

Paloalto-Networks

Exam Questions PCNSA

Palo Alto Networks Certified Network Security Administrator



NEW QUESTION 1

Which update option is not available to administrators?

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

Answer: B

NEW QUESTION 2

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 3

Based on the screenshot presented which column contains the link that when clicked opens a window to display all applications matched to the policy rule?

No App Specified
 These are security policies that have no application specified and allow any application on the configured service which can present a security risk. Palo Alto Networks you convert these service only security policies to application based policies.

	Name	Service	Traffic (Bytes, 30 days)	App Usage			Compare	Modified
				Apps Allowed	Apps Seen	Days with No New Apps		
3	egress-outside	application-default	25.3G	any	8	8	Compare	2019-06-2...
1	inside-portal	any	372.6M	any	9	8	Compare	2019-06-2...

- A. Apps Allowed
- B. Name
- C. Apps Seen
- D. Service

Answer: C

NEW QUESTION 4

Which type of security policy rule will match traffic that flows between the Outside zone and inside zone, but would not match traffic that flows within the zones?

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

Answer: C

Explanation:

Reference:

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/software-and-content-updates/dynamic-contentupdates.html#:~:text=WildFire%20signature%20updates%20are%20made,within%20a%20minute%20of%20availability>

NEW QUESTION 5

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 6

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 7

Which action related to App-ID updates will enable a security administrator to view the existing security policy rule that matches new application signatures?

- A. Review Policies
- B. Review Apps
- C. Pre-analyze
- D. Review App Matches

Answer: A

Explanation:

References:

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

NEW QUESTION 8

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 9

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-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 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 10

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 13

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

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

Answer: B

NEW QUESTION 16

What are three factors that can be used in domain generation algorithms? (Choose three.)

- A. cryptographic keys
- B.

time of day

- C. other unique values
- D. URL custom categories
- E. IP address

Answer: ABC

Explanation:

Domain generation algorithms (DGAs) are used to auto-generate domains, typically in large numbers within the context of establishing a malicious command-and-control (C2) communications channel. DGA-based malware (such as Pushdo, BankPatch, and CryptoLocker) limit the number of domains from being blocked by hiding the location of their active C2 servers within a large number of possible suspects, and can be algorithmically generated based on factors such as time of day, cryptographic keys, or other unique values.

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/threat-prevention/dns-security/domain-generation-algorithm-detection>

NEW QUESTION 19

What is an advantage for using application tags?

- A. They are helpful during the creation of new zones
- B. They help with the design of IP address allocations in DHCP.
- C. They help content updates automate policy updates
- D. They help with the creation of interfaces

Answer: C

NEW QUESTION 24

How are Application Fillers or Application Groups used in firewall policy?

- A. An Application Filter is a static way of grouping applications and can be configured as a

- nested member of an Application Group
- B. An Application Filter is a dynamic way to group applications and can be configured as a nested member of an Application Group
 - C. An Application Group is a dynamic way of grouping applications and can be configured as a nested member of an Application Group
 - D. An Application Group is a static way of grouping applications and cannot be configured as a nested member of Application Group

Answer: B

NEW QUESTION 29

Which statement is true regarding NAT rules?

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

Answer: C

Explanation:

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/networking/nat/nat-policy-rules/nat-policy-overview>

NEW QUESTION 31

Which data flow direction is protected in a zero trust firewall deployment that is not protected in a perimeter-only firewall deployment?

- A. outbound
- B. north south
- C. inbound
- D. east west

Answer: D

NEW QUESTION 33

Which dynamic update type includes updated anti-spyware signatures?

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

Answer: A

NEW QUESTION 34

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

Device SN: 007251000156342 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: 26251 X-Forwarded-For IP: 0.0.0.0	NAT IP: 8.8.4.4 NAT Port: 53
Details		Flags
Threat Type: spyware Threat ID/Name: Phishing:151.136.74.in-adb.arp ID: 309010001 (View in Threat Vault) Category: dns-phishing Content Version: AppThreat-0-0 Severity: low Repeat Count: 2 File Name: URL: 151.136.74.in-adb.arp Partial Hash: 0 Pcap ID: 0 Source UUID: Destination UUID: Dynamic User Group: Network Slice ID SST: 0 Network Slice ID SD: App Category: networking App Subcategory: infrastructure App Technology: network-protocol App Characteristic: used-by-malware-has-known-vulnerability-persistent-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 35

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

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

Answer: BC

NEW QUESTION 38

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

- A. create the service object in the specific template
- B. uncheck the shared option

- C. ensure that disable override is selected
- D. ensure that disable override is cleared

Answer: D

Explanation:

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

NEW QUESTION 42

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 44

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 45

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 46

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 50

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

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

Answer: A

NEW QUESTION 55

Which statement is true about Panorama managed devices?

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

Answer: D

Explanation:

Explanation Explanation/Reference: Reference:

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

NEW QUESTION 56

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 61

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 66

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 69

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 70

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 71

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

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

Answer: A

NEW QUESTION 73

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

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

Answer: B

NEW QUESTION 75

Which interface does not require a MAC or IP address?

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

Answer: A

NEW QUESTION 77

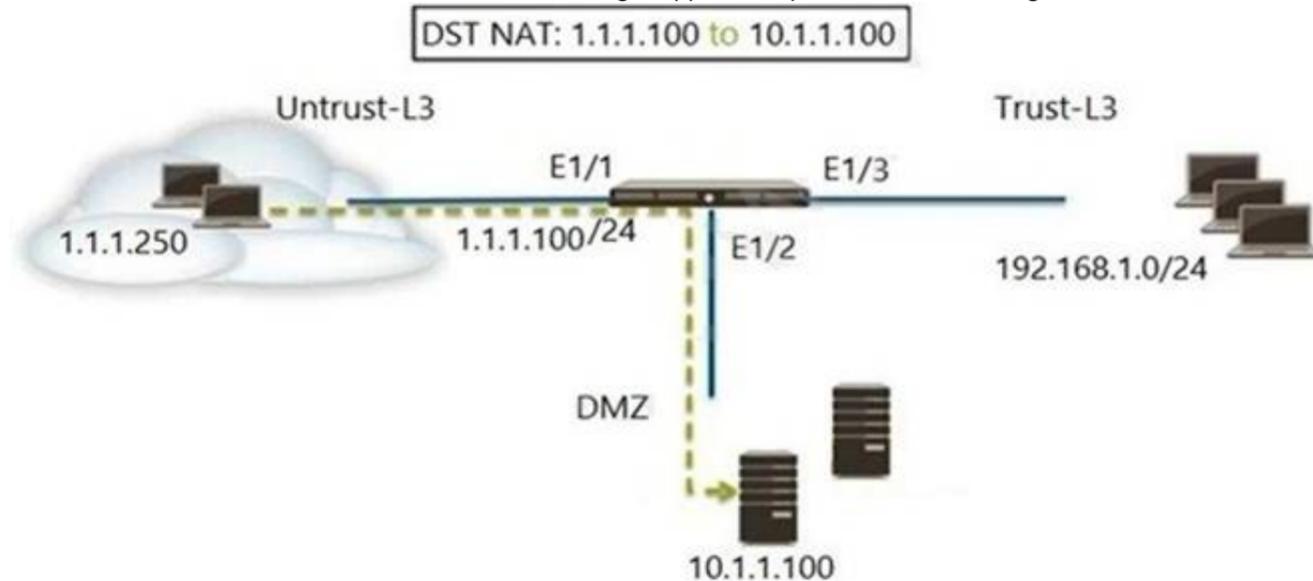
Which interface type is part of a Layer 3 zone with a Palo Alto Networks firewall?

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

Answer: C

NEW QUESTION 79

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



Which Security policy rule will allow traffic to flow to the web server?

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 83

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 87

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

The screenshot shows the configuration for Kerberos settings. The domain is lab.local and the profile is lab-kerberos. Several options are checked, including Enable Security Log, Enable Session, Enable Probing, and Enable User Identification Timeout. Below the settings is a 'Server Monitoring' table with the following data:

Name	Enabled	Type	Network Address	Status
lab-client	<input checked="" type="checkbox"/>	Microsoft Active Directory	client-a.lab.local	Connected

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

Answer: A

NEW QUESTION 91

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

- A. Mastered
- B. Not Mastered

Answer: A

NEW QUESTION 95

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 96

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 101

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 105

What must be configured for the firewall to access multiple authentication profiles for external services to authenticate a non-local account?

- A. authentication sequence
- B. LDAP server profile
- C. authentication server list
- D. authentication list profile

Answer: A

NEW QUESTION 108

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 109

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 113

Which interface type can use virtual routers and routing protocols?

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

Answer: B

NEW QUESTION 117

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

Detailed Log View		
General	Source	Destination
Session ID 781868	Source User	Destination User
Action drop	Source 192.168.101.25	Destination 8.8.4.4
Host ID	Source DAG	Destination DAG
Application dns	Country 192.168.0.0-192.168.255.255	Country United States
Rule Outbound DNS	Port 46282	Port 53
Rule UUID ea9f3b96-e280-467c-aca5-0b1902857791	Zone Servers	Zone Internet
Device SN 007251000156341	Interface ethernet1/4	Interface ethernet1/8
IP Protocol udp	NAT IP 67.190.64.58	NAT IP 8.8.4.4
Log Action global-logs	NAT Port 26351	NAT Port 53
Generated Time 2021/08/27 02:02:49	X-Forwarded-For IP 0.0.0.0	
Receive Time 2021/08/27 02:02:53		
Tunnel Type N/A		
	Details	Flags
		Captive Portal <input type="checkbox"/>

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

Answer: B

NEW QUESTION 122

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=kA10g0000>

00ClomCAC

NEW QUESTION 123

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 125

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?

- default
- universal
- intrazone
- interzone

Answer: C

NEW QUESTION 127

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

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

Answer: D

NEW QUESTION 131

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 134

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 138

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 140

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

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

Answer: B

Explanation:

NEW QUESTION 141

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

An application filter is an object that dynamically groups applications based on application attributes that you define, including category, subcategory, technology, risk factor, and characteristic. This is useful when you want to safely enable access to applications that you do not explicitly sanction, but that you want users to be able to access. For example, you may want to enable employees to choose their own office programs (such as Evernote, Google Docs, or Microsoft Office 365) for business use. To safely enable these types of applications, you could create an application filter that matches on the Category business-systems and the

Subcategory office-programs. As new applications office programs emerge and new App-IDs get created, these new applications will automatically match the filter you defined; you will not have to make any additional changes to your policy rulebase to safely enable any application that matches the attributes you defined for the filter. <https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/app-id/use-application-objects-in-policy/create-an-application-filter.html>

NEW QUESTION 143

What can be achieved by disabling the Share Unused Address and Service Objects with Devices setting on Panorama?

- A. Increase the backup capacity for configuration backups per firewall
- B. Increase the per-firewall capacity for address and service objects
- C. Reduce the configuration and session synchronization time between HA pairs
- D. Reduce the number of objects pushed to a firewall

Answer: D

NEW QUESTION 145

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

- A. Windows-based agent deployed on the internal network
- B. PAN-OS integrated agent deployed on the internal network
- C. Citrix terminal server deployed on the internal network
- D. Windows-based agent deployed on each of the WAN Links

Answer: A

Explanation:

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

NEW QUESTION 150

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 154

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 158

Which administrative management services can be configured to access a management interface?

- A. HTTP, CLI, SNMP, HTTPS
- B. HTTPS, SSH telnet SNMP
- C. SSH: telnet HTTP, HTTPS
- D. HTTPS, HTT
- E. CLI, API

Answer: D

Explanation:

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

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

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

NEW QUESTION 160

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 165

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?

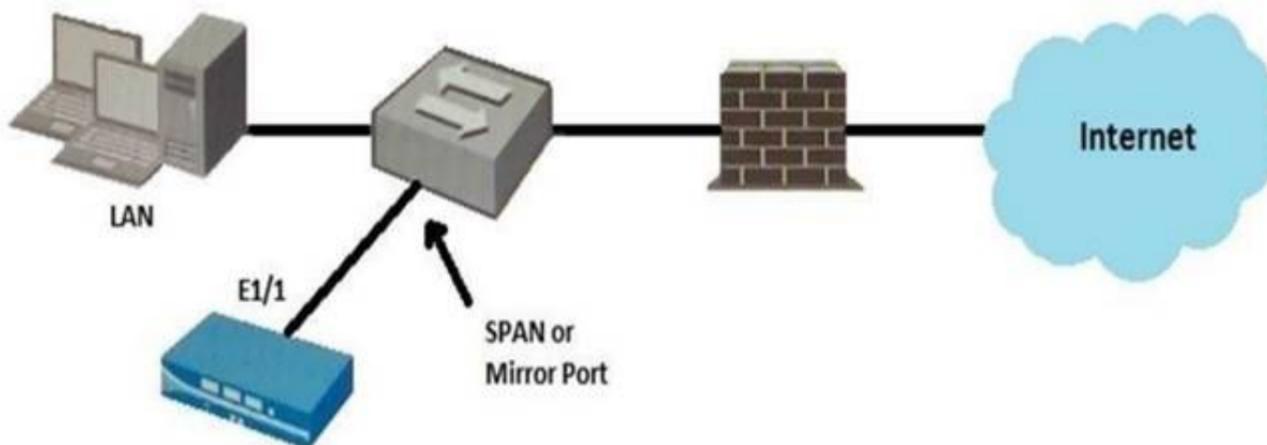
- A. antivirus profile applied to outbound security policies
- B. data filtering profile applied to inbound security policies
- C. data filtering profile applied to outbound security policies
- D. vulnerability profile applied to inbound security policies

Answer: C

Explanation:

NEW QUESTION 167

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 172

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 176

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

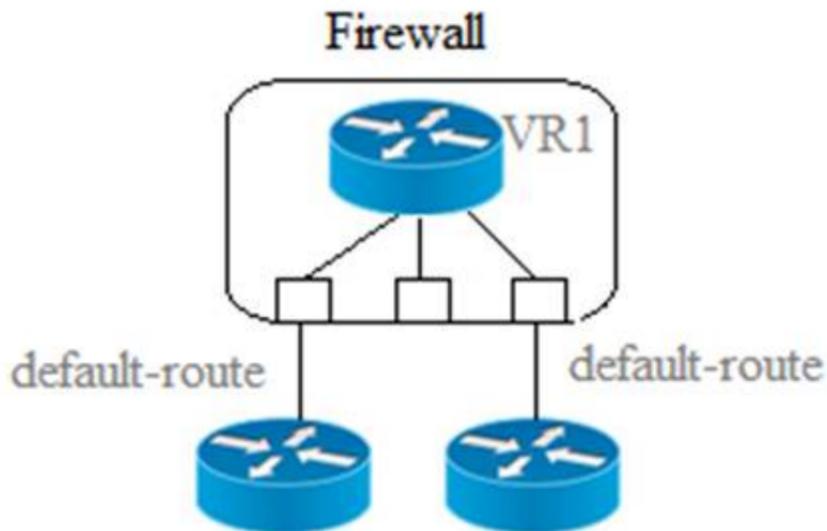
- A. Content updates for firewall A/P HA pairs can only be pushed to the active firewall.
- B. Content updates for firewall A/A HA pairs need a defined master device.
- C. Before deploying content updates, always check content release version compatibility.
- D. After deploying content updates, perform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

Answer: C

NEW QUESTION 181

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

Multiple Static Default Routes



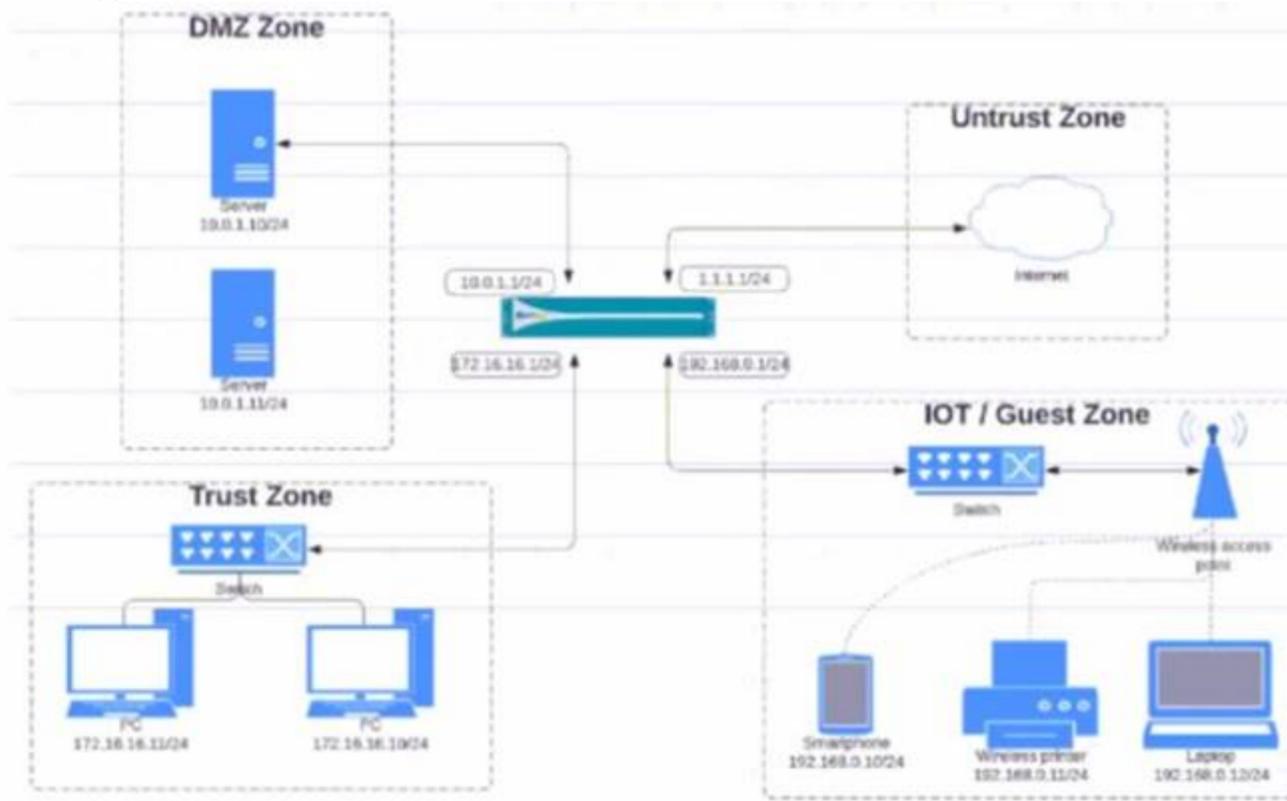
Path monitoring does not determine if route is useable

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

Answer: CD

NEW QUESTION 182

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
01-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 185

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 190

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

- A. XML API
- B. log forwarding auto-tagging
- C. GlobalProtect agent
- D. User-ID Windows-based agent

Answer: AD

Explanation:

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

NEW QUESTION 191

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 194

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 199

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

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

- A. Add all the URLs from the gambling category except powerball.com to the block list and then set the action for the gambling category to allow.
- B. Manually remove powerball.com from the gambling URL category.
- C. Add *.powerball.com to the allow list
- D. Create a custom URL category called PowerBall and add *.powerball.com to the category and set the action to allow.

Answer: CD

Explanation:

NEW QUESTION 200

When is the content inspection performed in the packet flow process?

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

Answer: A

Explanation:

Reference: <https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g00000 0CIVHCA0>

NEW QUESTION 201

Which type firewall configuration contains in-progress configuration changes?

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

Answer: C

NEW QUESTION 205

A network administrator created an intrazone Security policy rule on the firewall. The source zones were set to IT, Finance, and HR. Which two types of traffic will the rule apply to? (Choose two)

- A. Mastered
- B. Not Mastered

Answer: A

NEW QUESTION 208

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

- A. Interzone
- B. Universal
- C. Intrazone

D. Shadowed

Answer: C

NEW QUESTION 209

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?

Data Filtering Profile applied to outbound Security policy rules

- A. Antivirus Profile applied to outbound Security policy rules
- B. Antivirus Profile applied to inbound 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 212

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

- A. decryption profile
- B. destination interface
- C. timeout (min)
- D. application

Answer: D

Explanation:

Reference:

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

NEW QUESTION 213

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 215

An administrator wants to prevent users from submitting corporate credentials in a phishing attack. Which Security profile should be applied?

- A. antivirus
- B. anti-spyware
- C. URL filtering
- D. vulnerability protection

Answer: B

NEW QUESTION 217

What are the two default behaviors for the intrazone-default policy? (Choose two.)

- A. Allow
- B. Logging disabled
- C. Log at Session End
- D. Deny

Answer: AB

NEW QUESTION 220

Your company occupies one floor in a single building. You have two active directory domain controllers on a single network. The firewall's management plane is only slightly utilized.

Which user-ID agent is sufficient in your network?

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

Answer: D

Explanation:

Reference:

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/user-id/map-ip-addresses-to-users/configureuser-mapping-using-the-windows-user-id-agent/configure-the-windows-based-user-id-agent-for-usermapping.html>

NEW QUESTION 223

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 227

Given the screenshot what two types of route is the administrator configuring? (Choose two)



- A. default route
- B. OSPF
- C. BGP
- D. static route

Answer: A

NEW QUESTION 229

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

- A. Select the unified log entry in the side menu.
- B. Modify the number of columns visible on the page
- C. Modify the number of logs visible on each page.
- D. Select the system logs entry in the side menu.

Answer: A

Explanation:

The best way to view a complete overview of the logs is to select the unified log entry in the side menu. The unified log is a single view that displays all the logs generated by the firewall, such as traffic, threat, URL filtering, data filtering, and WildFire logs¹. The unified log allows the administrator to filter, sort, and export the logs based on various criteria, such as time range, severity, source, destination, application, or action¹.

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

References:

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

NEW QUESTION 231

Which two matching criteria are used when creating a Security policy involving NAT? (Choose two.)

- A. Post-NAT address
- B. Post-NAT zone
- C. Pre-NAT zone
- D. Pre-NAT address

Answer: BD

NEW QUESTION 235

Files are sent to the WildFire cloud service via the WildFire Analysis Profile. How are these files used?

- A. WildFire signature updates
- B. Malware analysis
- C. Domain Generation Algorithm (DGA) learning
- D. Spyware analysis

Answer: B

NEW QUESTION 238

Which URL profiling action does not generate a log entry when a user attempts to access that URL?

- A. Override
- B. Allow
- C. Block
- D. Continue

Answer: B

NEW QUESTION 239

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 241

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 244

.....

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](#)