



Paloalto-Networks

Exam Questions PCNSA

Palo Alto Networks Certified Network Security Administrator

NEW QUESTION 1

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

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

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

Answer: A

NEW QUESTION 4

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

A.

destination address

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

Answer: B

Explanation:

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

NEW QUESTION 5

DRAG DROP

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reconnaissance – stage where the attacker scans for network vulnerabilities and services that can be exploited.

Installation – stage where the attacker will explore methods such as a root kit to establish persistence

Command and Control – stage where the attacker has access to a specific server so they can communicate and pass data to and from infected devices within a network.

Act on the Objective – stage where an attacker has motivation for attacking a network to deface web property

NEW QUESTION 6

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

- A. Configure an authentication policy

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

Answer: C

NEW QUESTION 7

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

A.

uncommitted changes

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

Answer: D

Explanation:

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

NEW QUESTION 8

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-username-using-captive-portal.html>

NEW QUESTION 9

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 10

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

Palo Alto Networks User-ID Agent Setup

Enable Security Log ✓
Server Log Monitor Frequency (sec) **15**
Enable Session ✓
Server Session Read Frequency (sec) **10**
Novell eDirectory Query Interval (sec) **30**
Syslog Service Profile
Enable Probing
Probe Interval (min) **20**
Enable User Identification Timeout ✓
User Identification Timeout (min) **45**
Allow matching usernames without domains
Enable NTLM
NTLM Domain
User-ID Collector Name

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

Answer: BC

NEW QUESTION 10

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: AD

NEW QUESTION 14

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 Security policy selected
- D. Policy Optimizer can be used on a schedule to automatically create a disabled Layer 7 App-ID Security policy for every Layer 4 policy that exists Admins can then manually enable policies they want to keep and delete ones they want to remove

Answer: B

NEW QUESTION 19

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 in a device group to which to push policy rules
- D. You specify the location as pre or post-rules to push policy rules

Answer: C

NEW QUESTION 20

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

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

Answer: AB

Explanation:

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

[administrators/administrative-authentication.html](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.

NEW QUESTION 21

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 26

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

- A. Prisma SaaS
- B. AutoFocus
- C. Panorama
- D. GlobalProtect

Answer: A

NEW QUESTION 27

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

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

Answer: C

NEW QUESTION 30

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

NEW QUESTION 31

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

NEW QUESTION 32

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>

NEW QUESTION 33

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

An administrator is implementing an exception to an external dynamic list by adding an entry to the list manually. The administrator wants to save the changes, but the OK button is grayed out.

What are two possible reasons the OK button is grayed out? (Choose two.)

- A. The entry contains wildcards.
- B. The entry is duplicated.
- C. The entry doesn't match a list entry.
- D. The entry matches a list entry.

Answer: BC

NEW QUESTION 37

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 45

DRAG DROP

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

Threat Intelligence Cloud	Drag answer here	Identifies and inspects all traffic to block known threats.
Next-Generation Firewall	Drag answer here	Gathers, analyzes, correlates, and disseminates threats to and from the network and endpoints located within the network.
Advanced Endpoint Protection	Drag answer here	Inspects processes and files to prevent known and unknown exploits.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Threat Intelligence Cloud	Next-Generation Firewall	Identifies and inspects all traffic to block known threats.
Next-Generation Firewall	Threat Intelligence Cloud	Gathers, analyzes, correlates, and disseminates threats to and from the network and endpoints located within the network.
Advanced Endpoint Protection	Advanced Endpoint Protection	Inspects processes and files to prevent known and unknown exploits.

NEW QUESTION 49

In a security policy what is the quickest way to reset 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

NEW QUESTION 50

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

- A. GlobalProtect agent
- B. XML API
- C.

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

Answer: BC

NEW QUESTION 53

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

NEW QUESTION 54

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

- A. Mastered
- B. Not Mastered

Answer: A

NEW QUESTION 57

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 60

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

NEW QUESTION 65

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. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 70

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 75

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

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

Answer: B

Explanation:

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

? Gain full visibility into all traffic, including SSL, and block high-risk applications.

Extend those protections to remote and mobile devices.

? Protect against perimeter breaches by blocking malicious or risky websites through URL filtering.

? Block known exploits, malware and inbound command-and-control communications using multiple threat prevention disciplines, including IPS, anti- malware, anti-CnC, DNS monitoring and sinkholing, and file and content blocking.

? Detect unknown malware and automatically deliver protections globally to thwart new attacks.

? Provide ongoing education to users on spear phishing links, unknown emails, risky websites, etc.

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

NEW QUESTION 78

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

- A. Mastered
- B. Not Mastered

Answer: A

NEW QUESTION 81

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

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

Answer: D

NEW QUESTION 82

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

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

- A. any port
- B. same port as ssl and snmpv3
- C. the default port
- D. only ephemeral ports

Answer: C

NEW QUESTION 86

What is the main function of the Test Policy Match function?

- A. verify that policy rules from Expedition are valid
- B. confirm that rules meet or exceed the Best Practice Assessment recommendations
- C. confirm that policy rules in the configuration are allowing/denying the correct traffic
- D. ensure that policy rules are not shadowing other policy rules

Answer: D

NEW QUESTION 90

What does an administrator use to validate whether a session is matching an expected NAT policy?

- A. system log
- B. test command
- C. threat log
- D. config audit

Answer: B

Explanation:

Reference: <https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g00000 0CIQSCA0>

NEW QUESTION 94

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

NEW QUESTION 97

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, lo
- C. or informational severity.
- D. It dynamically groups applications based on application attributes such as category and subcategory.
- E. It dynamically shapes defined application traffic based on active sessions and bandwidth usage.

Answer: C

NEW QUESTION 99

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 102

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.

References:

1: Security Profiles - Palo Alto Networks 2: WildFire Analysis Profile - Palo Alto

Networks 3: WildFire - Palo Alto Networks 4: Advanced Wildfire as an ICAP Alternative | Palo Alto Networks 5: Vulnerability Protection Profile - Palo Alto Networks : [Content-ID - Palo Alto Networks] : [Advanced Threat Prevention - Palo Alto Networks]

NEW QUESTION 106

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

General Settings

Hostname

Domain

☐ Accept DHCP server provided Hostname

☐ Accept DHCP server provided Domain

Login Banner

☐ Force Admins to Acknowledge Login Banner

SSL/TLS Service ProfileNone

Time ZoneNone

LocaleEnglish

Date

Time

Latitude

Longitude

☐ Automatically Acquire Commit Lock

☐ Certificate Expiration Check

☐ Use Hypervisor Assigned MAC Addresses

☐ GTP Security

☐ SCTP Security

☒ Policy Rule Hit Count

OK

Cancel

- 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.

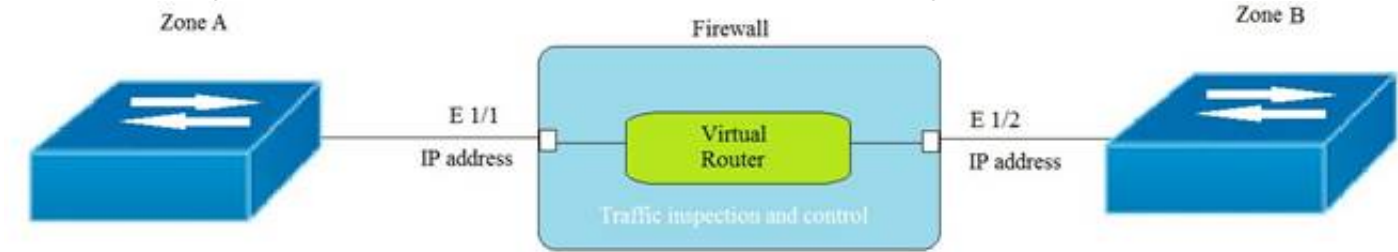
Answer: C

Explanation:

Reference:<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g00000 0CIFGCA0>

NEW QUESTION 108

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 109

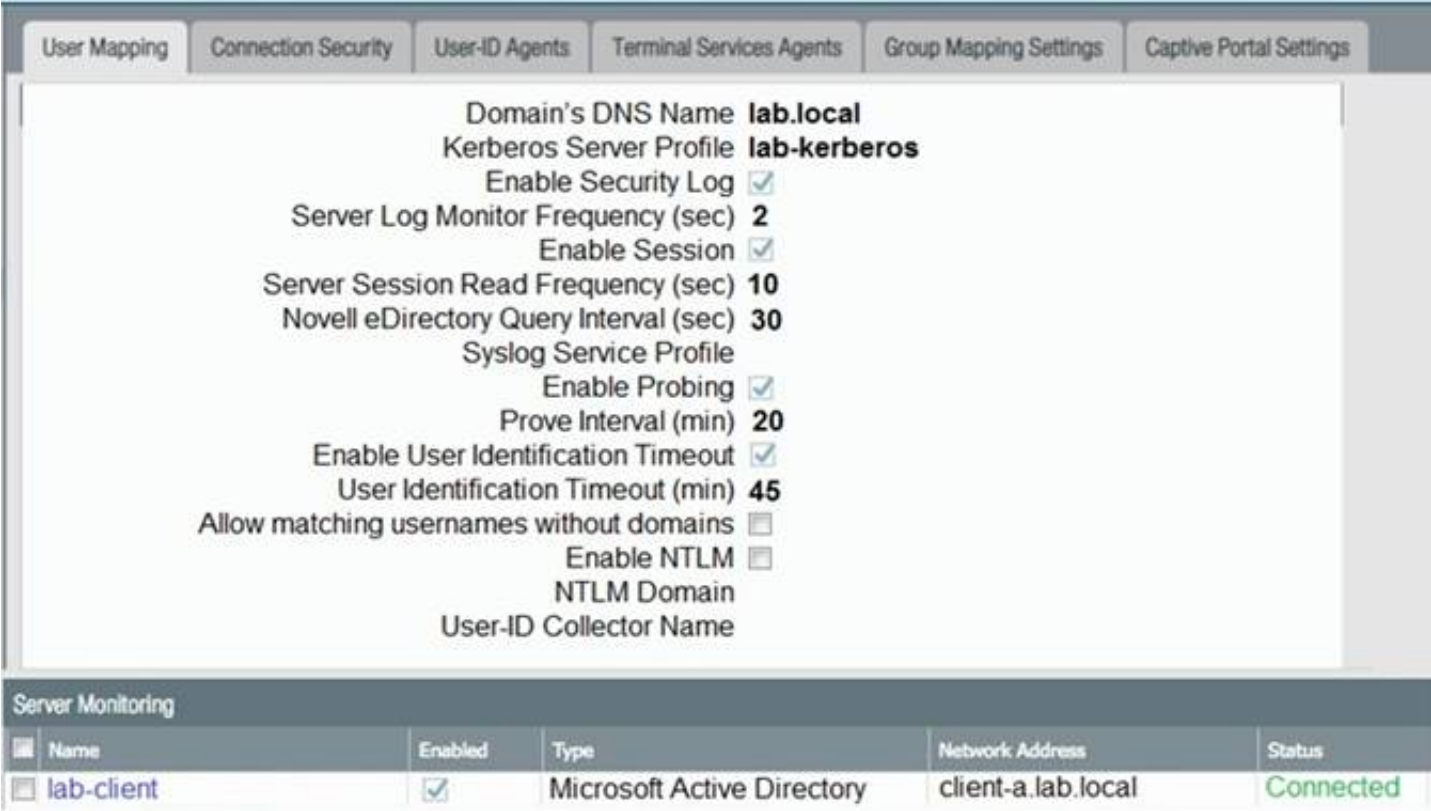
An administrator wants to prevent access to media content websites that are risky
Which two URL categories should be combined in a custom URL category to accomplish this goal? (Choose two)

- A. Mastered
- B. Not Mastered

Answer: A

NEW QUESTION 114

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



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

Answer: A

NEW QUESTION 117

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 122

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 124

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%20maintai ning%20user%20visibility.>

NEW QUESTION 126

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

NEW QUESTION 127

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

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

Answer: D

Explanation:

NEW QUESTION 130

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

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

Answer: D

Explanation:

References:[https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g00000](https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g0000000ClomCAC)

NEW QUESTION 134

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

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

Answer: B

Explanation:

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

NEW QUESTION 136

DRAG DROP

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

Answer Area

Microsoft Exchange	Drag answer here	syslog monitoring
Linux authentication	Drag answer here	Terminal Services agent
Windows clients	Drag answer here	server monitoring
Citrix client	Drag answer here	client probing

Answer:

Answer Area

Microsoft Exchange	server monitoring	syslog monitoring
Linux authentication	syslog monitoring	Terminal Services agent
Windows clients	client probing	server monitoring
Citrix client	Terminal Services agent	client probing

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 138

When creating a custom URL category object, which is a valid type?

- A. domain match
- B. host names
- C. wildcard
- D. category match

Answer: D

Explanation:

Reference:<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/objects/objects-custom-objects-url-category.html>

NEW QUESTION 139

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

- A. Biometric scanning results from iOS devices

- B. Firewall logs
- C. Custom API scripts
- D. Security Information and Event Management Systems (SIEMS), such as Splunk
- E. DNS Security service

Answer: BCE

NEW QUESTION 141

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

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

Answer: D

NEW QUESTION 143

Complete the statement. A security profile can block or allow traffic

- A. on unknown-tcp or unknown-udp traffic
- B. after it is matched by a security policy that allows traffic
- C. before it is matched by a security policy
- D. after it is matched by a security policy that allows or blocks traffic

Answer: B

Explanation:

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

NEW QUESTION 145

What is the maximum volume of concurrent administrative account sessions?

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

Answer: C

NEW QUESTION 149

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

Answer: B

NEW QUESTION 154

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 158

Which service protects cloud-based applications such as Dropbox and Salesforce by administering permissions and scanning files for sensitive information?

- A. Aperture
- B. AutoFocus
- C. Parisma SaaS
- D. GlobalProtect

Answer: C

NEW QUESTION 161

DRAG DROP

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

reconnaissance		stage that reveals the attacker's motivation
installation		stage where the attacker scans for network
command and control		exploited
act on the objectives		stage where the attacker will explore methods of persistence
		stage where the attacker has access to a system

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

reconnaissance	reconnaissance	stage that reveals the attacker's motivation
installation	installation	stage where the attacker scans for network
command and control	command and control	exploited
act on the objectives	act on the objectives	stage where the attacker will explore methods of persistence
		stage where the attacker has access to a system

NEW QUESTION 163

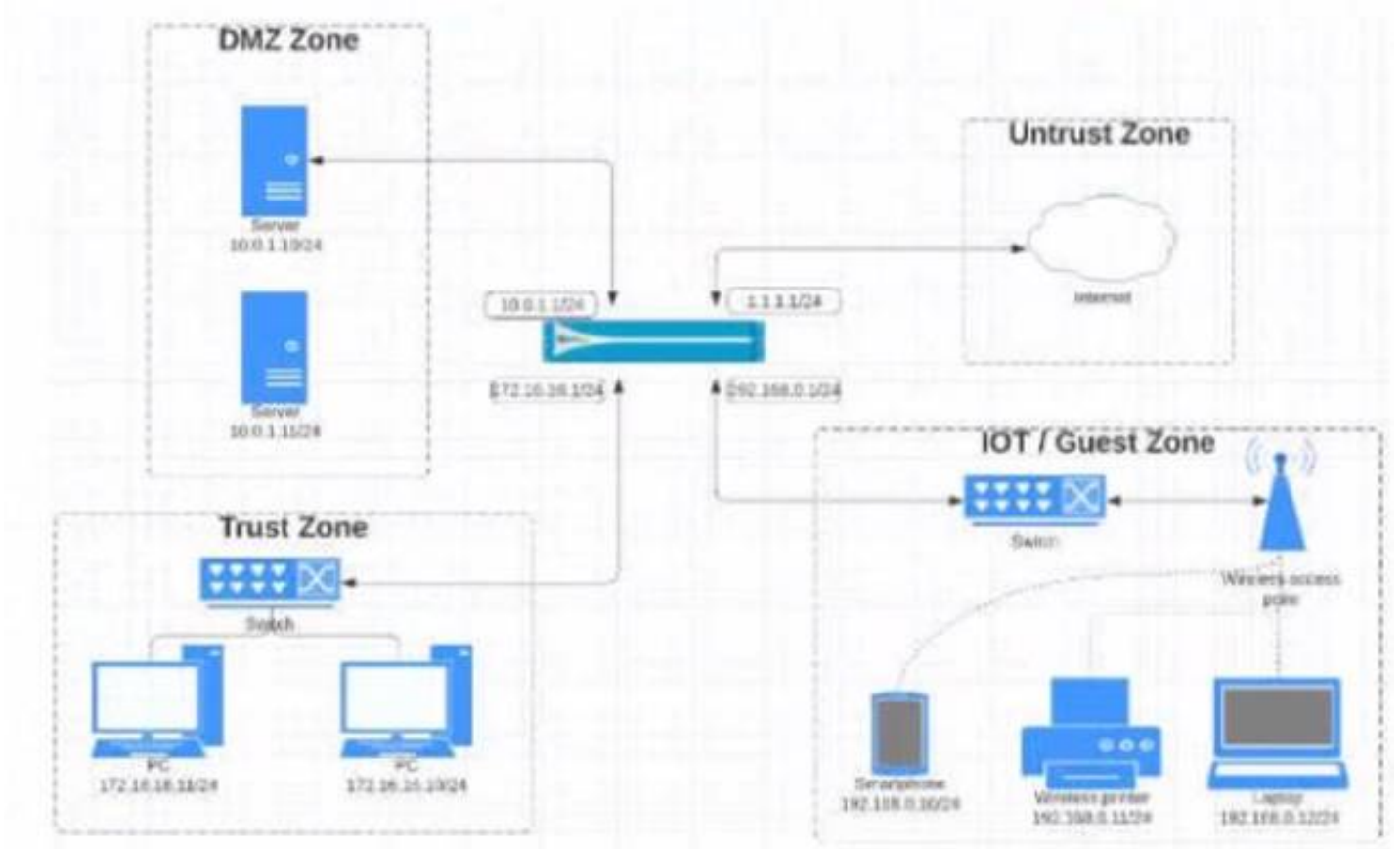
An administrator is troubleshooting traffic that should match the interzone-default rule. However, the administrator doesn't see this traffic in the traffic logs on the firewall. The interzone-default was never changed from its default configuration. Why doesn't the administrator see the traffic?

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

Answer: D

NEW QUESTION 165

View the diagram.



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

A)

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

B)

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

C)

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

D)

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

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

Answer: C

NEW QUESTION 166

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 171

An administrator would like to silently drop traffic from the internet to a ftp server. Which Security policy action should the administrator select?

- A. Reset-server
B. Block
C. Deny
D. Drop

Answer: D

NEW QUESTION 175

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

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

Answer: BD

NEW QUESTION 178

What is the minimum frequency for which you can configure the firewall to 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.
----------	---

NEW QUESTION 181

In the example security policy shown, which two websites are blocked? (Choose two.)

	Name	Tags	Zone	Address	Zone	Address	Application	Service	URL Category	Action	Profile
1	Block-Sites	outbound	Inside	Any	Outside	Any	Any	any	Social-networking	Deny	None

- A. LinkedIn
- B. Facebook
- C. YouTube
- D. Amazon

Answer: AB

NEW QUESTION 186

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 190

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

NEW QUESTION 194

An administrator is reviewing the Security policy rules shown in the screenshot below. Which statement is correct about the information displayed?



- A. Eleven rules use the "Infrastructure*" tag.
- B. The view Rulebase as Groups is checked.
- C. There are seven Security policy rules on this firewall.
- D. Highlight Unused Rules is checked.

Answer: B

Explanation:

NEW QUESTION 196

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
- E. CLI, API

Answer: D

Explanation:

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/firewall-administration/management-interfaces>

You can use the following user interfaces to manage the Palo Alto Networks firewall:

- ? Use the Web Interface to perform configuration and monitoring tasks with relative ease. This graphical interface allows you to access the firewall using HTTPS (recommended) or HTTP and it is the best way to perform administrative tasks.
- ? Use the Command Line Interface (CLI) to perform a series of tasks by entering commands in rapid succession over SSH (recommended), Telnet, or the console port. The CLI is a no-frills interface that supports two command modes, operational and configure, each with a distinct hierarchy of commands and statements. When you become familiar with the nesting structure and syntax of the commands, the CLI provides quick response times and administrative efficiency.
- ? Use the XML API to streamline your operations and integrate with existing, internally developed applications and repositories. The XML API is a web service implemented using HTTP/HTTPS requests and responses.
- ? Use Panorama to perform web-based management, reporting, and log collection for multiple firewalls. The Panorama web interface resembles the firewall web interface but with additional functions for centralized management.

NEW QUESTION 197

An administrator would like to apply a more restrictive Security profile to traffic for file sharing applications. The administrator does not want to update the Security policy or object when new applications are released.

Which object should the administrator use as a match condition in the Security policy?

- A. the Content Delivery Networks URL category
- B. the Online Storage and Backup URL category
- C. an application group containing all of the file-sharing App-IDs reported in the traffic logs
- D. an application filter for applications whose subcategory is file-sharing

Answer: D

NEW QUESTION 199

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 204

Which administrator receives a global notification for a new malware that infects hosts. The infection will result in the infected host attempting to contact and command-and-control (C2) server.

Which security profile components will detect and prevent this threat after the firewall's signature database has been updated?

- A. antivirus profile applied to outbound security policies

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

Answer: C

Explanation:

NEW QUESTION 205

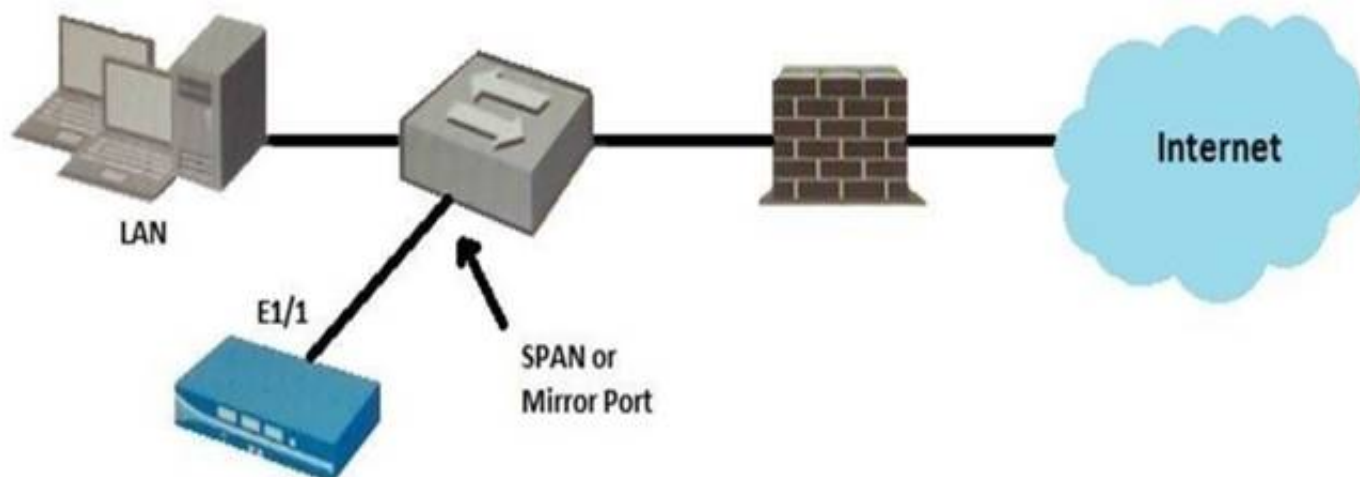
Which the app-ID application will you need to allow in your security policy to use facebook- chat?

- A. facebook-email
- B. facebook-base
- C. facebook
- D. facebook-chat

Answer: BD

NEW QUESTION 210

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

NEW QUESTION 212

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 213

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:

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.

NEW QUESTION 216

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

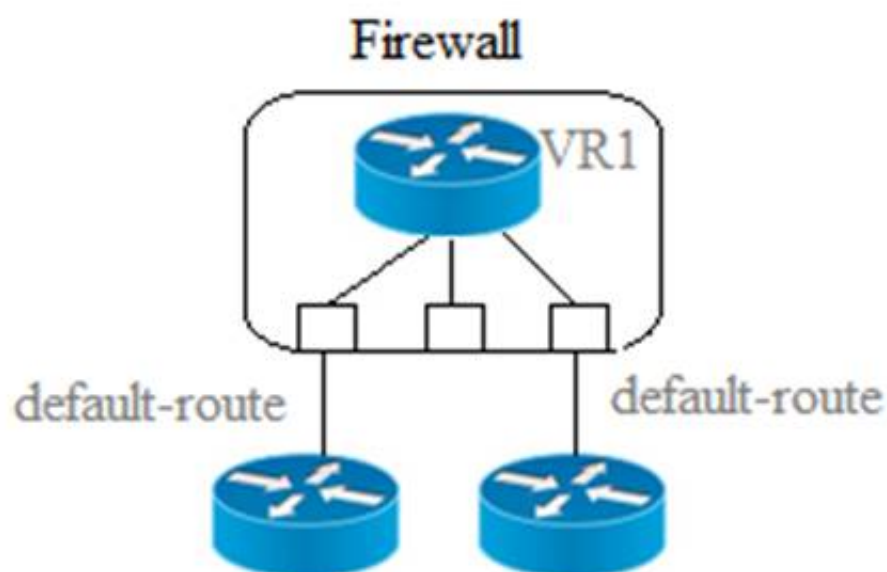
- A. Content updates for firewall A/P HA pairs can only be pushed to the active firewall.
- B. Content updates for firewall A/A HA pairs need a defined master device.
- C. Before deploying content updates, always check content release version compatibility.
- D. After deploying content updates, perform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

Answer: C

NEW QUESTION 218

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 223

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?

NAT Policy Rule

General **Original Packet** **Translated Packet**

Source Address Translation		Destination Address Translation	
Translation Type	<input type="text"/>	Translation Type	<input type="text" value="None"/>
Address Type	<input type="text"/>		
Interface	<input type="text"/>		
IP Address	<input type="text"/>		

OK **Cancel**

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

Answer: A

NEW QUESTION 228

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?

Windows-based agent on a domain controller

- A. Captive Portal
- B. Citrix terminal server with adequate data-plane resources
- C. PAN-OS integrated agent
- D. PAN-OS integrated agent

Answer: A

NEW QUESTION 230

Which type of address object is "10 5 1 1/0 127 248 2"?

- A. IP subnet
- B. IP wildcard mask
- C. IP netmask
- D. IP range

Answer: B

NEW QUESTION 231

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

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

Answer: B

NEW QUESTION 236

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

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

Answer: A

NEW QUESTION 237

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

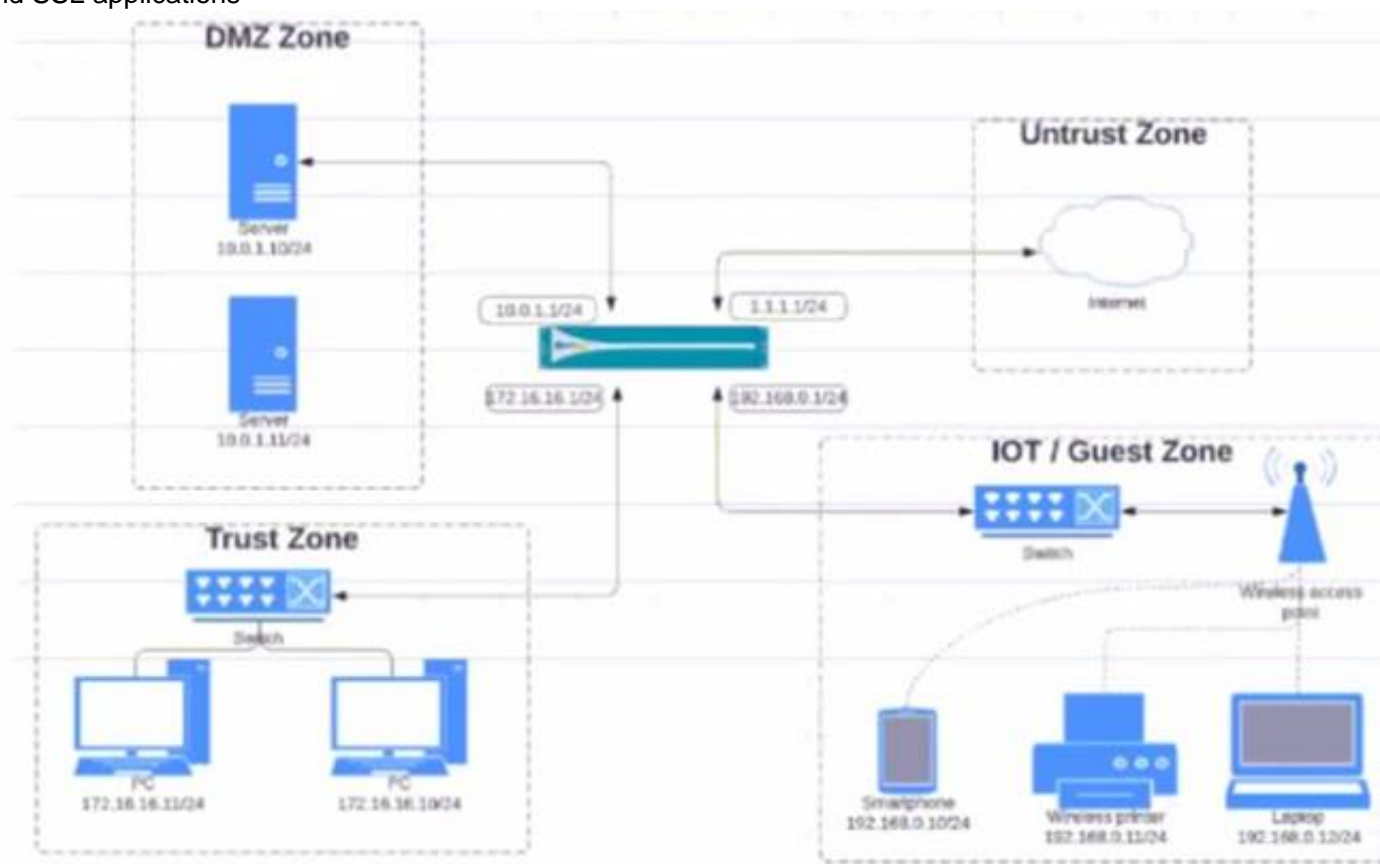
Explanation:

Reference:

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

NEW QUESTION 241

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 243

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

NEW QUESTION 244

Why does a company need an Antivirus profile?

- A. Mastered
- B. Not Mastered

Answer: A

NEW QUESTION 249

Which type of administrative role must you assign to a firewall administrator account, if the account must include a custom set of firewall permissions?

- A. SAML
- B. Multi-Factor Authentication
- C. Role-based
- D. Dynamic

Answer: C

Explanation:

Reference:<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/firewall-administration/manage-firewall-administrators/administrative-role-types.html>

NEW QUESTION 251

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 254

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 258

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 262

Where within the firewall GUI can all existing tags be viewed?

- A. Network > Tags
- B. Monitor > Tags
- C. Objects > Tags
- D. Policies > Tags

Answer: C

NEW QUESTION 266

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

- A. authentication
- B. decryption
- C application override
- C. NAT

Answer: AB

Explanation:

Reference:<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/url-filtering/url-filtering-concepts/url-category-as-policy-match-criteria.html>

NEW QUESTION 270

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

NEW QUESTION 275

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

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

Answer: BDE

NEW QUESTION 280

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

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

Answer: D

NEW QUESTION 285

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 289

The NetSec Manager asked to create a new firewall Local Administrator profile with customized privileges named NewAdmin. This new administrator has to authenticate without inserting any username or password to access the WebUI.

What steps should the administrator follow to create the New_Admin Administrator profile?

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

A.

Answer: B

NEW QUESTION 294

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

NEW QUESTION 296

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 300

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 302

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 303

Which prevention technique will prevent attacks based on packet count?

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

Answer: A

NEW QUESTION 304

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. Mastered
- B. Not Mastered

Answer: A

NEW QUESTION 307

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 308

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: AC

Explanation:

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

NEW QUESTION 310

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 312

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

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

Answer: C

NEW QUESTION 316

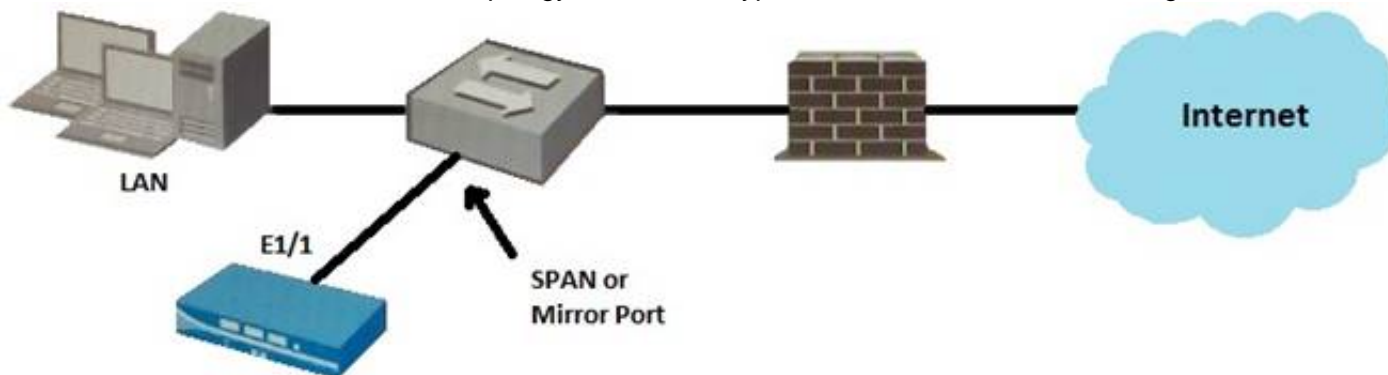
An administrator is troubleshooting traffic that should match the interzone-default rule. However, the administrator doesn't see this traffic in the traffic logs on the firewall. The interzone-default was never changed from its default configuration. Why doesn't the administrator see the traffic?

- 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

NEW QUESTION 317

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 319

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

	Name	Type	Source		Destination		Application
			Zone	Address	Zone	Address	
1	allow-it	universal	inside	any	DMZ	any	it-tools

Allows users to access IT applications on all ports

- A. Allows users in group "DMZ" to access IT applications
- B. Allows "any" users to access servers in the DMZ zone
- C. Allows users in group "it" to access IT applications
- D. Allows users in group "it" to access IT applications

Answer: D

NEW QUESTION 323

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 logging?

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

Answer: D

NEW QUESTION 325

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

PCNSA Practice Exam Features:

- * PCNSA Questions and Answers Updated Frequently
- * PCNSA Practice Questions Verified by Expert Senior Certified Staff
- * PCNSA Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * PCNSA Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The PCNSA Practice Test Here](#)