

PCNSA Dumps

Palo Alto Networks Certified Network Security Administrator

<https://www.certleader.com/PCNSA-dumps.html>



NEW QUESTION 1

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

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

Answer: ABD

Explanation:

NEW QUESTION 2

Which Security 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:

NEW QUESTION 3

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

NEW QUESTION 4

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: AD

Explanation:

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

NEW QUESTION 5

DRAG DROP

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

Answer Area

First	Drag answer here	PAN-DB Cloud
Second	Drag answer here	External Dynamic Lists
Third	Drag answer here	Custom URL Categories
Fourth	Drag answer here	Block List
Fifth	Drag answer here	Downloaded PAN-DB File
Sixth	Drag answer here	Allow Lists

Answer:

Answer Area

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 6

When creating a Panorama administrator type of Device Group and Template Admin, which two things must you create first? (Choose two.)

- A. password profile
- B.

access domain

- C. admin role
- D. server profile

Answer: CD

NEW QUESTION 7

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

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

Answer: C

NEW QUESTION 8

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

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

Answer: AC

NEW QUESTION 9

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Cm8SCAS#:~:text=Details,using%20https%20on%20port%204443>

NEW QUESTION 10

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

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

Answer: A

NEW QUESTION 10

What do you configure if you want to set up a group of objects based on their ports alone?

- A. Application groups
- B. Service groups
- C. Address groups
- D. Custom objects

Answer: B

NEW QUESTION 15

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: ABC

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.

NEW QUESTION 19

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

- A. Mastered
- B. Not Mastered

Answer: A

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: URLs learned from External Dynamic Lists (EDLs) - 5) Pre-Defined Categories: PAN-DB or Brightcloud categories.

NEW QUESTION 20

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

- A. interzone
- B. shadowed

- C. intrazone
- D. universal

Answer: A

NEW QUESTION 21

Which two settings allow you to restrict access to the management interface? (Choose two)

- A. Mastered
- B. Not Mastered

Answer: A

NEW QUESTION 25

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

Device SN: 007251000156341 IP Protocol: udp Log Action: global-logs Generated Time: 2021/08/27 02:02:49 Receive Time: 2021/08/27 02:02:53 Tunnel Type: N/A	Interface: ethernet1/4 NAT IP: 67.290.64.58 NAT Port: 26351 X-Forwarded-For IP: 0.0.0.0	NAT IP: 8.8.8.4 NAT Port: 53
Details		Flags
Threat Type: spyware Threat ID/Name: Phishing:151.136.74.in-addr.arpa ID: 109010001 (View in Threat Hunt) Category: dns-phishing Content Version: AppThreat-0-0 Severity: low Repeat Count: 2 File Name: URL: 151.136.74.in-addr.arpa Partial Hash: 0 Prap ID: 0 Source UUID: Destination UUID: Dynamic User Group: Network Slice ID SST: 0 Network Slice ID SD: App Category: networking App Subcategory: infrastructure App Technology: network-protocol App Characteristic: used by malware has known vulnerability pervasive use App Container: App Risk: 3		Captive Portal: <input type="checkbox"/> Proxy Transaction: <input type="checkbox"/> Decrypted: <input type="checkbox"/> Packet Capture: <input type="checkbox"/> Client to Server: <input checked="" type="checkbox"/> Server to Client: <input type="checkbox"/> Tunnel Inspected: <input type="checkbox"/>
DeviceID		Source Device Category: Virtual Machine Source Device Profile: VMware Source Device Model: Source Device Vendor: VMware, Inc. Source Device OS Family: Source Device OS Version: Source Device Host: ubuntu-server Source Device MAC: 00:50:56:a2:19:63 Destination Device Category: Destination Device Profile: Destination Device Model:

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

Answer: C

NEW QUESTION 30

The PowerBall Lottery has reached an unusually high value this week. Your company has decided to raise morale by allowing employees to access the PowerBall Lottery website (www.powerball.com) for just this week. However, the company does not want employees to access any other websites also listed in the URL filtering “gambling” category.

Which method allows the employees to access the PowerBall Lottery website but without unblocking access to the “gambling” URL category?

- A. Add just the URL www.powerball.com to a Security policy allow rule.
- B.

Manually remove powerball.com from the gambling URL category.

- C. Add *.powerball.com to the URL Filtering allow list.
- D. Create a custom URL category, add *.powerball.com to it and allow it in the Security Profile.

Answer: CD

NEW QUESTION 34

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

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

Answer: BC

NEW QUESTION 36

At which point in the app-ID update process can you determine if an existing policy rule is affected by an app-ID update?

- A.

after clicking Check New in the Dynamic Update window

- B. after connecting the firewall configuration
- C. after downloading the update
- D. after installing the update

Answer: A

Explanation:

Reference:<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/device/device-dynamicupdates>

NEW QUESTION 40

Which option is part of the content inspection process?

- A. IPsec tunnel encryption
- B.

Packet egress process

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

Answer: C

NEW QUESTION 41

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

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

Answer: D

NEW QUESTION 43

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

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

Answer: B

NEW QUESTION 48

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

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

Answer: AD

NEW QUESTION 50

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

NEW QUESTION 51

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

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

Answer: BD

Explanation:

NEW QUESTION 55

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:

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

- A. Mastered
- B. Not Mastered

Answer: A

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

NEW QUESTION 56

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
Destination 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)

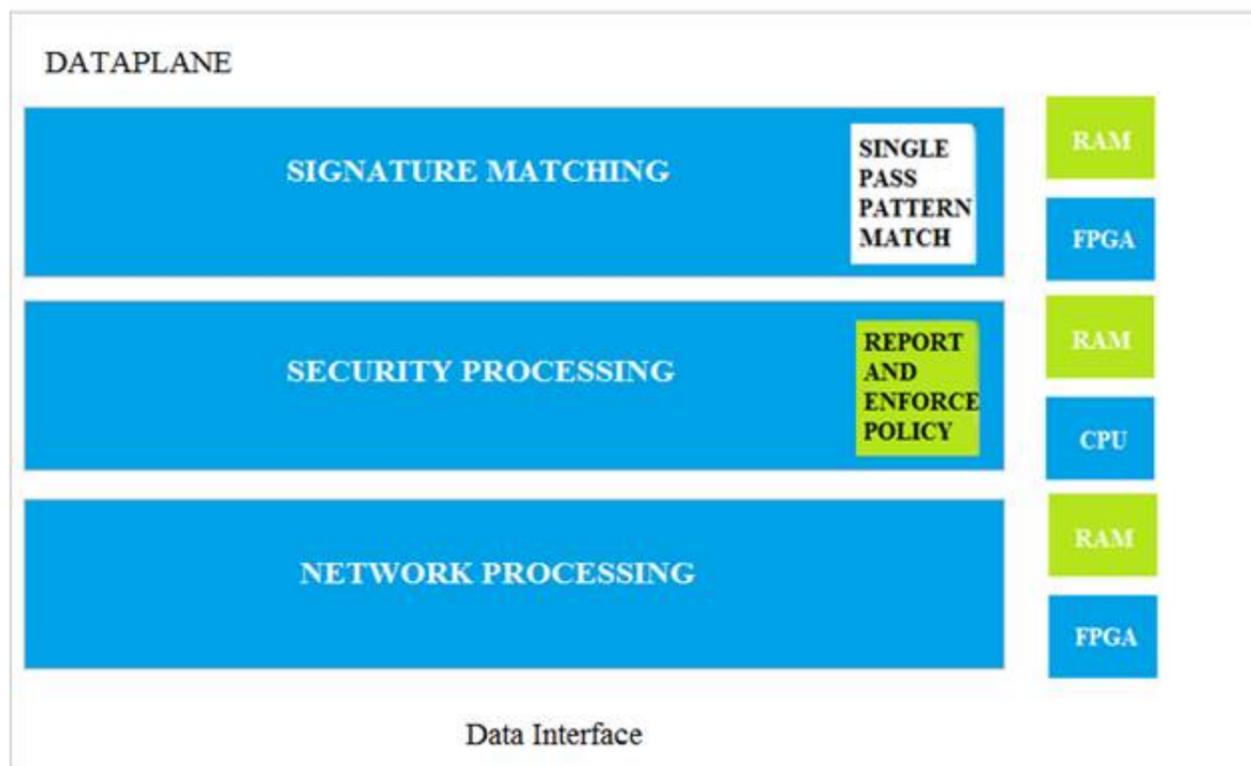
Source Zone: Trusted
Destination Zone: DMZ
Services: Application-Default
Applications: SSH
Action: Allow

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

Answer: D

NEW QUESTION 60

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

NEW QUESTION 62

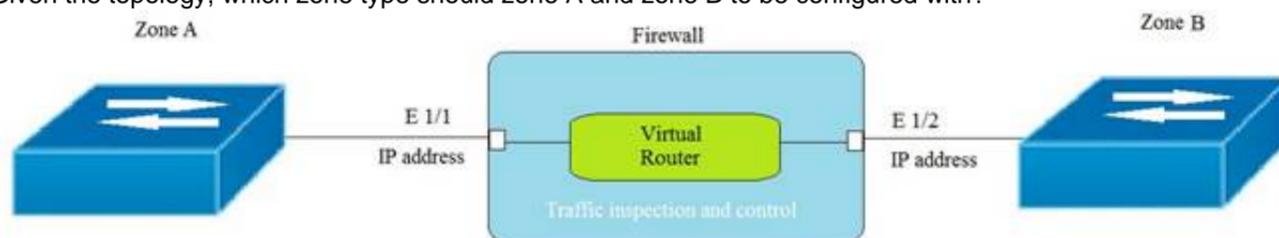
Which interface type is part of a Layer 3 zone with a Palo Alto Networks firewall?

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

Answer: C

NEW QUESTION 64

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



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

Answer: A

NEW QUESTION 69

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 architecture.

all areas of network and security

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>

NEW QUESTION 70

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: AB

Explanation:

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

NEW QUESTION 71

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

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

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

Answer: C

Explanation:

NEW QUESTION 76

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>

NEW QUESTION 79

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 verify

Answer: C

Explanation:

Reference:

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

NEW QUESTION 81

The CFO found a USB drive in the parking lot and decide to plug it into their corporate laptop. The USB drive had malware on it that loaded onto their computer and then contacted a known command and control (CnC) server, which ordered the infected machine to begin Exfiltrating data from the laptop. Which security profile feature could have been used to prevent the communication with the CnC server?

- A. Create an anti-spyware profile and enable DNS Sinkhole
- B. Create an antivirus profile and enable DNS Sinkhole
- C. Create a URL filtering profile and block the DNS Sinkhole category
- D. Create a security policy and enable DNS Sinkhole

Answer: A

Explanation:

NEW QUESTION 84

What is the correct process for 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:

NEW QUESTION 87

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>

NEW QUESTION 92

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

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

Answer: C

NEW QUESTION 96

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 route to route between the two interfaces

Answer: D

Explanation:

NEW QUESTION 97

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

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

Answer: A

NEW QUESTION 101

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

Answer: C

NEW QUESTION 105

What is the maximum volume of concurrent administrative account sessions?

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

Answer: C

NEW QUESTION 107

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>

NEW QUESTION 111

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

- A. Device
- B. Policies
- C. Monitor
- D. Objects

Answer: D

NEW QUESTION 113

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

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

Answer: D

NEW QUESTION 114

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

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

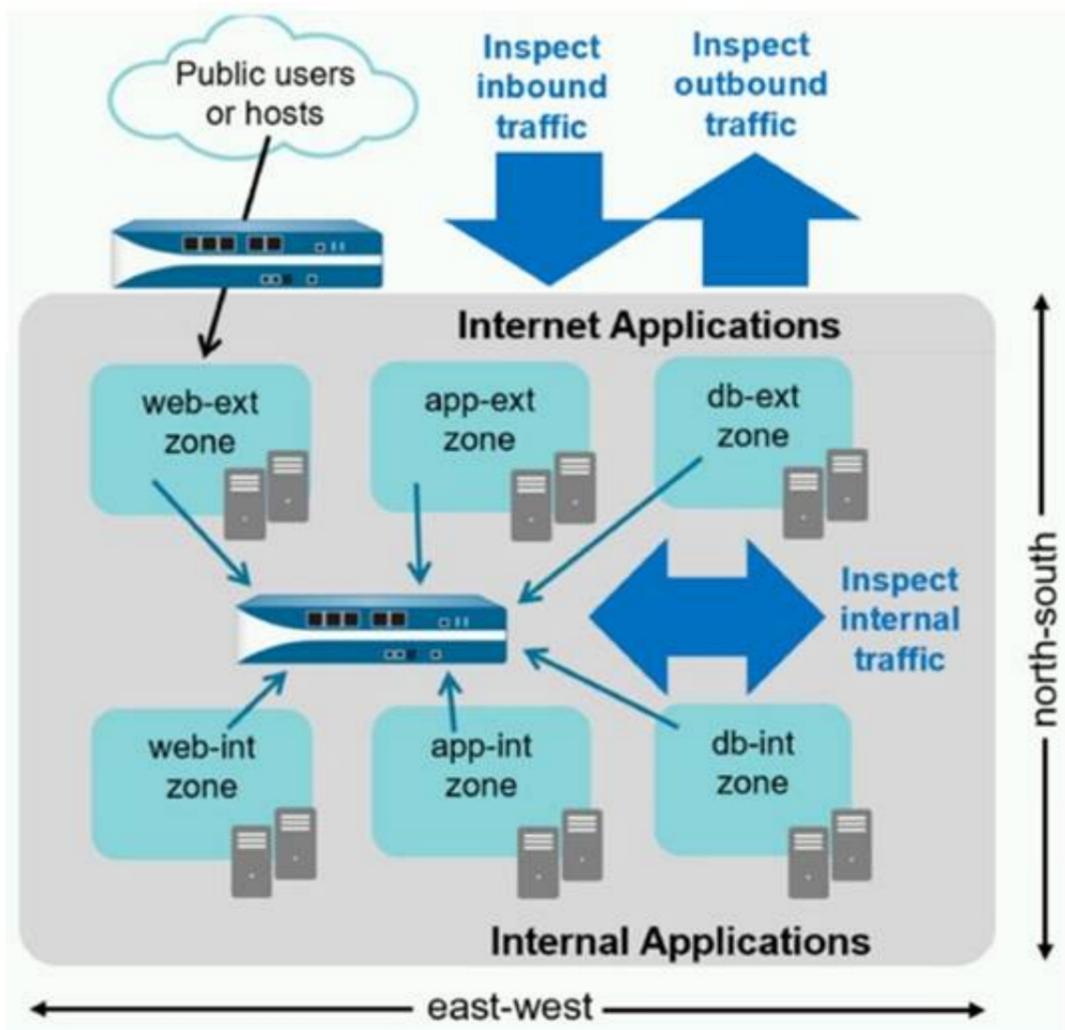
Answer: A

Explanation:

GlobalProtect: GlobalProtect safeguards your mobile workforce by inspecting all traffic using your next-generation firewalls deployed as internet gateways, whether at the perimeter, in the Demilitarized Zone (DMZ), or in the cloud.

NEW QUESTION 115

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

NEW QUESTION 118

How are service routes used in PAN-OS?

- A. By the OSPF protocol, as part of Dijkstra's algorithm, to give access to the various services offered in the network
- B. To statically route subnets so they are joinable from, and have access to, the Palo Alto Networks external services
- C. For routing, because they are the shortest path selected by the BGP routing protocol
- D. To route management plane services through data interfaces rather than the management interface

Answer: D

Explanation:

? Service routes are a feature of PAN-OS that allows the administrator to customize the interface that the firewall uses to send requests to external services, such as DNS, email, Palo Alto Networks updates, User-ID agent, syslog, Panorama, dynamic updates, URL updates, licenses, and AutoFocus1.

? By default, the firewall uses the management interface for all service routes, unless the packet destination IP address matches the configured destination service route, in which case the source IP address is set to the source address configured for the destination1.

? However, in some scenarios, the administrator may want to use a different interface for service routes, such as when the management interface does not have public internet access, or when the administrator wants to isolate or monitor the traffic for certain services23.

? To configure service routes, the administrator can select Device > Setup > Services > Service Route Configuration and customize each service with a source interface and a source address. The administrator can also configure destination service routes to specify a destination IP address and a gateway for each service1.

? Service routes are not related to routing protocols such as OSPF or BGP, which are used to exchange routing information between routers and determine the best path to reach a network destination. Service routes are only used to change the

interface that the firewall uses to communicate with external services. Therefore, service routes are used to route management plane services through data interfaces rather than the management interface.

References:

1: Configure Service Routes - Palo Alto Networks 2: Setting a Service Route for Services to Use a Dataplane's Interface - Palo Alto Networks 3: How to Perform Updates when Management Interface does not have Public Internet Access - Palo Alto Networks

NEW QUESTION 122

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: AD

NEW QUESTION 125

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>

NEW QUESTION 126

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

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

Answer: ABD

NEW QUESTION 131

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

NEW QUESTION 136

What is a function of application tags?

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

Answer: C

NEW QUESTION 141

DRAG DROP

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

content inspection

QoS shaping applied

Security policy lookup

DoS protection

Answer Area

first

second

third

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 146

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

- A. Add the address range to the Manual Exceptions list and exclude the IP address by selecting the entry. adding it to the Manual Exceptions list.
- B. Add each IP address in the range as a list entry and then exclude the IP address by selecting the entry.
- C. Select the address range in the List Entries list.
- D. A column will open with the IP addresses.
- E. Select the entry to exclude.
- F. Add the specific IP address from the address range to the Manual Exceptions list by using regular expressions to define the entry.

Answer: D

NEW QUESTION 149

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:

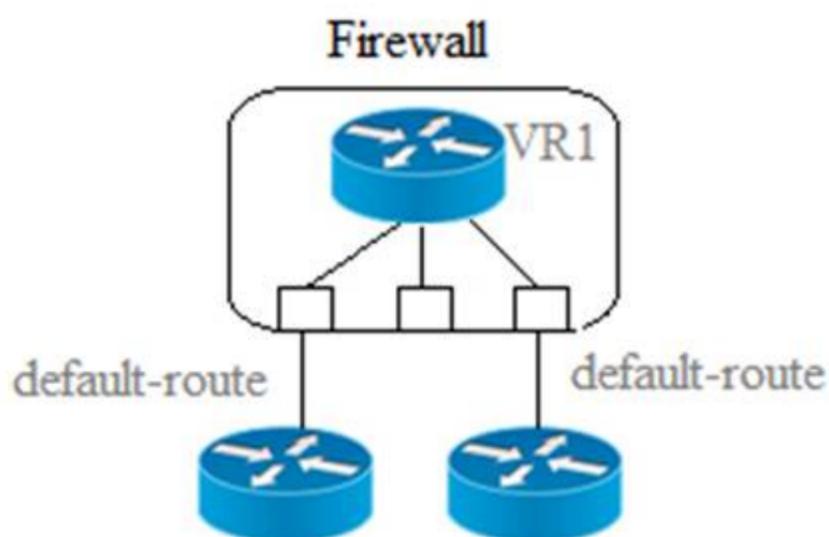
Reference:

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

NEW QUESTION 154

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

Multiple Static Default Routes



Path monitoring does not determine if route is useable

- A. Route with highest metric is actively used
- B. Path monitoring determines if route is useable
- C. Path monitoring determines if route is useable
- D. Route with lowest metric is actively used

Answer: CD

NEW QUESTION 156

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

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

Answer: A

NEW QUESTION 161

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

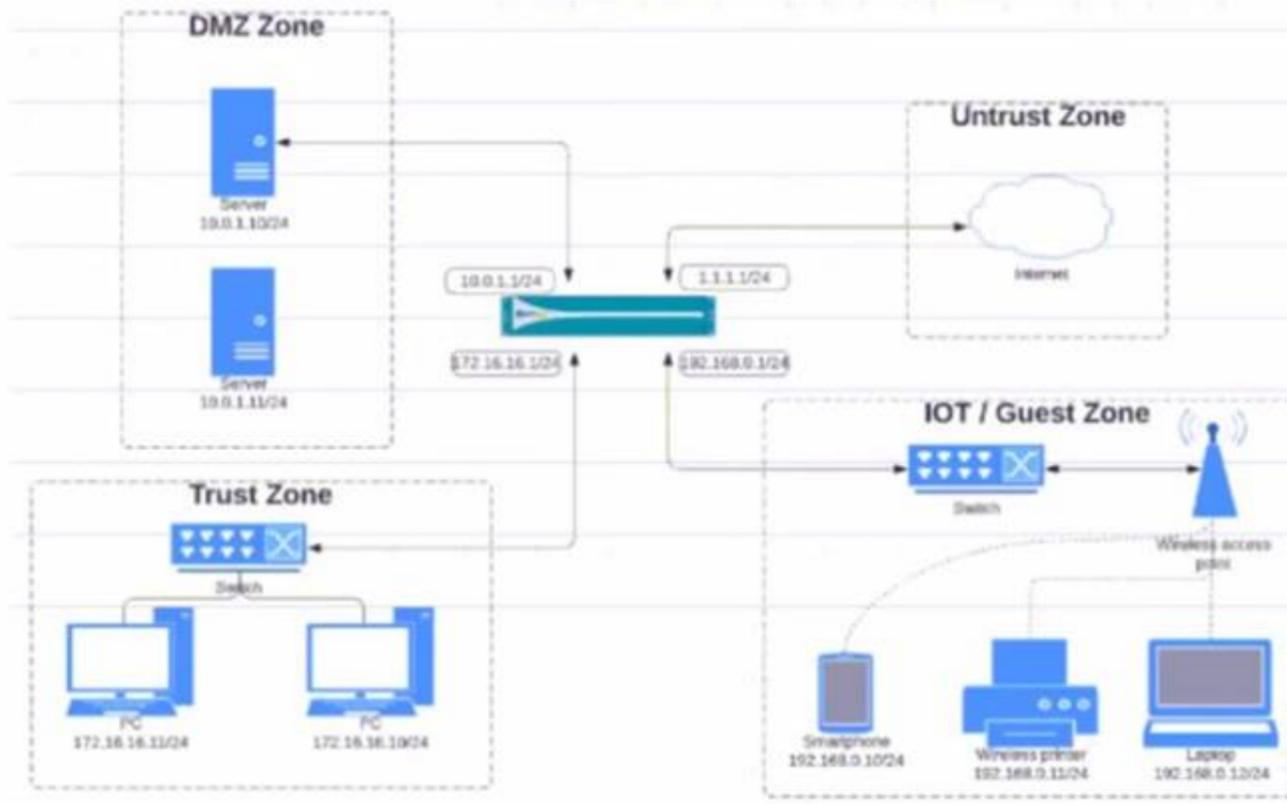
Explanation:

Reference:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIt5CAC>

NEW QUESTION 166

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



Which policy achieves the desired results?

- A)
- | NAME | TAGS | TYPE | Source | | | | Destination | |
|------|------|-----------|-----------|----------------|------|--------|-------------|---------|
| | | | ZONE | ADDRESS | USER | DEVICE | ZONE | ADDRESS |
| 04-A | none | universal | IOT-Guest | 172.16.16.0/24 | any | any | DMZ | any |
| | | | Trust | 192.168.0.0/24 | | | Untrust | |
- B)
- | NAME | TAGS | TYPE | Source | | | | Destination | |
|------|------|-----------|-----------|----------------|------|--------|-------------|-------------|
| | | | ZONE | ADDRESS | USER | DEVICE | ZONE | ADDRESS |
| 03-A | none | universal | IOT-Guest | 172.16.16.0/24 | any | any | DMZ | 1.1.1.0/24 |
| | | | Trust | 192.168.0.0/24 | | | Untrust | 10.0.1.0/24 |
- C)
- | NAME | TAGS | TYPE | Source | | | | Destination | |
|------|------|-----------|-----------|----------------|------|--------|-------------|---------|
| | | | ZONE | ADDRESS | USER | DEVICE | ZONE | ADDRESS |
| 02-A | none | universal | IOT-Guest | 172.16.16.0/24 | any | any | DMZ | any |
| | | | Trust | 192.168.0.0/24 | | | Untrust | |
- D)
- | NAME | TAGS | TYPE | Source | | | | Destination | |
|------|------|-----------|-----------|----------------|------|--------|-------------|----------------|
| | | | ZONE | ADDRESS | USER | DEVICE | ZONE | ADDRESS |
| 01-A | none | universal | IOT-Guest | 10.0.1.0/24 | any | any | DMZ | 1.1.1.0/24 |
| | | | Trust | 172.16.16.0/24 | | | Untrust | 192.168.0.0/24 |

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

Answer: C

NEW QUESTION 167

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

NEW QUESTION 169

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

NEW QUESTION 172

Your company is highly concerned with their Intellectual property being accessed by unauthorized resources. There is a mature process to store and include metadata tags for all confidential documents.

Which Security profile can further ensure that these documents do not exit the corporate network?

- A. File Blocking
- B. Data Filtering
- C. Anti-Spyware
- D. URL Filtering

Answer: B

Explanation:

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/objects/objects-security-profiles-data-filtering>

NEW QUESTION 174

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.

NEW QUESTION 178

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

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

Answer: BC

Explanation:

Reference:

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

NEW QUESTION 182

How frequently can wildfire updates be made available to firewalls?

- A. every 15 minutes
- B. every 30 minutes
- C. every 60 minutes
- D. every 5 minutes

Answer:

D

NEW QUESTION 185

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIKECA0>

NEW QUESTION 190

The compliance officer requests that all evasive applications need to be blocked on all perimeter firewalls out to the internet. The firewall is configured with two zones;

- * 1. trust for internal networks
- * 2. untrust to the internet

Based on the capabilities of the Palo Alto Networks NGFW, what are two ways to configure a security policy using App-ID to comply with this request? (Choose two)

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

Answer: AD

NEW QUESTION 194

Access to which feature requires PAN-OS Filtering licenses?

- 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>

NEW QUESTION 195

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

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

Answer: AB

NEW QUESTION 197

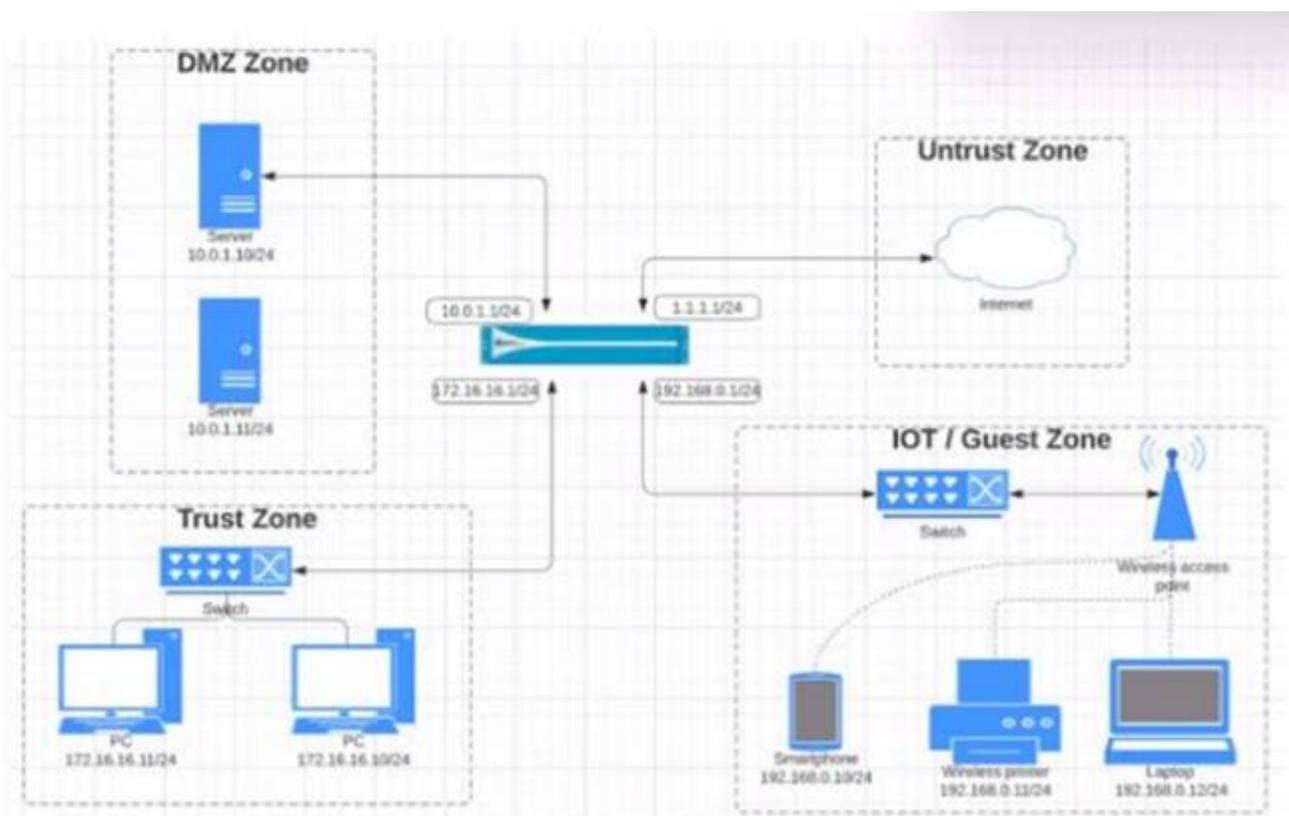
Which interface type requires no routing or switching but applies Security or NAT policy rules before passing allowed traffic?

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

Answer: A

NEW QUESTION 201

View the diagram.



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

A)

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE		
02-A	None	universal	IOT-Guest	172.16.16.0/24	any	any	DMZ	any	any	ssh	application-default
			Trust	172.16.16.0/24			Untrust			ssh	
										web-browsing	

B)

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE		
02-A	None	universal	IOT-Guest	172.16.16.0/24	any	any	DMZ	1.1.1.0/24	any	ssh	application-default
			Trust	172.16.16.0/24			Untrust	10.0.1.0/24		ssh	
										web-browsing	

C)

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE		
02-A	None	universal	IOT-Guest	10.0.1.0/24	any	any	DMZ	1.1.1.0/24	any	ssh	application-default
			Trust	172.16.16.0/24			Untrust	172.16.16.0/24		ssh	
										web-browsing	

D)

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE		

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

Answer: C

NEW QUESTION 203

What can be used as match criteria for creating a dynamic address group?

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

Answer: C

NEW QUESTION 208

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

NAME	SERVICE	TRAFFIC (BYTES, 30 DAYS)	App Usage				MODIFIED	CREATED
			APPS ALLOWED	APPS SEEN	DAYS WITH NO NEW APPS	COMPARE		
55	Unrestricted Traffic	1.7T	any	142	258	Compare	2022-01-06 18:30:02	2020-11-16
25	Outbound Trust2	6.5G	any	26	447	Compare	2022-01-06 18:30:02	2020-11-16
29	CorObj003	912.3M	any	1	448	Compare	2022-01-06 18:30:02	2020-11-16
20	2019-08-16388at E...	508.0M	any	18	448	Compare	2022-01-06 18:30:02	2020-11-16
31	CorObj-vrf2	235.3M	any	1	448	Compare	2022-01-06 18:30:02	2020-11-16
32	GRE-EndPoint	140.8M	any	1	448	Compare	2022-01-06 18:30:02	2020-11-16
47	Workstation-applet...	23.1M	any	3	448	Compare	2022-01-06 18:30:02	2020-11-16
27	CorObj006	22.8M	any	2	448	Compare	2022-01-06 18:30:02	2020-11-16
30	CorObj-@C	1.2M	any	1	446	Compare	2022-01-06 18:30:02	2020-11-16
28	CorObj004	590.2k	any	1	445	Compare	2022-01-06 18:30:02	2020-11-16
17	LogSinkholeTraffic	0	any	2	452	Compare	2022-01-06 18:30:02	2020-11-16
24	Outbound Trust	0	any	1	419	Compare	2022-01-06 18:30:02	2020-11-16

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

Answer: C

NEW QUESTION 213

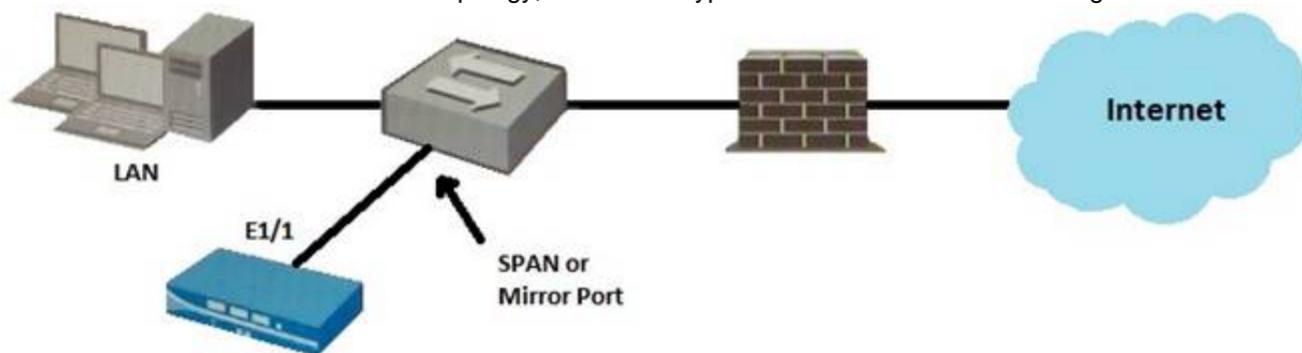
An administrator is reviewing another administrator's Security policy log settings. Which log setting configuration is consistent with best practices for normal traffic?

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

Answer: B

NEW QUESTION 214

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



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

Answer: A

NEW QUESTION 215

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

NEW QUESTION 219

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your PCNSA Exam with Our Prep Materials Via below:

<https://www.certleader.com/PCNSA-dumps.html>