IP address (the sinkhole IP address) that is under the control of the administrator. This action prevents hacking attacks by isolating the client from the malicious domain and allowing the administrator to monitor and remediate the infected host1.

The override action is not a valid DNS policy action, but a setting in an Anti-Spyware security profile that allows the administrator to create exceptions for specific spyware signatures that they want to override the default action or log settings3.

Therefore, the two DNS policy actions that can prevent hacking attacks through DNS queries to malicious domains are block and sinkhole.

Reference:

1: Enable DNS Security - Palo Alto Networks 2: How To Disable the DNS Security Feature from an Anti-Spyware Profile - Palo Alto Networks 3: Security Profile: Anti-Spyware - Palo Alto Networks

Question: 292

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

A. WildFire analysis

B. Vulnerability profile

C. Content-ID

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.

Reference:

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]

Question: 293

How can a complete overview of the logs be displayed to an administrator who has permission in the system to view them?

A. Select the unified log entry in the side menu.

B. Modify the number of columns visible on the page

C. Modify the number of logs visible on each page.

D. Select the system logs entry in the side menu.

Answer: A

Explanation:

The best way to view a complete overview of the logs is to select the unified log entry in the side menu. The unified log is a single view that displays all the logs generated by the firewall, such as

traffic, threat, URL filtering, data filtering, and WildFire logs1. The unified log allows the administrator to filter, sort, and export the logs based on various criteria, such as time range, severity, source, destination, application, or action1.

Modifying the number of columns visible on the page or the number of logs visible on each page does not provide a complete overview of the logs, but only changes the display settings of the current log view. Selecting the system logs entry in the side menu does not show all the logs generated by the firewall, but only shows the logs related to system events, such as configuration changes, system alerts, or HA status2.

Reference:

1: View Logs - Palo Alto Networks 2: View and Manage Logs - Palo Alto Networks

Question: 294

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.

Reference:

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

Question: 295

What is the default action for the SYN Flood option within the DoS Protection profile?

A. Alert

B. Random Early Drop

C. Reset-client

D. Sinkhole

Answer: B

Explanation:

Random Early Drop —The firewall uses an algorithm to progressively start dropping that type of packet. If the attack continues, the higher the incoming cps rate (above the Activate Rate) gets, the more packets the firewall drops. .. (https://docs.paloaltonetworks.com/pan-os/9-1/pan-os- admin/zone-protection-and-dos-protection/dos-protection-against-flooding-of-new- sessions/configure-dos-protection-against-flooding-of-new-sessions)

Question: 296

Which Security policy set should be used to ensure that a policy is applied first?

A. Child device-group pre-rulebase

B. Shared pre-rulebase

C. Parent device-group pre-rulebase

D. Local firewall policy

Answer: B

Explanation:

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/panorama-web- interface/defining-policies-on-panorama

Question: 297

Which type of DNS signatures are used by the firewall to identify malicious and command-and- control domains?

A. DNS Malicious signatures

B. DNS Malware signatures

C. DNS Block signatures

D. DNS Security signatures

Answer: D

Explanation:

https://docs.paloaltonetworks.com/dns-security/administration/configure-dns-security/enable-dns-security#tabs-id066476b2-c4dd-4fc0-b7e4-f4ba32e19f60

Question: 298

Which three types of entries can be excluded from an external dynamic list (EDL)? (Choose three.)

A. IP addresses

B. Domains

C. User-ID

D. URLs

E. Applications

Answer: A,B,D

Explanation:

Three types of entries that can be excluded from an external dynamic list (EDL) are IP addresses, domains, and URLs. An EDL is a text file that is hosted on an external web server and contains a list of objects, such as IP addresses, URLs, domains, International Mobile Equipment Identities (IMEIs), or International Mobile Subscriber Identities (IMSIs) that the firewall can import and use in policy rules. You can exclude entries from an EDL to prevent the firewall from enforcing policy on those entries. For example, you can exclude benign domains that applications use for background traffic from Authentication policy1. To exclude entries from an EDL, you need to:

Select the EDL on the firewall and click Manual Exceptions.

Add the entries that you want to exclude in the Manual Exceptions list. The entries must match the type and format of the EDL. For example, if the EDL contains IP addresses, you can only exclude IP addresses.

Click OK to save the changes. The firewall will not enforce policy on the excluded entries.

Reference: Exclude Entries from an External Dynamic List, External Dynamic List, Certifications - Palo Alto Networks, Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0) or Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0).

Question: 299

The administrator profile "SYS01 Admin" is configured with authentication profile "Authentication

Sequence SYS01," and the authentication sequence SYS01 has a profile list with four authentication profiles:

- Auth Profile LDAP
- Auth Profile Radius
- Auth Profile Local
- Auth Profile TACACS

After a network outage, the LDAP server is no longer reachable. The RADIUS server is still reachable but has lost the "SYS01 Admin" username and password.

What is the "SYS01 Admin" login capability after the outage?

A. Auth KO because RADIUS server lost user and password for SYS01 Admin

B. Auth KO because LDAP server is not reachable

C. Auth OK because of the Auth Profile Local

D. Auth OK because of the Auth Profile TACACS -

Answer: C

Explanation:

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/authentication/configure-an- authentication-profile-and-sequence

Question: 300

In which two Security Profiles can an action equal to the block IP feature be configured? (Choose two.)

A. Antivirus

B. URL Filtering

C. Vulnerability Protection

D. Anti-spyware

Answer: C,D

Explanation:

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/objects/objects-security- profiles/actions-in-security-profiles

Question: 301

What are two valid selections within an Anti-Spyware profile? (Choose two.)

A. Default

B. Deny

C. Random early drop

D. Drop

Answer: A,D

Explanation:

Deny is a policy action, random early drop is part of the inner workings of DoS protection

Question: 302

When is an event displayed under threat logs?

A. When traffic matches a corresponding Security Profile

B. When traffic matches any Security policy

C. Every time a session is blocked

D. Every time the firewall drops a connection

Answer: A

Explanation:

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/monitoring/view-and-manage- logs/log-types-and-severity-levels/threat-logs#:~:text=Threat%20logs%20display%20entries%20when,security%20rule%20on%20the%20firew all.

Question: 303

Which Security profile should be applied in order to protect against illegal code execution?

A. Vulnerability Protection profile on allowed traffic

B. Antivirus profile on allowed traffic

C. Antivirus profile on denied traffic

D. Vulnerability Protection profile on denied traffic

Answer: A

Explanation:

The Security profile that should be applied in order to protect against illegal code execution is the Vulnerability Protection profile on allowed traffic. The Vulnerability Protection profile defines the actions that the firewall takes to protect against exploits and vulnerabilities in applications and protocols. The firewall can block or alert on traffic that matches a specific threat signature or a group of threats. The Vulnerability Protection profile can prevent illegal code execution by detecting and blocking attempts to exploit buffer overflows, format string vulnerabilities, or other code injection techniques1. To apply the Vulnerability Protection profile on allowed traffic, you need to:

Create or modify a Vulnerability Protection profile on the firewall or Panorama and configure the rules and exceptions for the threats that you want to protect against2.

Attach the Vulnerability Protection profile to a Security policy rule that allows traffic that you want to scan for vulnerabilities3.

Commit the changes to the firewall or Panorama and the managed firewalls.

Reference: Vulnerability Protection Profile, Create a Vulnerability Protection Profile, Attach a Vulnerability Protection Profile to a Security Policy Rule, Certifications - Palo Alto Networks, Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0) or [Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0)].

Question: 304

Which three types of Source NAT are available to users inside a NGFW? (Choose three.)

A. Dynamic IP and Port (DIPP)

B. Static IP

C. Static Port

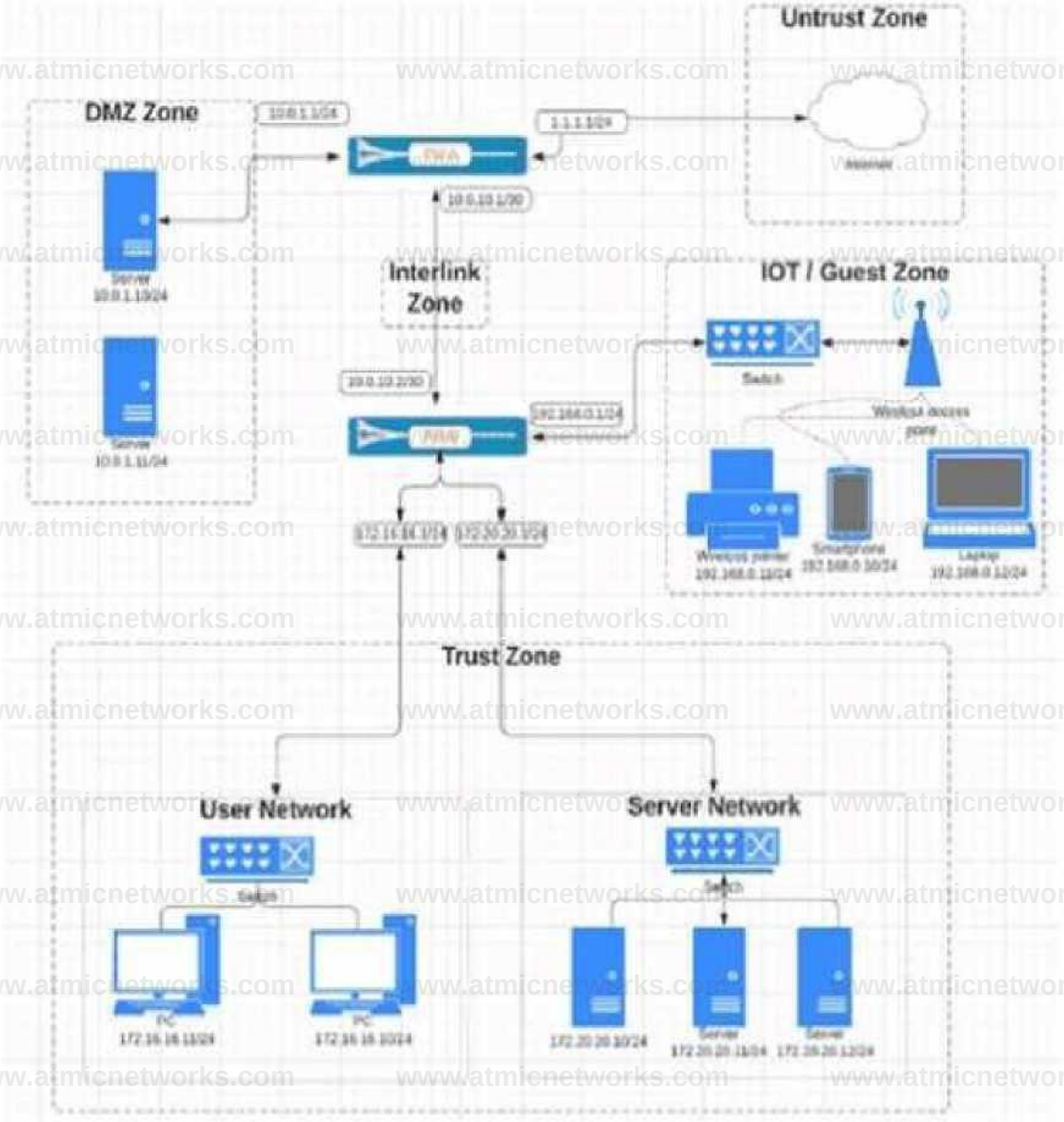
D. Dynamic IP

E. Static IP and Port (SIPP)

Answer: A,B,E

Explanation:

Question: 305



Based on the network diagram provided, which two statements apply to traffic between the User and Server networks? (Choose two.)

A. Traffic is permitted through the default intrazone "allow" rule.

B. Traffic restrictions are possible by modifying intrazone rules.

C. Traffic restrictions are not possible, because the networks are in the same zone.

D. Traffic is permitted through the default interzone "allow" rule.

Answer: A,B

Explanation:

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail? id=kA10g000000ClTHCA0&lang=es

Question: 306

Which two types of profiles are needed to create an authentication sequence? (Choose two.)

A. Server profile

B. Authentication profile

C. Security profile

D. Interface Management profile

Answer: A,B

Explanation:

In the FW you define an Auth sequence which specifies the Auth Profile. If you click add on an Auth Profile and define one named TACACS for example, the Auth Profile calls in the TACACS+ Server Profile.

Question: 307

Which setting is available to edit when a tag is created on the local firewall?

A. Location

B. Color

C. Order

D. Priority

Answer: B

Explanation:

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/objects/objects- tags/create-tags

Question: 308

What is the best-practice approach to logging traffic that traverses the firewall?

A. Enable both log at session start and log at session end.

B. Enable log at session start only.

C. Enable log at session end only.

D. Disable all logging options.

Answer: C

Explanation:

The best-practice approach to logging traffic that traverses the firewall is to enable log at session end only. This option allows the firewall to generate a log entry only when a session ends, which reduces the load on the firewall and the log storage. The log entry contains information such as the source and destination IP addresses, ports, zones, application, user, bytes, packets, and duration of the session. The log at session end option also provides more accurate information about the session, such as the final application and user, the total bytes and packets, and the session end reason1. To enable log at session end only, you need to:

Create or modify a Security policy rule that matches the traffic that you want to log.

Select the Actions tab in the policy rule and check the Log at Session End option.

Commit the changes to the firewall or Panorama and the managed firewalls.

Reference: View and Manage Logs, Log at Session End, Certifications - Palo Alto Networks, [Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0)] or [Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0)].

Question: 309

Where in Panorama Would Zone Protection profiles be configured?

A. Shared

B. Templates

C. Device Groups

D. Panorama tab

Answer: B

Explanation:

https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/manage-firewalls/use-case- configure-firewalls-

using-panorama/set-up-your-centralized-configuration-and-policies/use- templates-to-administer-a-base-configuration

Question: 310

Based on the image provided, which two statements apply to the Security policy rules? (Choose two.)

	N^M(	TAGS	TYPE	Source ZONE	ADDRESS	DEVICE	Destination ZONE	ADDRESS	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
19	Allow-O#6c?-Protr*mt	none	universal	^ Mtrm^J	any		e^ F eternal		|@ offne proteins	^ Application-defa...	0 Allow		a&
20	Allow HP	none	u reversal	»R internal	any	Any	^ External	^ FTP Server	any	& FT*	© Allow	®	■B
21	Allow Social Media	none	universal	■R internal	any	any	^ Externa?	any	g tttrbook	^ applicatlwdeta...	©Allow	®	g&
22	•rtraionc-dcfault *	none	intrarono	*W	any	any	fintrazorw)	any	any	any	© Allow	none	130.
23	interrow-default £	none	interrow	*Y	any	any	any	any	any	any	g|tw	none	(H(3.

A. The Allow-Office-Programs rule is using an application filter.

B. The Allow-Office-Programs rule is using an application group.

C. The Allow-Social-Media rule allows all Facebook functions.

D. In the Allow-FTP policy, FTP is allowed using App-ID.

Answer: A,C

Explanation:

Question: 311

How would a Security policy need to be written to allow outbound traffic using Secure Shell (SSH) to destination ports tcp/22 and tcp/4422?

A. The admin creates a custom service object named "tcp-4422" with port tcp/4422. The admin then creates a Security policy allowing application "ssh" and service "tcp-4422".

B. The admin creates a custom service object named "tcp-4422" with port tcp/4422. The admin then creates a Security policy allowing application "ssh", service "tcp-4422". and service "applicationdefault".

C. The admin creates a Security policy allowing application "ssh" and service "application-default".

D. The admin creates a custom service object named "tcp-4422" with port tcp/4422. The admin also creates a custom service object named "tcp-22" with port tcp/22.The admin then creates a Security policy allowing application "ssh", service "tcp-4422". and service "tcp-22".

Answer: D

Explanation:

Question: 312

Which feature must be configured to enable a data plane interface to submit DNS queries originated from the firewall on behalf of the control plane?

A. Service route

B. Admin role profile

C. DNS proxy

D. Virtual router

Answer: A

Explanation:

By default, the firewall uses the management (MGT) interface to access external services, such as DNS servers, external authentication servers, Palo Alto Netw orks services such as soft ware, URL updates, licenses, and AutoFocus. An alternative to using the MGT interface is configuring a data port (a standard interface) to access these services. The path from the interface to th e service on a server is aservice route. [Palo Alto Networks]

PAN-OS 10 -> Device -> Setup -> Services -> Service Features -> Service Route Configuration

Question: 313

An administrator creates a new Security policy rule to allow DNS traffic from the LAN to the DMZ zones. The administrator does not change the rule type from its default value.

What type of Security policy rule is created?

A. Tagged

B. Intrazone

C. Universal

D. Interzone

Answer: C

Explanation:

Question: 314

When HTTPS for management and GlobalProtect are enabled on the same data plane interface, which TCP port is used for management access?

A. 80

B. 443

C. 4443

D. 8443

Answer: C

Explanation:

The GlobalProtect Portal can be accessed by going to the IP address of the designated interface using https on port 443. The WebUI on the same interface can be accessed by going to the interface's IP address using https on port 4443. The port for WebUI management is changed because the tcp/443 socket used by GlobalProtect takes precedence

Question: 315

An administrator manages a network with 300 addresses that require translation. The administrator configured NAT with an address pool of 240 addresses and found that connections from addresses that needed new translations were being dropped.

Which type of NAT was configured?

A. Static IP

B. Dynamic IP

C. Destination NAT

D. Dynamic IP and Port

Answer: B

Explanation:

The size of the NAT pool should be equal to the number of internal hosts that require address translations. By default, if the source address pool is larger than the NAT address pool and eventually all of the NAT addresses are allocated, new connections that need address translation are dropped. To override this default behavior, use Advanced (Dynamic IP/Port Fallback) to enable the use of DIPP addresses when necessary

Question: 316

What are the two main reasons a custom application is created? (Choose two.)

A. To correctly identify an internal application in the traffic log

B. To change the default categorization of an application

C. To visually group similar applications

D. To reduce unidentified traffic on a network

Answer: A,D

Explanation:

https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/app-id/use-application-objects-in- policy/create-a-custom-application

Question: 317

What Policy Optimizer policy view differ from the Security policy do?

A. It shows rules that are missing Security profile configurations.

B. It indicates rules with App-ID that are not configured as port-based.

C. It shows rules with the same Source Zones and Destination Zones.

D. It indicates that a broader rule matching the criteria is configured above a more specific rule.

Answer: B

Explanation:

Policy Optimizer policy view differs from the Security policy view in several ways. One of them is that it indicates rules with App-ID that are not configured as port-based. These are rules that have the application set to “any” instead of a specific application or group of applications. These rules are overly permissive and can introduce security gaps, as they

allow any application traffic on the specified ports. Policy Optimizer helps you convert these rules to application-based rules that follow the principle of least privilege access12. You can use Policy Optimizer to discover and convert portbased rules to application-based rules, and also to remove unused applications, eliminate unused rules, and discover new applications that match your policy criteria3. Reference:

Policy Optimizer Best Practices - Palo Alto Networks

Manage: Policy Optimizer - Palo Alto Networks | TechDocs

Why use Security Policy Optimizer and what are the benefits?

Question: 318

How does the Policy Optimizer policy view differ from the Security policy view?

A. It provides sorting options that do not affect rule order.

B. It displays rule utilization.

C. It details associated zones.

D. It specifies applications seen by rules.

Answer: A

Explanation:

You can't filter or sort rules in PoliciesSecurity because that would change the order of the policy rules in the rulebase. Filtering and sorting PoliciesSecurityPolicy OptimizerNo App Specified, PoliciesSecurityPolicy OptimizerUnused Apps, and PoliciesSecurityPolicy OptimizerNew App Viewer (if you have a SaaS Inline Security subscription) does not change the order of the rules in the rulebase. https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/app-id/security-policy- rule-optimization/policy-optimizer-concepts/sorting-and-filtering-security-policy-rules

Question: 319

Which System log severity level would be displayed as a result of a user password change?

A. High

B. Critical

C. Medium

D. Low

Answer: D

Explanation:

System logs display entries for each system event on the firewall.

1. Critical - Hardware failures, including high availability (HA) failover and link failures.
2. High - Serious issues, including dropped connections with external devices, such as LDAP and RADIUS servers.
3. Medium - Mid-level notifications, such as antivirus package upgrades.
4. Low - Minor severity notifications, such as user password changes.
5. Informational - Log in/log off, administrator name or password change, any configuration change, and all other events not covered by the other severity levels.

https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/monitoring/view-and-manage- logs/log-types-and-severity-levels/system-logs#id8edbfdae-ed92-4d8e-ab76-6a38f96e8cb1

Question: 320

Which situation is recorded as a system log?

A. An attempt to access a spoofed website has been blocked.

B. A connection with an authentication server has been dropped.

C. A file that has been analyzed is potentially dangerous for the system.

D. A new asset has been discovered on the network.

Answer: B

Explanation:

Question: 321

Where within the URL Filtering security profile must a user configure the action to prevent credential submissions?

A. URL Filtering > Inline Categorization

B. URL Filtering > Categories

C. URL Filtering > URL Filtering Settings

D. URL Filtering > HTTP Header Insertion

Answer: B

Explanation:

URL filtering technology protects users from web-based threats by providing granular control over user access and interaction with content on the Internet. You can develop a URL filtering policy that limits access to sites based on URL categories, users, and groups. For example, you can block access to sites known to host malware and prevent end users from entering corporate credentials to sites in certain categories.

Question: 322

Which two features implement one-to-one translation of a source IP address while allowing the source port to change? (Choose two.)

A. Static IP

B. Dynamic IP / Port Fallback

C. Dynamic IP

D. Dynamic IP and Port (DIPP)

Answer: A,D

Explanation:

Static IP and Dynamic IP and Port (DIPP) are two features that implement one-to-one translation of a source IP address while allowing the source port to change. Static IP translates a single source address to a specific public address, and allows the source port to change dynamically1. Dynamic IP and Port (DIPP) translates the source IP address or range to a single IP address, and uses the source port to differentiate between multiple source IPs that share the same translated address2. Both of these features provide a one-to-one translation of IP addresses, but do not restrict the source port.

Reference:

Static IP - Palo Alto Networks

Dynamic IP and Port - Palo Alto Networks

Question: 323

A network administrator creates an intrazone security policy rule on a NGFW. The source zones are set to IT. Finance, and HR.

To which two types of traffic will the rule apply? (Choose two.)

A. Within zone HR

B. Within zone IT

C. Between zone IT and zone HR

D. Between zone IT and zone Finance

Answer: A,B

Explanation:

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClTHCA0

Question: 324

An organization has some applications that are restricted for access by the Human Resources Department only, and other applications that are available for any known user in the organization.

What object is best suited for this configuration?

A. Application Group

B. Tag

C. External Dynamic List

D. Application Filter

Answer: A

Explanation:

Question: 325

Which order of steps is the correct way to create a static route?

A. 1) Enter the route and netmask2) Enter the IP address for the specific next hop3) Specify the outgoing interface for packets to use to go to the next hop4) Add an IPv4 or IPv6 route by name

B. 1) Enter the route and netmask2) Specify the outgoing interface for packets to use to go to the next hop3) Enter the IP address for the specific next hop4) Add an IPv4 or IPv6 route by name

C. 1) Enter the IP address for the specific next hop2) Enter the route and netmask3) Add an IPv4 or IPv6 route by name4) Specify the outgoing interface for packets to use to go to the next hop

D. 1) Enter the IP address for the specific next hop2) Add an IPv4 or IPv6 route by name3) Enter the route and netmask4) Specify the outgoing interface for packets to use to go to the next hop

Answer: A

Explanation:

Enter the route and netmask

Enter the IP address for the specific next hop

Specify the outgoing interface for packets to use to go to the next hop

Add an IPv4 or IPv6 route by name Comprehensive This is the correct order of steps to create a static route in a virtual router on the firewall. The first step is to enter the route and netmask for the destination network, such as 192.168.2.2/24 for an IPv4 address or 2001:db8:123:1::1/64 for an IPv6 address. The second step is to enter the IP address for the specific next hop, such as 192.168.56.1 or 2001:db8:49e:1::1. The third step is to specify the outgoing interface for packets to use to go to the next hop, such as ethernet1/1. The fourth step is to add an IPv4 or IPv6 route by name, such as route11. Reference:

Configure a Static Route - Palo Alto Networks

Question: 326

Which two actions are needed for an administrator to get real-time WildFire signatures? (Choose two.)

A. Obtain a Threat Prevention subscription.

B. Enable Dynamic Updates.

C. Move within the WildFire public cloud region.

D. Obtain a WildFire subscription.

Answer: B,D

Explanation:

https://docs.paloaltonetworks.com/wildfire/u-v/wildfire-whats-new/wildfire-features-in-panos- 100/wildfire-real-time-signature-updates

Question: 327

Which path in PAN-OS 10.2 is used to schedule a content update to managed devices using Panorama?

A. Panorama > Device Deployment > Dynamic Updates > Schedules > Add

B. Panorama > Device Deployment > Content Updates > Schedules > Add

C. Panorama > Dynamic Updates > Device Deployment > Schedules > Add

D. Panorama > Content Updates > Device Deployment > Schedules > Add

Answer: A

Explanation:

https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-upgrade/upgrade-panorama/deploy- updates-to-firewalls-log-collectors-and-wildfire-appliances-using-panorama/schedule-a-content- update-using-panorama

Question: 328

Which Security policy action will message a user's browser that their web session has been terminated?

A. Drop

B. Deny

C. Reset client

D. Reset server

Answer: C

Explanation:

Sending a reset only to the client would ensure, for example, internal hosts receive a notification the

session was reset and the browser is not left spinning or the application can close the established session while the remote server is left unaware.

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClItCAC

Question: 329

Which two addresses should be reserved to enable DNS sinkholing? (Choose two.)

A. IPv6

B. Email

C. IPv4

D. MAC

Answer: A,C

Explanation:

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClGECA0

Question: 330

Which feature enables an administrator to review the Security policy rule base for unused rules?

A. Test Policy Match

B. Policy Optimizer

C. View Rulebase as Groups

D. Security policy tags eb

Answer: B

Explanation:

Policy Optimizer provides a simple workflow to migrate your legacy Security policy rulebase to an App-ID based rulebase, which improves your security by reducing the attack surface and gaining visibility into applications so you can safely enable them. Policy Optimizer can also identify unused rules, duplicate rules, and rules that can be merged or reordered to optimize your rulebase. You can use Policy Optimizer to review the usage statistics of your rules and take actions to clean up or modify your rulebase as needed1. Reference: Security Policy Rule Optimization, Updated Certifications for PAN-OS 10.1, Free PCNSE Questions for Palo Alto Networks PCNSE Exam

Question: 331

A systems administrator momentarily loses track of which is the test environment firewall and which is the production firewall. The administrator makes changes to the candidate configuration of the production firewall, but does not commit the changes. In addition, the configuration was not saved prior to

making the changes.

Which action will allow the administrator to undo the changes?

A. Load configuration version, and choose the first item on the list.

B. Load named configuration snapshot, and choose the first item on the list.

C. Revert to last saved configuration.

D. Revert to running configuration.

Answer: D

Explanation:

Reverting to the running configuration will undo the changes made to the candidate configuration since the last commit. This operation will replace the settings in the current candidate configuration with the settings from the running configuration. The firewall provides the option to revert all the changes or only specific changes by administrator or location1. Reference: Revert Firewall Configuration Changes, How to Revert to a Previous Configuration, How to revert uncommitted changes on the firewall?.

Question: 332

What is used to monitor Security policy applications and usage?

A. Policy Optimizer

B. App-ID

C. Security profile

D. Policy-based forwarding

Answer: A

Explanation:

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/policies/policies- security/applications-and-usage

Question: 333

What is a default setting for NAT Translated Packets when the destination NAT translation is selected as Dynamic IP (with session distribution)?

A. IP Hash

B. Source IP Hash

C. Round Robin

D. Least Sessions

Answer: C

Explanation:

When the destination NAT translation is selected as Dynamic IP (with session distribution), the firewall uses a round-robin algorithm to distribute sessions among the available IP addresses that are resolved from the FQDN. This option

allows you to load-balance traffic to multiple servers that have dynamic IP addresses1. Reference: Destination NAT, NAT, Getting Started: Network Address Translation (NAT).

Question: 334

Which table for NAT and NPTv6 (IPv6-to-IPv6 Network Prefix Translation) settings is available only on Panorama?

A. NAT Target Tab

B. NAT Active/Active HA Binding Tab

C. NAT Translated Packet Tab

D. NAT Policies General Tab

Answer: A

Explanation:

The NAT Target tab is a table that allows you to specify the target firewalls or device groups for each NAT policy rule on Panorama. This tab is available only on Panorama and not on individual firewalls. The NAT Target tab enables you to create a single NAT policy rulebase on Panorama and then selectively push the rules to the firewalls or device groups that require them. This reduces the complexity and duplication of managing NAT policies across multiple firewalls1. Reference: NAT Target Tab, NAT Policy Overview, NPTv6 Overview, Updated Certifications for PAN-OS 10.1.

Question: 335

Which three Ethernet interface types are configurable on the Palo Alto Networks firewall? (Choose three.)

A. Virtual Wire

B. Tap

C. Dynamic

D. Layer 3

E. Static

Answer: A,B,D

Explanation:

Palo Alto Networks firewalls support three types of Ethernet interfaces that can be configured on the firewall: virtual wire, tap, and layer 31. These interface types determine how the firewall processes traffic and applies security policies. Some of the characteristics of these interface types are:

Virtual Wire: A virtual wire interface allows the firewall to transparently pass traffic between two network segments without modifying the packets or affecting the routing. The firewall can still apply security policies and inspect the traffic based on the source and destination zones of the virtual wire2.

Tap: A tap interface allows the firewall to passively monitor traffic from a network switch or router without affecting the traffic flow. The firewall can only receive traffic from a tap interface and cannot send traffic out of it. The firewall can apply security policies and inspect the traffic based on the source and destination zones of the tap interface3.

Layer 3: A layer 3 interface allows the firewall to act as a router and participate in the network routing. The firewall can send and receive traffic from a layer 3 interface and apply security policies and inspect the traffic based on the source and destination IP addresses and zones of the interface4.

Reference: Ethernet Interface Types, Virtual Wire Interfaces, Tap Interfaces, Layer 3 Interfaces, Updated Certifications for PAN-OS 10.1, [Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0)] or [Palo Alto Networks Certified Network Security Administrator (PANOS 10.0)].

Question: 336

Which action can be performed when grouping rules by group tags?

A. Delete Tagged Rule(s)

B. Edit Selected Rule(s)

C. Apply Tag to the Selected Rule(s)

D. Tag Selected Rule(s)

Answer: D

Explanation:

When grouping rules by group tags, the action that can be performed is to tag selected rule(s). This action allows you to assign one or more tags to the selected rules, which will group them together and display them under the corresponding tag group. You can use tags to organize and visually distinguish your rules based on different criteria, such as function, location, or priority1. Reference: View Rules by Tag Group, Use Tags to Group and Visually Distinguish Objects, Certifications - Palo Alto Networks, Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0) or [Palo Alto Networks Certified Network Security Administrator (PANOS 10.0)].

Question: 337

Which path in PAN-OS 11.x would you follow to see how new and modified App-IDs impact a Security policy?

A. Objects > Dynamic Updates > Review App-IDs

B. Device > Dynamic Updates > Review Policies

C. Device > Dynamic Updates > Review App-IDs

D. Objects > Dynamic Updates > Review Policies

Answer: C

Explanation:

To see how new and modified App-IDs impact your Security policy, you need to follow the path Device > Dynamic Updates > Review App-IDs on PAN-OS 11.x. This option allows you to perform a content update policy review for both downloaded and installed content. You can view the list of new and modified App-IDs and their descriptions, and see which Security policy rules are affected by them. You can also modify the rules or create new ones to adjust your Security policy as needed1. Reference: See How New and Modified App-IDs Impact Your Security Policy, Updated Certifications for PAN-OS 10.1, Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0) or [Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0)].

Question: 338

An administrator wants to enable access to www.paloaltonetworks.com while denying access to all other sites in the same category.

Which object should the administrator create to use as a match condition for the security policy rule that allows access to www.paloaltonetworks.com?

A. Application group

B. Address ab

C. URL category

D. Service

Answer: C

Explanation:

A URL category object is the object that the administrator should create to use as a match condition for the security policy rule that allows access to www.paloaltonetworks.com while denying access to all other sites in the same category. A URL category object allows the administrator to define a custom list of URLs that belong to a specific category, such as Business and Economy. The administrator can then use this object in a security policy rule to allow or deny access to the URLs based on the category1. For example, the administrator can create a URL category object that contains www.paloaltonetworks.com and assign it to the Business and Economy category. Then, the administrator can create a security policy rule that allows access to this URL category object and denies access to the predefined Business and Economy category2. Reference: Create a Custom URL Category, Create a Security Policy Rule to Allow or Deny Access to a Custom URL Category, Certifications - Palo Alto Networks, Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0) or [Palo Alto Networks Certified Network Security Administrator (PANOS 10.0)].

Question: 339

When a security rule is configured as Intrazone, which field cannot be changed?

A. Actions
B. Source Zone
C. Application
D. Destination Zone

Answer: D

Explanation:

When a security rule is configured as Intrazone, the destination zone field cannot be changed. This is because an

intrazone rule applies to traffic that originates and terminates in the same zone. The destination zone is automatically set to the same value as the source zone and cannot be modified1. An intrazone rule allows you to control and inspect traffic within a zone, such as applying security profiles or logging options2. Reference: What are Universal, Intrazone and Interzone Rules?, Security Policy, Updated Certifications for PAN-OS 10.1, Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0) or [Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0)].

Question: 340

In which two Security Profiles can an action equal to the block IP feature be configured? (Choose two.)

A. URL Filtering

B. Vulnerability Protection

C. Antivirus b

D. Anti-spyware

Answer: B,D

Explanation:

The block IP feature can be configured in two Security Profiles: Vulnerability Protection and Antispyware. The block IP feature allows the firewall to block traffic from a source IP address for a specified period of time after detecting a threat. This feature can help prevent further attacks from the same source and reduce the load on the firewall1. The block IP feature can be enabled in the following Security Profiles:

Vulnerability Protection: A Vulnerability Protection profile defines the actions that the firewall takes to protect against exploits and vulnerabilities in applications and protocols. You can configure a rule in the Vulnerability Protection profile to block IP connections for a specific threat or a group of threats2.

Anti-spyware: An Anti-spyware profile defines the actions that the firewall takes to protect against spyware and command-and-control (C2) traffic. You can configure a rule in the Anti-spyware profile to block IP addresses for a specific spyware or C2 signature.

Reference: Monitor Blocked IP Addresses, Block IP Addresses, Vulnerability Protection Profile, [AntiSpyware Profile], Certifications - Palo Alto Networks, [Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0)] or [Palo Alto Networks Certified Network Security Administrator (PANOS 10.0)].

Question: 341

In which section of the PAN-OS GUI does an administrator configure URL Filtering profiles?

A. Network ab
B. Policies
C. Objects
D. Device

Answer: C

Explanation:

URL Filtering profiles are configured in the Objects section of the PAN-OS GUI. A URL Filtering profile defines the actions that the firewall takes for different URL categories, such as allow, block, alert, continue, or override. You can also configure settings for credential phishing prevention, URL filtering inline machine learning, and safe search enforcement in a URL Filtering profile1. To create or modify a URL Filtering profile, you need to go to Objects > Security Profiles > URL Filtering2. Reference: URL Filtering Profile, Create a URL Filtering Profile, Updated Certifications for PAN-OS 10.1, Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0) or [Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0)].

Question: 342

What are three valid source or D=destination conditions available as Security policy qualifiers? (Choose three.)

A. Service
B. User
C. Application
D. Address
E. Zone ab

Answer: B,C,E

Explanation:

Three valid source or destination conditions available as Security policy qualifiers are User, Application, and Zone. These qualifiers allow you to define the match criteria for a Security policy rule based on the identity of the user, the application used, and the zone where the traffic originates or terminates. You can use these qualifiers to enforce granular security policies that control access to network resources and prevent threats1. Some of the characteristics of these qualifiers are:

User: The User qualifier allows you to specify the source or destination user or user group for a Security policy rule. The firewall can identify users based on various methods, such as User-ID, Captive Portal, or GlobalProtect. You can use the User qualifier to apply different security policies for different users or user groups, such as allowing access to certain applications or resources based on user roles or privileges2.

Application: The Application qualifier allows you to specify the application or application group for a Security policy rule. The firewall can identify applications based on App-ID, which is a technology that classifies applications based on multiple attributes, such as signatures, protocol decoders, heuristics, and SSL decryption. You can use the Application qualifier to allow or deny access to specific applications or application groups, such as enabling web browsing but blocking social networking or file sharing3.

Zone: The Zone qualifier allows you to specify the source or destination zone for a Security policy rule. A zone is a logical grouping of one or more interfaces that have similar functions or security requirements. The firewall can apply security policies based on the zones where the traffic originates or terminates, such as intrazone, interzone, or universal. You can use the Zone qualifier to segment your network and isolate traffic based on different trust levels or network functions4.

Reference: Security Policy, Zones, User-ID, App-ID, Certifications - Palo Alto Networks, [Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0)] or [Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0)].

Question: 343

In which three places on the PAN-OS interface can the application characteristics be found? (Choose three.)

A. Objects tab > Application Filters

B. Policies tab > Security

C. ACC tab > Global Filters

D. Objects tab > Application Groups

E. Objects tab > Applications

Answer: A,D,E

Explanation:

The application characteristics can be found in three places on the PAN-OS interface: Objects tab > Application Filters, Objects tab > Application Groups, and Objects tab > Applications. These places allow you to view and manage the applications and application groups that are used in your Security policy rules. You can also create custom applications and application filters based on various attributes, such as category, subcategory, technology, risk, and behavior1. Some of the characteristics of these places are:

Objects tab > Application Filters: An application filter is a dynamic object that groups applications based on specific criteria. You can use an application filter to match multiple applications in a Security policy rule without having to list them individually. For example, you can create an application filter that includes all applications that have a high risk level or use peer-to-peer technology.

Objects tab > Application Groups: An application group is a static object that groups applications based on your custom requirements. You can use an application group to match multiple applications in a Security policy rule without having to list them individually. For example, you can create an application group that includes all applications that are related to a specific business function or project.

Objects tab > Applications: An application is an object that identifies and classifies network traffic based on App-ID, which is a technology that uses multiple attributes to identify applications. You can use an application to match a specific application in a Security policy rule and control its access and behavior. For example, you can use an application to allow web browsing but block file sharing or social networking.

Reference: Objects, [Application Filters], [Application Groups], [Applications], Updated Certifications for PAN-OS 10.1, Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0) or [Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0)].

Question: 344

An administrator wants to reference the same address object in Security policies on 100 Panorama managed firewalls, across 10 device groups and five templates.
Which configuration action should the administrator take when creating the address object?

A. Ensure that the Shared option is checked.

B. Ensure that the Shared option is cleared.

C. Ensure that Disable Override is cleared.

D. Tag the address object with the Global tag.

Answer: A

Explanation:

To reference the same address object in Security policies on 100 Panorama-managed firewalls, across 10 device groups and five templates, the administrator should ensure that the Shared option is checked when creating the address object. This option allows the administrator to create a shared address object that is available to all device groups and templates on Panorama. The shared address object can then be used in multiple firewall policy rules, filters, and other functions1. This reduces the complexity and duplication of managing address objects across multiple firewalls2. Reference: Address Objects, Create a Shared Address Object, Certifications - Palo Alto Networks, Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0) or [Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0)].

Question: 345

What are three configurable interface types for a data-plane ethernet interface? (Choose three.)

A. Layer 3

B. HSCI

C. VWire

D. Layer 2

E. Management

Answer: A,C,D

Explanation:

Three configurable interface types for a data-plane ethernet interface are Layer 3, VWire, and Layer 2. These interface types determine how the firewall processes traffic and applies security policies. Some of the characteristics of these interface types are:

Layer 3: A layer 3 interface allows the firewall to act as a router and participate in the network routing. The firewall can send and receive traffic from a layer 3 interface and apply security policies and inspect the traffic based on the source and destination IP addresses and zones of the interface1.

VWire: A virtual wire interface allows the firewall to transparently pass traffic between two network segments without modifying the packets or affecting the routing. The firewall can still apply security policies and inspect the traffic based on the source and destination zones of the virtual wire2.

Layer 2: A layer 2 interface allows the firewall to act as a switch and forward traffic based on MAC addresses. The firewall can send and receive traffic from a layer 2 interface and apply security policies and inspect the traffic based on the source and destination zones of the interface3.

Reference: Ethernet Interface Types, Virtual Wire Interfaces, Layer 2 Interfaces, Layer 3 Interfaces, [Certifications - Palo Alto Networks], [Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0)] or [Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0)].

Question: 346

Where does a user assign a tag group to a policy rule in the policy creation window?

A. Application tab
B. General tab
C. Actions tab
D. Usage tab

Answer: B

Explanation:

A user can assign a tag group to a policy rule in the policy creation window by selecting the General tab. A tag group is a collection of tags that can be used to identify and filter policy rules based on different criteria, such as function, location, or priority. A user can create a tag group on Panorama and assign it to a policy rule to apply the same set of tags to multiple firewalls or device groups1. To assign a tag group to a policy rule, the user needs to:

Select the General tab in the policy creation window.

Click the Tag Group drop-down menu and select the tag group that the user wants to assign to the policy rule.

Click OK to save the changes. The policy rule will inherit the tags from the tag group and display them in the Tag column.

Reference: Assign a Tag Group to a Policy Rule, Policy, Certifications - Palo Alto Networks, Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0) or [Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0)].

Question: 347

Which policy set should be used to ensure that a policy is applied just before the default security rules?

A. Parent device-group post-rulebase

B. Child device-group post-rulebase

C. Local Firewall policy

D. Shared post-rulebase

Answer: D

Explanation:

The policy set that should be used to ensure that a policy is applied just before the default security rules is the shared post-rulebase. The shared post-rulebase is a set of Security policy rules that are defined on Panorama and apply to all firewalls or device groups. The shared post-rulebase is

evaluated after the local firewall policy and the child device-group post-rulebase, but before the default security rules. The shared post-rulebase can be used to enforce common security policies across multiple firewalls or device groups, such as blocking high-risk applications or

traffic1. Reference: Security Policy Rule Hierarchy, Security Policy Rulebase, Certifications - Palo Alto Networks, Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0) or [Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0)].

Question: 348

In which two types of NAT can oversubscription be used? (Choose two.)

A. Static IP
B. Destination NAT
C. Dynamic IP and Port (DIPP)
D. Dynamic IP

Answer: C,D

Explanation:

Oversubscription is a feature that allows you to use more private IP addresses than public IP addresses for NAT. This means that multiple private IP addresses can share the same public IP address, as long as they use different ports. Oversubscription can be used in two types of NAT: Dynamic IP and Port (DIPP) and Dynamic IP. DIPP NAT translates both the source IP address and the source port number of the outgoing packets, and can have an oversubscription rate greater than 1. Dynamic IP NAT translates only the source IP address of the outgoing packets, and can have an oversubscription rate of 1 or less. Static IP and Destination NAT do not support oversubscription, as they require a one-to-one mapping between the private and public IP addresses. Reference: Source NAT, Configure NAT, NAT

Question: 349

Where in the PAN-OS GUI can an administrator monitor the rule usage for a specified period of time?

A. Objects > Schedules
B. Policies > Policy Optimizer
C. Monitor > Packet Capture
D. Monitor > Reports

Explanation:

Answer: B

The Policy Optimizer is a feature in the PAN-OS GUI that allows an administrator to monitor the rule usage for a specified period of time, as well as optimize the security policies based on the traffic logs and recommendations. The Policy Optimizer can help the administrator to improve the security posture, reduce the attack surface, and simplify the policy management. The Policy Optimizer can be accessed from Policies > Policy Optimizer in the PAN-OS GUI. Reference: Policy

Optimizer, View Policy Rule Usage, Updated Certifications for PAN-OS 10.1

Question: 350

Which security profile should be used to classify malicious web content?

A. URL Filtering
B. Antivirus
C. Web Content
D. Vulnerability Protection

Answer: A

Explanation:

URL Filtering is a security profile that allows you to classify web content based on the URL category and reputation of the website. URL Filtering can help you block access to malicious web content, such as phishing, malware, or command and control sites, as well as enforce acceptable use policies for web browsing. URL Filtering uses the PAN-DB cloud service to provide up-to-date information on the URL categories and reputations of millions of websites. You can configure URL Filtering policies to allow, block, alert, continue, or override web requests based on the URL category and reputation, as well as customize the response pages and exceptions for different user groups. Reference: URL Filtering, Set Up a Basic Security Policy, Updated Certifications for PAN-OS 10.1

Question: 351

In order to attach an Antivirus, Anti-Spyware and Vulnerability Protection security profile to your Security Policy rules, which setting must be selected?

A. Policies > Security >Actions Tab > Select Group-Profiles as Profile Type
B. Policies > Security >Actions Tab > Select Default-Profiles as Profile Type
C. Policies > Security >Actions Tab > Select Profiles as Profile Type
D. Policies > Security >Actions Tab > Select Tagged-Profiles as Profile Type

Answer: C

Explanation:

To enable the firewall to scan the traffic that it allows based on a Security policy rule, you must also attach Security Profiles —including URL Filtering, Antivirus, Anti-Spyware, File Blocking, and WildFire Analysis—to each rule. To attach a Security Profile to a Security policy rule, you must select Profiles as the Profile Type in the Actions tab of the rule. This allows you to choose from the predefined or custom Security Profiles that you have configured. Group-Profiles, Default-Profiles, and Tagged- Profiles are not valid options for attaching Security Profiles to Security policy rules. Reference: Set

Question: 352

Within a WildFire Analysis Profile, what match criteria can be defined to forward samples for analysis?

A. Application Category
B. Source
C. File Size
D. Direction

Answer: D

Explanation:

A WildFire Analysis Profile allows you to specify which files or email links to forward for WildFire analysis based on the application, file type, and transmission direction (upload or download) of the traffic. The direction match criteria determines whether the file or email link was sent from the source zone to the destination zone (upload) or from the destination zone to the source zone (download). You can also select both directions to forward files or email links regardless of the direction of the traffic. Reference: Security Profile: Wildfire Analysis, Objects > Security Profiles > WildFire Analysis

Question: 353

What must first be created on the firewall for SAML authentication to be configured?

A. Server Policy
B. Server Profile
C. Server Location
D. Server Group

Answer: B

Explanation:

A server profile identifies the external authentication service and instructs the firewall on how to connect to that authentication service and access the authentication credentials for your users. To configure SAML authentication, you must create a server profile and register the firewall and the identity provider (IdP) with each other. You can import a SAML metadata file from the IdP to automatically create a server profile and populate the connection, registration, and IdP certificate information. Reference: Configure SAML Authentication, Set Up SAML Authentication, Introduction to SAML

Question: 354

Which two options does the firewall use to dynamically populate address group members? (Choose two.)

A. IP Addresses
B. Tags
C. MAC Addresses
D. Tag-based filters

Answer: B,D

Explanation:

A dynamic address group populates its members dynamically using look ups for tags and tag-based filters. Tags are metadata elements or attribute-value pairs that are registered for each IP address. Tag-based filters use logical and and or operators to match the tags and determine the membership of the dynamic address group. For example, you can create a dynamic address group that includes all IP addresses that have the tags “web-server” and “linux”. You can also use static tags as part of the filter criteria. Reference: Policy Object: Address Groups, Use Dynamic Address Groups in Policy, Statics vs. Dynamic Address Objects Groups

Question: 355

What two actions can be taken when implementing an exception to an External Dynamic List? (Choose two.)

A. Exclude an IP address by making use of wildcards.
B. Exclude a URL entry by making use of regular expressions.
C. Exclude an IP address by making use of regular expressions.
D. Exclude a URL entry by making use of wildcards.

Answer: A,B

Explanation:

Question: 356

Which feature enables an administrator to review the Security policy rule base for unused rules?

A. Security policy tags

B. Test Policy Match

C. View Rulebase as Groups

D. Policy Optimizer

Answer: D

Explanation:

The Policy Optimizer feature enables an administrator to review the Security policy rule base for unused rules, unused applications, and shadowed rules. The Policy Optimizer provides information and recommendations to help optimize the Security policy rules and reduce the attack surface. The Policy Optimizer can also identify rules that can be converted to use App-ID instead of port-based criteria12. Reference: Policy Optimizer, Tips & Tricks: How to Identify Unused Policies on a Palo Alto Networks Device

Question: 357

An administrator should filter NGFW traffic logs by which attribute column to determine if the entry is for the start or end of the session?

A. Receive Time
B. Type
C. Destination
D. Source

Answer: B

Explanation:

The Type attribute column in the NGFW traffic logs indicates whether the log entry is for the start or end of the session. The possible values are START, END, DROP, DENY, and INVALID. The START value means that the log entry is for the start of the session, and the END value means that the log entry is for the end of the session. The other values indicate that the session was terminated by the firewall for various reasons12. Reference: Traffic Log Fields, Session Log Best Practices

Question: 358

Which CLI command will help confirm if FQDN objects are resolved in the event there is a shadow rule?

A. >show system fqdn
B. >request fqdn show system
C. >request show system fqdn
D. >request system fqdn show

Answer: A

Explanation:

The show system fqdn command displays the FQDN objects configured on the firewall and their resolved IP addresses. This can help confirm if the FQDN objects are resolved correctly and if they match the expected traffic. A shadow rule is a rule that is never matched because a preceding rule covers the same traffic. If a shadow rule uses FQDN objects, it is possible that the FQDN objects are not resolved or have different IP addresses than the traffic, causing the rule to be ineffective.

Question: 359

In the PAN-OS Web Interface, which is a session distribution method offered under NAT Translated Packet Tab to choose how the firewall assigns sessions?

A. Destination IP Hash b

B. Concurrent Sessions

C. Max Sessions

D. IP Modulo

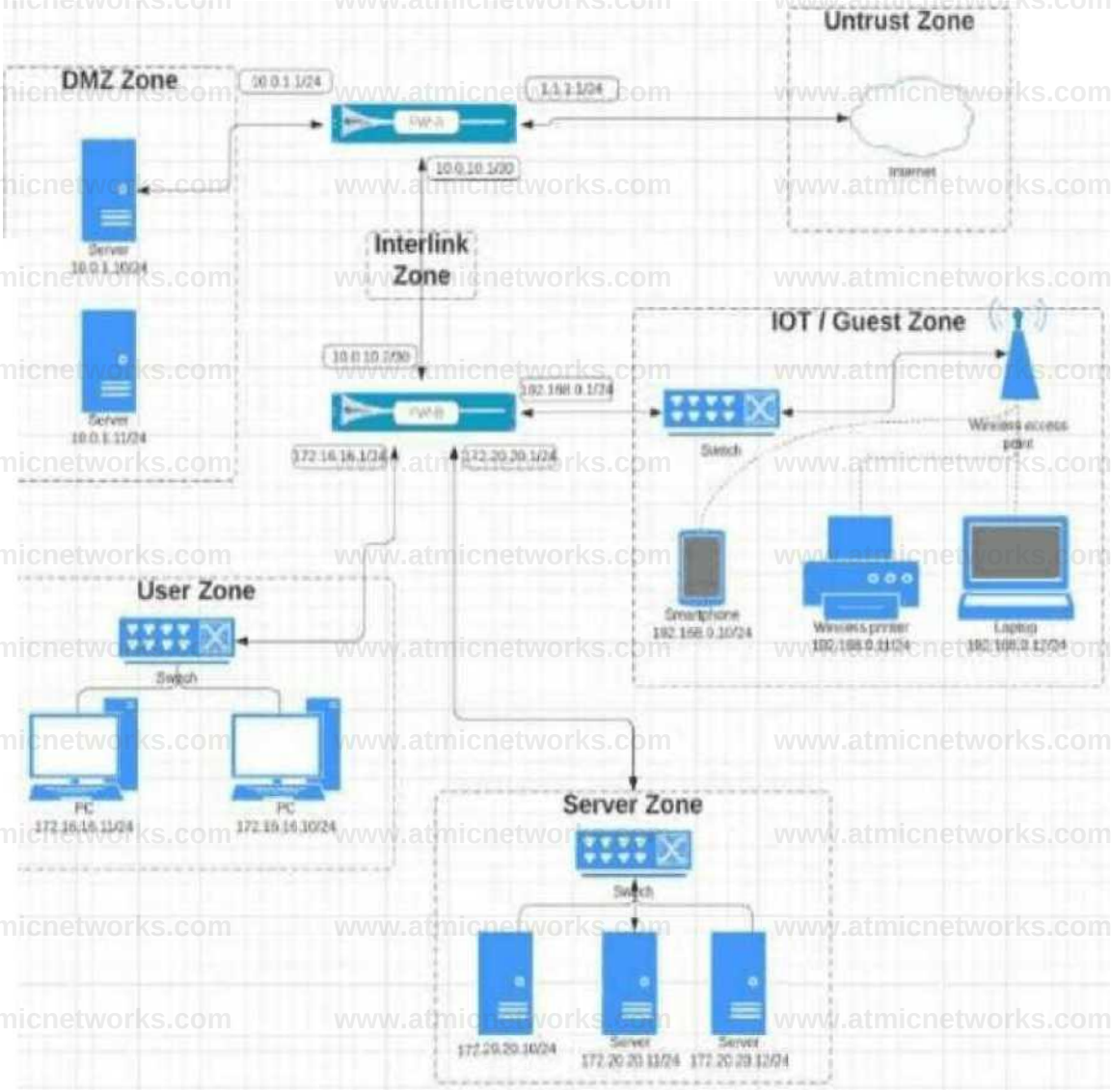
Answer: D

Explanation:

The IP Modulo session distribution method assigns sessions to dataplane processors (DPs) based on the modulo of the source and destination IP addresses. This method is suitable for environments that use NAT with a large number of translated IP addresses and ports. It ensures that sessions with the same source and destination IP addresses are processed by the same DP, regardless of the port numbers. This can improve performance and avoid out-of-order packets.

Question: 360

Review the Screenshot:



Given the network diagram, traffic must be permitted for SSH and MYSQL from the DMZ to the SERVER zones, crossing two firewalls. In addition, traffic should be permitted from the

SERVER zone to the DMZ on SSH only.

Which rule group enables the required traffic?

A)

			Sorer				DoRkaMn							
KAMI	TAGS	I TYPE	ZONE	ADDRESS	USER	DEVICE	IONE	ADO MISS	DEVICE	N	APPLICATIO	SERVICE	URI CATEGORY	ACTION
WA WeGrumsOJ-W		uniters*	RDM?	^auM.–	W		RIMKUVt	giMUCM.	R		a I>R* g cm	a WRMOa-RWI	MT	0 AR#
W^RukGwTOX		untwnl	RIMrtjM	^ 10CXOG4	R	R	RSMW	^17220X0 0/24			8 mu B®	a sawessen dRutt	MT	G**ow
FWX MeGnwO?-Y		«rtw«sa R		5 injfiJBJM*	R		RDM	5 1Q0X0/24	R		BR	awtamiMRa		
IW B RJe&oupCZZ		untvars*	R Sonar	^1722020 0/24	MV		RMsUr*	^AMAM	R		a an	£ AOOKitiwuJefiiR		0NR

B)

				Scarce				DesonoRn					
NAME	TAGS	TYRE	ZONE	ADDRESS	UMI	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATIO N	SERVICE	URL CATEGORY	ACTION
fW A .RuTGmKHjJ W		unrYPi*	ROMZ	SB^	R	R	R sew	1722020.0/2"	1 MV	©ww ®R	a »P5< rxr «<MS		
FVV 8 .RRGcutHIXX	ESI	uNvers*	Row	^IOOiQ'24	R		Ricw	^ 1722020.0/2"	1 R	BR* a "	a ARpIKaQan ATault	R	0 ARCW
FW-A. UlGwOI-V		iWversN	RSrrwt	BI 72JO 20 OXA	R	R	Rwa	^ Kill LOTH	R	B1*	a ARf*c*aon<«S»u"	R	OARS
FW B RIZKlWD C2 2		urn WHO	Rs»	Ep 17X20X00.24	R	W	RDW	IOLQ. 1XU24	R	©«•	a «ettM»we»uH	R	QAR.

C)

				Sourer				DcitinMMWi				
NAME	TAGS	TYRE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DOME	APPLICATION	SERVICE	ACTION
rw A ItosGrouo-O4W		untversl	RDM?	^10010/24	R	am	RStm	51™»™	R	a **R BR	a sooEunendefautt R	©AR.
FW-B BRGailHXX	E3	urVverui	RMWLMI	^ UUU.W24	R	R	R5W	^17220 20 0/24	R	a nR B*	a wtXtsncn Gerjun R	
FW-A IM&GIW-04Y		uiVverui	R Sever	^172X2 20 0/24	R	R	RDMZ	^10.0X0/34	R	81*1	a scptaiDcn GcTauH	©RM
FW-B RcCAUJ>-M-Z		uni verm	R5RV	^172 2020 0/24	R		R IntottM	S WUW4	R	a**	a ;»p«ut'on default R	

D)

			towns				Owaruoon				
NAMI	TAGS	TV»f	low	ADDRESS	USER	DEvrCl	low	ADDRESS	MVKB	A RPC IC AT ION	SERVICE
FW-* Itoe&o«pO!W	CD		unMna RDMI	QUIUM.	„	.		^KUMUa W		B e/pW g»m	a—-^Twwt R
FW-B IEuleGroup4M X		i	univetM R irwn «		R 1		Rtenw	^ I72.70X00/24 R		BRR gsm	a«™ R 0AJR
FW-A RuleG«ksKH -V			iiniwrMI RIiIWM	^loawwio	R		RDMZ			B«*	»R*«** R @Mw
fW-B .RUetko up-01 -Z		I	univRrU R5»w	517220 20 0^4			RnwtM	6 BUMMSO R		a iM	4l«TiUlt

A. Option A

B. Option B

C. Option C

D. Option D

Answer: B

Explanation:

Option B enables the required traffic by allowing SSL and web-browsing from UNTRUST to DMZ, denying SSH from UNTRUST to DMZ, allowing MYSQL from DMZ to SERVER, and allowing SSH from SERVER to DMZ. Option A allows SSH from UNTRUST to DMZ, which is not required. Option C denies all the required traffic. Option D denies all traffic from UNTRUST to TRUST, which is irrelevant to the question

https://www.paloaltonetworks.com/services/education/palo-alto-networks-certified-network- security-administrator

Question: 361

Which action should be taken to identify threats that have been detected by using inline cloud analysis?

A. Filter Threat logs by Type

B. Filter Threat logs by Action

C. Filter Threat logs by Application

D. Filter Threat logs by Threat Category

Answer: B

Explanation:

To identify threats detected by inline cloud analysis, you should filter the Threat logs by Action. This helps in pinpointing the specific actions taken by the firewall in response to detected threats, allowing for a more focused analysis of how threats were handled.

Reference:

Filtering Threat Logs by Action: "Filter Threat logs by Action" .

Question: 362

With Strata Cloud Manager (SCM) or Panorama, customers can monitor and manage which three solutions? (Choose three.)

A. Prisma Access

B. Prisma Cloud

C. Cortex XSIAM

D. NGFW

E. Prisma SD-WAN

Answer: A,D,E

Explanation:

Prisma Access (Answer A):

Strata Cloud Manager (SCM) and Panorama provide centralized visibility and management for Prisma Access, Palo Alto Networks' cloud-delivered security platform for remote users and branch offices.

NGFW (Answer D):

Both SCM and Panorama are used to manage and monitor Palo Alto Networks Next-Generation Firewalls (NGFWs) deployed in on-premise, hybrid, or multi-cloud environments.

Prisma SD-WAN (Answer E):

SCM and Panorama integrate with Prisma SD-WAN to manage branch connectivity and security, ensuring seamless operation in an SD-WAN environment.

Why Not B:

Prisma Cloud is a distinct platform designed for cloud-native security and is not directly managed through Strata Cloud Manager or Panorama.

Why Not C:

Cortex XSIAM (Extended Security Intelligence and Automation Management) is part of the Cortex platform and is not managed by SCM or Panorama.

Reference from Palo Alto Networks Documentation:

Strata Cloud Manager Overview

Question: 363

According to a customer's CIO, who is upgrading PAN-OS versions, "Finding issues and then engaging with your support people requires expertise that our operations team can better utilize elsewhere on more valuable tasks for the business." The upgrade project was initiated in a rush because the company did not have the appropriate tools to indicate that their current NGFWs were reaching capacity.

Which two actions by the Palo Alto Networks team offer a long-term solution for the customer? (Choose two.)

A. Recommend that the operations team use the free machine learning-powered AIOps for NGFW tool.

B. Suggest the inclusion of training into the proposal so that the operations team is informed and confident in working on their firewalls.

C. Inform the CIO that the new enhanced security features they will gain from the PAN-OS upgrades will fix any future problems with upgrading and capacity.

D. Propose AIOps Premium within Strata Cloud Manager (SCM) to address the company's issues from within the existing technology.

Answer: B,D

Explanation:

The customer's CIO highlights two key pain points: (1) the operations team lacks expertise to efficiently manage PAN-OS upgrades and support interactions, diverting focus from valuable tasks, and (2) the company lacked tools to monitor NGFW capacity, leading to a rushed upgrade. The goal is to recommend long-term solutions leveraging Palo Alto Networks' offerings for Strata Hardware Firewalls. Options B and D—training and AIOps Premium within Strata Cloud Manager (SCM)—address these issues by enhancing team capability and providing proactive management tools. Below is a detailed explanation, verified against official documentation.

Step 1: Analyzing the Customer's Challenges

Expertise Gap: The CIO notes that identifying issues and engaging support requires expertise the operations team doesn't fully have or can't prioritize. Upgrading PAN-OS on Strata NGFWs involves tasks like version compatibility checks, pre-upgrade validation, and troubleshooting, which demand familiarity with PAN-OS tools and processes.

Capacity Visibility: The rushed upgrade stemmed from not knowing the NGFWs were nearing capacity (e.g., CPU, memory, session limits), indicating a lack of monitoring or predictive analytics.

Long-term solutions must address both operational efficiency and proactive capacity management, aligning with Palo

Alto Networks' ecosystem for Strata firewalls.

Reference: PAN-OS Administrator's Guide (11.1) - Upgrade Overview

"Successful upgrades require planning, validation, and monitoring to avoid disruptions and ensure capacity is sufficient."

Step 2: Evaluating the Recommended Actions

Option A: Recommend that the operations team use the free machine learning-powered AIOps for NGFW tool.

Analysis: AIOps for NGFW (free version) is a cloud-based tool that uses machine learning to monitor firewall health, detect anomalies, and provide upgrade recommendations. It offers basic telemetry (e.g., CPU usage, session counts) and alerts, which could have flagged capacity issues earlier. However, it lacks advanced features like automated remediation, detailed capacity planning, or integration with Strata Cloud Manager, limiting its long-term impact. Additionally, it doesn't address the expertise gap, as the team still needs knowledge to interpret and act on insights.

Conclusion: Helpful but not a comprehensive long-term solution.

Reference: AIOps for NGFW Documentation

"The free version provides basic health monitoring and ML-driven insights but lacks premium features for proactive management."

Option B: Suggest the inclusion of training into the proposal so that the operations team is informed and confident in working on their firewalls.

Analysis: Palo Alto Networks offers training through the Palo Alto Networks Authorized Training Partners and Cybersecurity Academy, covering PAN-OS administration, upgrades, and troubleshooting. For Strata NGFWs, courses like "Firewall Essentials: Configuration and Management (EDU-210)" teach upgrade best practices, capacity monitoring (e.g., via Device > High Availability > Resources), and support engagement.

How It Solves the Issue:

Reduces reliance on external expertise by upskilling the team.

Enables efficient upgrade planning (e.g., using Best Practice Assessment (BPA) tool).

Frees the team for higher-value tasks by minimizing support escalations.

Long-Term Benefit: A trained team can proactively manage upgrades and capacity, addressing the CIO's concern about expertise allocation.

Conclusion: A strong long-term solution.

Reference: Palo Alto Networks Training Catalog

"Training empowers operations teams to confidently manage NGFWs, including upgrades and capacity planning."

Option C: Inform the CIO that the new enhanced security features they will gain from the PAN-OS upgrades will fix any future problems with upgrading and capacity.

Analysis: New PAN-OS versions (e.g., 11.1) bring features like enhanced App-ID, decryption, or ML- based threat detection, improving security. However, these don't inherently solve upgrade complexity or capacity visibility. Capacity issues depend on hardware limits (e.g., PA-5200 Series max sessions), not software features, and upgrades still require expertise. This response oversells benefits without addressing root causes.

Conclusion: Not a valid long-term solution.

Reference: PAN-OS 11.1 Release Notes

"New features enhance security but do not automate upgrade processes or capacity monitoring."

Option D: Propose AIOps Premium within Strata Cloud Manager (SCM) to address the company's issues from within the existing technology.

Analysis: AIOps Premium, integrated with Strata Cloud Manager (SCM), is a subscription-based service for managing Strata NGFWs. It provides:

Predictive Analytics: Forecasts capacity needs (e.g., CPU, memory, sessions) using ML.

Upgrade Planning: Recommends optimal upgrade paths and validates configurations.

Proactive Alerts: Identifies issues before they escalate, reducing support calls.

Centralized Management: Monitors all firewalls from SCM, integrating with existing PAN-OS deployments.

How It Solves the Issue:

Prevents rushed upgrades by predicting capacity limits (e.g., via Capacity Saturation Reports).

Simplifies upgrade preparation with automated insights, reducing expertise demands.

Aligns with existing Strata technology, enhancing ROI.

Long-Term Benefit: Offers a scalable, proactive toolset to manage NGFWs, addressing both capacity and operational efficiency.

Conclusion: A robust long-term solution.

Reference: Strata Cloud Manager AIOps Premium Documentation

"AIOps Premium provides advanced capacity planning and upgrade readiness, minimizing operational burden."

Step 3: Why B and D Are the Best Choices

B (Training): Directly tackles the expertise gap, empowering the team to handle upgrades and capacity monitoring

independently. It's a foundational fix, ensuring long-term self-sufficiency.

D (AIOps Premium in SCM): Provides a technological solution to preempt capacity issues and streamline upgrades, reducing the need for deep expertise and support escalations. It complements training by automating complex tasks.

Synergy: Together, they address both human (expertise) and systemic (tools) challenges, aligning with the CIO's goals of operational efficiency and business value.

Step 4: How These Actions Integrate with Strata NGFWs

Training: Teaches use of PAN-OS tools like System Resources (CLI: show system resources) and Dynamic Updates for capacity and upgrade prep.

AIOps Premium: Enhances Strata NGFW management via SCM, pulling telemetry (e.g., from Device > Setup > Telemetry) to predict and resolve issues.

Reference: PAN-OS Administrator's Guide (11.1) - Monitoring

"Combine training and tools like AIOps to optimize NGFW performance and upgrades."

Question: 364

A systems engineer (SE) successfully demonstrates NGFW managed by Strata Cloud Manager (SCM) to a company. In the resulting planning phase of the proof of value (POV), the CISO requests a test

that shows how the security policies are either meeting, or are progressing toward meeting, industry standards such as Critical Security Controls (CSC), and how the company can verify that it is effectively utilizing the functionality purchased.

During the POV testing timeline, how should the SE verify that the POV will meet the CISO's request?

A. Near the end, pull a Security Lifecycle Review (SLR) in the POV and create a report for the customer.

B. At the beginning, work with the customer to create custom dashboards and reports for any information required, so reports can be pulled as needed by the customer.

C. Near the end, the customer pulls information from these SCM dashboards: Best Practices, CDSS Adoption, and NGFW Feature Adoption.

D. At the beginning, use PANhandler golden images that are designed to align to compliance and to turning on the features for the CDSS subscription being tested.

Answer: B

Explanation:

The SE has demonstrated an NGFW managed by SCM, and the CISO now wants the POV to show progress toward industry standards (e.g., CSC) and verify effective use of purchased features (e.g., CDSS subscriptions like Advanced Threat Prevention). The SE must ensure the POV delivers measurable evidence during the testing timeline. Let's evaluate the options.

Step 1: Understand the CISO's Request

Industry Standards (e.g., CSC): The Center for Internet Security's Critical Security Controls (e.g., CSC 1: Inventory of Devices, CSC 4: Secure Configuration) require visibility, threat prevention, and policy enforcement, which NGFW and SCM can address.

Feature Utilization: Confirm that licensed functionalities (e.g., App-ID, Threat Prevention, URL Filtering) are active and effective.

POV Goal: Provide verifiable progress and utilization metrics within the testing timeline.

Reference: Strata Cloud Manager Overview (docs.paloaltonetworks.com/strata-cloud-manager); CIS Critical Security Controls (www.cisecurity.org/controls).

Step 2: Define SCM Capabilities

Strata Cloud Manager (SCM): A cloud-based management platform for Palo Alto NGFWs, offering dashboards (e.g., Best Practices, Feature Adoption) and custom reporting to monitor security
posture, policy compliance, and subscription usage.

Security Lifecycle Review (SLR): A report generated via the Customer Support Portal (not SCM) analyzing traffic logs for security gaps, not real-time POV progress.

Dashboards and Reports: SCM provides prebuilt and customizable views for real-time insights into policy effectiveness and feature adoption.

Reference: SCM Dashboards and Reports (docs.paloaltonetworks.com/strata-cloud- manager/dashboards-and-reports).

Step 3: Evaluate Each Option

A . Near the end, pull a Security Lifecycle Review (SLR) in the POV and create a report for the customer.

Description: The SLR analyzes 7-30 days of traffic logs, providing a retrospective security posture assessment (e.g., threats blocked, policy gaps).

Process: Near POV end, upload logs to the Customer Support Portal (Support > Security Lifecycle Review), generate, and

share the report.

Limitations:

SLR is a point-in-time analysis, not a real-time progress tracker during the POV timeline.

Requires post-POV log collection, delaying feedback.

Doesn't directly show feature utilization progress or CSC alignment in SCM.

Fit: Misses the "during the POV timeline" requirement; better for post-POV analysis.

Reference: Security Lifecycle Review Guide (support.paloaltonetworks.com, requires login).

B . At the beginning, work with the customer to create custom dashboards and reports for any information required, so reports can be pulled as needed by the customer.

Description: SCM allows custom dashboards and reports (Monitor > Dashboards or Reports) tailored to metrics like policy compliance (CSC alignment) and feature usage (e.g., Threat Prevention hits).

Process:

At POV start, collaborate with the CISO to define metrics (e.g., "Threats blocked by ATP" for CSC 6, "App-ID usage" for feature adoption).

Configure custom dashboards in SCM (Dashboards > Add Dashboard > Custom).

Set up scheduled or on-demand reports (Reports > Custom Reports).

Enable the customer to monitor progress throughout the POV.

Benefits:

Real-time visibility into policy effectiveness and feature use during the timeline.

Aligns with CSC (e.g., blocked malware events) and shows subscription ROI.

Empowers the customer to verify results independently.

Fit: Meets the CISO's request fully within the POV timeline.

Reference: SCM Custom Dashboards (docs.paloaltonetworks.com/strata-cloud-manager/dashboards- and-reports/custom-dashboards).

C . Near the end, the customer pulls information from these SCM dashboards: Best Practices, CDSS Adoption, and NGFW Feature Adoption.

Description: SCM provides prebuilt dashboards:

Best Practices: Assesses policy alignment with security standards.

CDSS Adoption: Tracks subscription usage (e.g., ATP, URL Filtering).

NGFW Feature Adoption: Monitors features like App-ID or User-ID.

Limitations:

Waiting until "near the end" delays visibility, missing ongoing progress tracking.

Prebuilt dashboards may not fully align with CSC or specific customer needs without customization.

Fit: Useful but incomplete; lacks proactive setup and real-time monitoring throughout the POV.

Reference: SCM Prebuilt Dashboards (docs.paloaltonetworks.com/strata-cloud- manager/dashboards-and-reports/prebuilt-dashboards).

D . At the beginning, use PANhandler golden images that are designed to align to compliance and to turning on the features for the CDSS subscription being tested.

Description: PANhandler is a tool for managing Skillets (configuration templates), including "golden images" for compliance (e.g., NIST, CIS benchmarks).

Process: Apply a Skillet at POV start to configure the NGFW with compliance settings and CDSS features.

Limitations:

Configures the NGFW but doesn't verify progress or utilization during the POV.

No reporting or dashboard integration for the CISO to track results.

Fit: Sets up the environment but doesn't meet the verification requirement.

Reference: PANhandler Skillets (github.com/PaloAltoNetworks/panhandler).

Step 4: Select the Best Approach

B is the strongest choice:

Proactive: Starts at the beginning, ensuring metrics are tracked throughout the POV.

Customizable: Tailors dashboards/reports to CSC (e.g., threat detection for CSC 6) and feature use (e.g., ATP events).

Verifiable: Enables the customer to pull reports as needed, meeting the CISO's request within the timeline.

Why not A, C, or D?

A: SLR is retrospective, not real-time, missing the "during" aspect.

C: Prebuilt dashboards are helpful but delayed and less flexible than custom options.

D: Golden images configure but don't verify progress or utilization.

Step 5: Verification with Palo Alto Documentation

SCM Custom Dashboards: Supports real-time, tailored monitoring (SCM Docs).

SLR: Post-analysis tool, not POV-progressive (Support Portal Docs).

Prebuilt Dashboards: Limited customization (SCM Docs).

PANhandler: Configuration-focused, not reporting-focused (PANhandler Docs).

Thus, the verified answer is B.

Question: 365

Which two compliance frameworks are included with the Premium version of Strata Cloud Manager (SCM)? (Choose two)

A. Payment Card Industry (PCI)

B. National Institute of Standards and Technology (NIST)

C. Center for Internet Security (CIS)

D. Health Insurance Portability and Accountability Act (HIPAA)

Answer: A,B

Explanation:

Step 1: Understanding Strata Cloud Manager (SCM) Premium

Strata Cloud Manager is a unified management interface for Strata NGFWs, Prisma Access, and other Palo Alto Networks solutions. The Premium version (subscription-based) includes advanced features like:

AIOps Premium: Predictive analytics, capacity planning, and compliance reporting.

Compliance Posture Management: Pre-built dashboards and reports for specific regulatory frameworks.

Compliance frameworks in SCM Premium provide visibility into adherence to standards like PCI DSS and NIST, generating actionable insights and audit-ready reports based on firewall configurations, logs, and traffic data.

Reference: Strata Cloud Manager Documentation

"SCM Premium delivers compliance reporting for industry standards, integrating with NGFW telemetry to ensure regulatory alignment."

Step 2: Evaluating the Compliance Frameworks

Option A: Payment Card Industry (PCI)

Analysis: The Payment Card Industry Data Security Standard (PCI DSS) is a mandatory framework for organizations handling cardholder data. SCM Premium includes a PCI DSS Compliance Dashboard that maps NGFW configurations (e.g., security policies, decryption, Threat Prevention) to PCI DSS requirements (e.g., Requirement 1: Firewall protection, Requirement 6: Vulnerability protection). It tracks compliance with controls like network segmentation, encryption, and monitoring, critical for Strata NGFW deployments in payment environments.

Evidence: Palo Alto Networks emphasizes PCI DSS support in SCM Premium for retail, financial, and e-commerce customers, providing pre-configured reports for audits.

Conclusion: Included in SCM Premium.

Reference: Strata Cloud Manager Premium Features Overview
"PCI DSS compliance reporting ensures cardholder data protection with automated insights."

Option B: National Institute of Standards and Technology (NIST)

Analysis: NIST frameworks, notably the NIST Cybersecurity Framework (CSF) and NIST SP 800-53, are widely adopted for cybersecurity risk management, especially in government and critical infrastructure sectors. SCM Premium offers a NIST Compliance Dashboard, aligning NGFW settings (e.g., App-ID, User-ID, logging) with NIST controls (e.g., Identify, Protect, Detect, Respond, Recover). This is key for Strata customers needing federal compliance or a risk-based approach.

Evidence: Palo Alto Networks documentation highlights NIST CSF and 800-53 mapping in SCM Premium, reflecting its broad applicability.

Conclusion: Included in SCM Premium.

Reference: Strata Cloud Manager AIOps Premium Datasheet

"NIST compliance reporting supports risk management and regulatory adherence."

Option C: Center for Internet Security (CIS)

Analysis: The CIS Controls and Benchmarks provide practical cybersecurity guidelines (e.g., CIS Controls v8, CIS Benchmarks for OS hardening). While Palo Alto Networks supports CIS principles (e.g., via Best Practice Assessments), SCM Premium documentation does not explicitly list a dedicated CIS Compliance Dashboard. CIS alignment is often manual or supplementary, not a prebuilt feature like PCI or NIST.

Evidence: No direct evidence in SCM Premium feature sets confirms CIS as a standard inclusion; it's more commonly referenced in standalone tools like CIS-CAT or Expedition.

Conclusion: Not included in SCM Premium.

Reference: PAN-OS Administrator's Guide (11.1) - Best Practices

"CIS alignment is supported but not a native SCM Premium framework."

Option D: Health Insurance Portability and Accountability Act (HIPAA)

Analysis: HIPAA governs protected health information (PHI) security in healthcare. While Strata NGFWs can enforce HIPAA-compliant policies (e.g., encryption, access control), SCM Premium does not feature a dedicated HIPAA Compliance Dashboard. HIPAA compliance is typically achieved through custom configurations and external audits, not a pre-configured SCM framework.

Evidence: Palo Alto Networks documentation lacks mention of HIPAA as a standard SCM Premium offering, unlike PCI and NIST.

Conclusion: Not included in SCM Premium.

Reference: Strata Cloud Manager Documentation

"HIPAA compliance is supported via NGFW capabilities, not SCM Premium dashboards."

Step 3: Why A and B Are Correct

A (PCI): Directly addresses a common Strata NGFW use case (payment security) with a tailored dashboard, reflecting SCM Premium's focus on industry-specific compliance.

B (NIST): Provides a flexible, widely adopted framework for cybersecurity, integrated into SCM Premium for broad applicability across sectors.

Exclusion of C and D: CIS and HIPAA, while relevant to NGFW deployments, lack dedicated, pre-built compliance reporting in SCM Premium, making them supplementary rather than core inclusions.

Step 4: Verification Against SCM Premium Features

SCM Premium's compliance posture management explicitly lists PCI DSS and NIST (e.g., CSF, 800-53) as supported frameworks, leveraging NGFW telemetry (e.g., Monitor > Logs > Traffic) and AIOps analytics. This aligns with Palo Alto Networks' focus on high-demand regulations as of PAN-OS 11.1 and SCM updates through March 08, 2025.

Reference: Strata Cloud Manager Release Notes (March 2025)

"Premium version includes PCI DSS and NIST compliance dashboards for automated reporting."

Conclusion

The two compliance frameworks included with the Premium version of Strata Cloud Manager are A. Payment Card Industry (PCI) and B. National Institute of Standards and Technology (NIST). These are verified by SCM Premium's documented capabilities, ensuring Strata NGFW customers can meet regulatory requirements efficiently.

Question: 366

Which two products can be integrated and managed by Strata Cloud Manager (SCM)? (Choose two)

A. Prisma SD-WAN

B. Prisma Cloud

C. Cortex XDR

D. VM-Series NGFW

Answer: A,D

Explanation:

Strata Cloud Manager (SCM) is Palo Alto Networks' centralized cloud-based management platform for managing network security solutions, including Prisma Access and Prisma SD-WAN. SCM can also integrate with VM-Series firewalls for managing virtualized NGFW deployments.

Why A (Prisma SD-WAN) Is Correct

SCM is the management interface for Prisma SD-WAN, enabling centralized orchestration, monitoring, and configuration of SD-WAN deployments.

Why D (VM-Series NGFW) Is Correct

SCM supports managing VM-Series NGFWs, providing centralized visibility and control for virtualized firewall deployments in cloud or on-premises environments.

Why Other Options Are Incorrect

B (Prisma Cloud): Prisma Cloud is a separate product for securing workloads in public cloud environments. It is not managed via SCM.

C (Cortex XDR): Cortex XDR is a platform for endpoint detection and response (EDR). It is managed through its own console, not SCM.

Reference:

Palo Alto Networks Strata Cloud Manager Overview

Question: 367

An engineer at a managed services provider is updating an application that allows its customers to request firewall changes to also manage SD-WAN. The application will be able to make any approved changes directly to devices via API.

What is a requirement for the application to create SD-WAN interfaces?

A. REST API's "sdwanInterfaceprofiles" parameter on a Panorama device

B. REST API's "sdwanInterfaces" parameter on a firewall device

C. XML API's "sdwanprofiles/interfaces" parameter on a Panorama device

D. XML API's "InterfaceProfiles/sdwan" parameter on a firewall device

Answer: B

Explanation:

To create SD-WAN interfaces through an API, the correct approach is to use the REST API's "sdwanInterfaces" parameter on a firewall device. This parameter allows you to configure SD-WAN interfaces directly on the firewall devices via API, ensuring that the required interfaces are set up and managed for SD-WAN functionality.

Question: 368

Which two actions in the IKE Gateways will allow implementation of post-quantum cryptography when building VPNs between multiple Palo Alto Networks NGFWs? (Choose two.)

A. Select IKE v2, enable the Advanced Options • PQ PPK, then set a 64+ character string for the postquantum pre shared key.

B. Ensure Authentication is set to "certificate," then import a post-quantum derived certificate.

C. Select IKE v2 Preferred, enable the Advanced Options • PQ KEM, then add one or more "Rounds."

D. Select IKE v2, enable the Advanced Options • PQ KEM, then create an IKE Crypto Profile with Advanced Options adding one or more "Rounds."

Answer: C,D

Explanation:

To implement post-quantum cryptography (PQC) in VPNs between Palo Alto Networks NGFWs, you would enable the PQ KEM (Post-Quantum Key Encapsulation Mechanism) in the IKE gateway configuration. This enables the firewall to use quantum-resistant encryption for key exchange, which is an essential part of securing communications against the potential future threats posed by quantum computing.

By selecting IKE v2 Preferred and enabling the PQ KEM option under Advanced Options, you can add specific Rounds for the post-quantum cryptography process, which will help in implementing quantum-resistant key exchange methods. This option similarly selects IKE v2 and enables PQ KEM while also creating a dedicated IKE Crypto Profile with the necessary Rounds configured for post-quantum cryptography.

Question: 369

An NGFW engineer is establishing bidirectional connectivity between the accounting virtual system (VSYS) and the marketing VSYS. The traffic needs to transition between zones without leaving the firewall (no external physical connections). The interfaces for each VSYS are assigned to separate virtual routers (VRs), and inter-VR static routes have been configured. An external zone has been created correctly for each VSYS. Security policies have been added to permit the desired traffic between each zone and its respective external zone. However, the desired traffic is still unable to successfully pass from one VSYS to the other in either direction.

Which additional configuration task is required to resolve this issue?

A. Create a transit VSYS and route all inter-VSYS traffic through it.

B. Add each VSYS to the list of visible virtual systems of the other VSYS.

C. Enable the “allow inter-VSYS traffic” option in both external zone configurations.

D. Create Security policies to allow the traffic between the two external zones.

Answer: B

Explanation:

In Palo Alto Networks firewalls, each virtual system (VSYS) is typically isolated from other VSYSs, meaning that traffic between different VSYSs cannot pass through the firewall by default. In this case, since the interfaces for each VSYS are assigned to separate virtual routers (VRs), and the desired traffic is still not passing between the two VSYSs, the firewall needs to be explicitly configured to allow traffic between them.

The required configuration is to add each VSYS to the list of visible virtual systems of the other VSYS. This allows inter-VSYS communication to be enabled, effectively permitting the traffic to pass between the zones of different VSYSs.

Question: 370

Without performing a context switch, which set of operations can be performed that will affect the operation of a connected firewall on the Panorama GUI?

A. Restarting the local firewall, running a packet capture, accessing the firewall CLI

B. Modification of local security rules, modification of a Layer 3 interface, modification of the firewall device hostname

C. Modification of pre-security rules, modification of a virtual router, modification of an IKE Gateway Network Profile

D. Modification of post NAT rules, creation of new views on the local firewall ACC tab, creation of local custom reports

Answer: B

Explanation:

In Panorama, without performing a context switch, the administrator can perform local configuration tasks directly on the connected firewall. The following operations can be done:

Modification of local security rules: Security rules can be modified directly on the connected firewall from the Panorama GUI.

Modification of a Layer 3 interface: Changes to the Layer 3 interfaces on the connected firewall can be done from Panorama, without needing to switch to the firewall's local interface.

Modification of the firewall device hostname: The firewall's hostname can be changed via Panorama.

Question: 371

Which set of options is available for detailed logs when building a custom report on a Palo Alto Networks NGFW?

A. Traffic, User-ID, URL

B. Traffic, threat, data filtering, User-ID

C. GlobalProtect, traffic, application statistics

D. Threat, GlobalProtect, application statistics, WildFire submissions

Answer: B

Explanation:

When building a custom report on a Palo Alto Networks NGFW, you can select detailed logs that provide specific insights into various aspects of firewall activity. The available options for detailed logs typically include:

Traffic logs: These provide information on the network traffic passing through the firewall.

Threat logs: These logs capture data related to identified security threats, such as malware or intrusion attempts.

Data filtering logs: These logs capture events related to data filtering policies, such as preventing the transfer of sensitive

data.

User-ID logs: These logs associate user identities with the traffic and activities observed on the firewall, enabling user-based policy enforcement.

Question: 372

An administrator plans to upgrade a pair of active/passive firewalls to a new PAN-OS release. The environment is highly sensitive, and downtime must be minimized.

What is the recommended upgrade process for minimal disruption in this high availability (HA) scenario?

A. Suspend the active firewall to trigger a failover to the passive firewall. With traffic now running on the former passive unit, upgrade the suspended (now passive) firewall and confirm proper operation. Then fail traffic back and upgrade the remaining firewall.

B. Shut down the currently active firewall and upgrade it ofline, allowing the passive firewall to handle all traffic. Once the active firewall finishes upgrading, bring it back online and rejoin the HA cluster. Finally, upgrade the passive firewall while the newly upgraded unit remains active.

C. Isolate both firewalls from the production environment and upgrade them in a separate, ofline setup. Reconnect them only after validating the new software version, resuming HA functionality once both units are fully upgraded and tested.

D. Push the new PAN-OS version simultaneously to both firewalls, having them upgrade and reboot in parallel. Rely on automated HA reconvergence to restore normal operations without manually failing over traffic.

Answer: A

Explanation:

In an active/passive HA setup, the recommended process for upgrading involves minimizing downtime and ensuring traffic continuity by using the failover process:

Suspend the active firewall: This triggers a failover to the passive unit, making it the active unit.

Upgrade the former passive (now active) unit: With traffic now running on the previously passive unit, upgrade the suspended unit while the active unit continues handling traffic.

Confirm proper operation: Once the upgrade is complete, verify that the upgraded unit is functioning properly.

Fail traffic back: Once the upgraded firewall is confirmed to be working, fail the traffic back to the original active unit and upgrade the remaining firewall.