PCNSA$^{\text{Q\&As}}$

Palo Alto Networks Certified Network Security Administrator

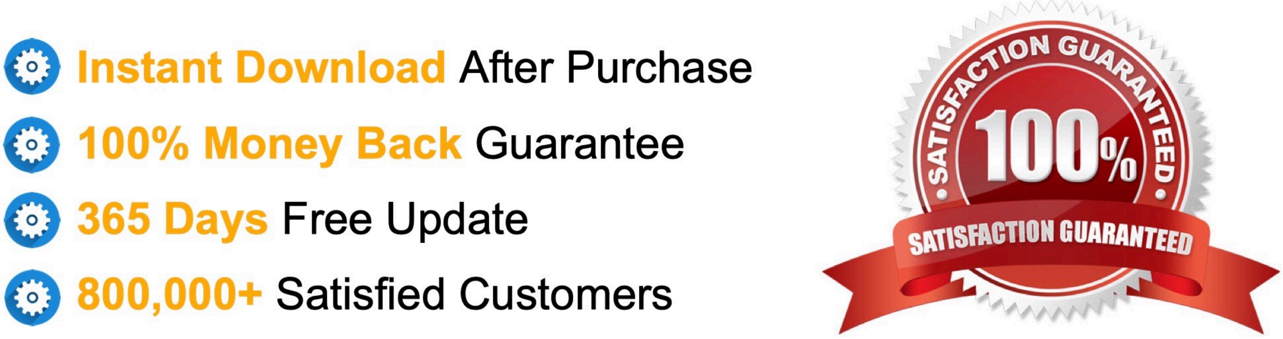
Pass Palo Alto Networks PCNSA Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/pcnsa.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Palo Alto Networks Official Exam Center


Instant Download After Purchase
100% Money Back Guarantee
365 Days Free Update
800,000+ Satisfied Customers
SATISFACTION GUARANTEED
100%
SATISFACTION GUARANTEED

QUESTION 1

Which security policy match condition would an administrator use to block traffic to IP addresses on the Palo Alto Networks Bulletproof IP Addresses list?

A. source address

B. destination address

C. source zone

D. destination zone

Correct Answer: B

QUESTION 2

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

A. Before deploying content updates, always check content release version compatibility.

B. Content updates for firewall A/P HA pairs can only be pushed to the active firewall.

C. Content updates for firewall A/A HA pairs need a defined master device.

D. After deploying content updates, perform a commit and push to Panorama.

Correct Answer: D

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

QUESTION 3

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

A. GlobalProtect

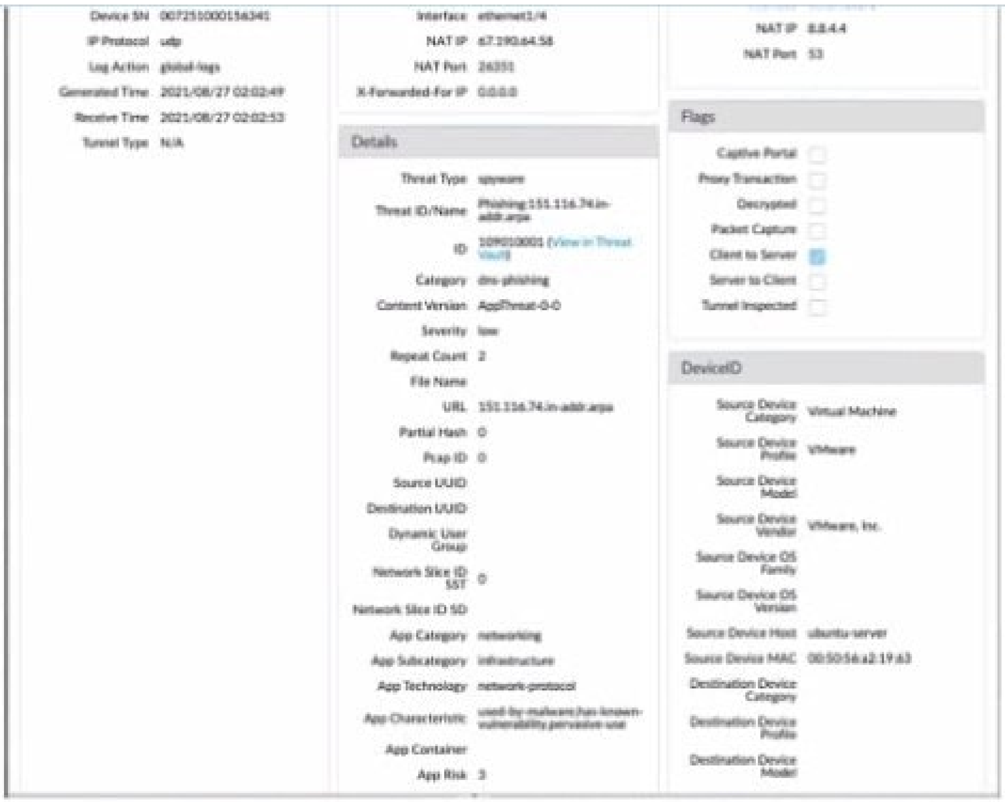
B. Panorama

C. Aperture

D. AutoFocus

Correct Answer: BD

QUESTION 4



Device SN 007251000156341
IP Protocol udp
Log Action global-logs
Generated Time 2021/08/27 02:02:49
Receive Time 2021/08/27 02:02:53
Tunnel Type N/A

Interface ethernet1/4
NAT IP 67.190.64.58
NAT Port 26351
X-Forwarded-For IP 0.0.0.0

Details

Threat Type spyware
Threat ID/Name Phishing:151.116.74.in-addr.arpa
ID 109010001 (View in Threat Vault)
Category dns-phishing
Content Version AppThreat-0-0
Severity low
Repeat Count 2
File Name
URL 151.116.74.in-addr.arpa
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,pervasive-use
App Container
App Risk 3

NAT IP 8.8.4.4
NAT Port 53

Flags

Captive Portal □
Proxy Transaction □
Decrypted □
Packet Capture □
Client to Server ☑
Server to Client □
Tunnel Inspected □

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

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

A. It was blocked by the Vulnerability Protection profile action.

B. It was blocked by the Anti-Virus Security profile action.

C. It was blocked by the Anti-Spyware Profile action.

D. It was blocked by the Security policy action.

Correct Answer: C

QUESTION 5

In which stage of the Cyber-Attack Lifecycle would the attacker inject a PDF file within an email?

A. Weaponization

B. Reconnaissance

C. Installation

D. Command and Control

E. Exploitation

Correct Answer: A

QUESTION 6

Which two statements apply to an Advanced Threat Prevention subscription? (Choose two.)

A. It contains all the features already in a Threat Prevention subscription.

B. It provides the ability to identify evasive and previously unseen command-and-control (C2) threats.

C. When it is active, a WildFire profile is no longer needed.

D. Due to its more advanced signatures, it provides the ability to identify new threats.

Correct Answer: AB

QUESTION 7

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

A. Create a Security policy rule to allow the traffic.

B. Create a new NAT rule with the correct parameters and leave the translation type as None

C. Create a static NAT rule with an application override.

D. Create a static NAT rule translating to the destination interface.

Correct Answer: B

QUESTION 8

Which security profile will provide the best protection against ICMP floods, based on individual combinations of a packet`s source and destination IP address?

A. DoS protection

B. URL filtering

C. packet buffering

D. anti-spyware

Correct Answer: A

QUESTION 9

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

Correct Answer: B

QUESTION 10

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

Correct Answer: D

QUESTION 11

A Panorama administrator would like to create an address object for the DNS server located in the New York City office, but does not want this object added to the other Panorama managed firewalls. Which configuration action should the administrator take when creating the address object?

A. Tag the address object with the New York Office tag.

B. Ensure that Disable Override is cleared.

C. Ensure that the Shared option is checked.

D. Ensure that the Shared option is cleared.

Correct Answer: D

Reference: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/panorama-web-interface/panorama-commit-operations

QUESTION 12

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

A. Wait until all running and pending jobs are finished before committing.

B. Export configuration after each single configuration change performed.

C. Validate configuration changes prior to committing.

D. Disable the automatic commit feature that prioritizes content database installations before committing.

Correct Answer: C

Reference: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-cli-quick-start/use-the-cli/commit-configuration-changes

QUESTION 13

Starting with PAN-OS version 9.1, application dependency information is now reported in which two locations? (Choose two.)

A. on the App Dependency tab in the Commit Statuswindow

B. on the Policy Optimizer\\'sRule Usagepage

C. ontheApplication tab in the Security Policy Rulecreation window

D. ontheObjects>Applicationsbrowser pages

Correct Answer: AC

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

QUESTION 14

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

Correct Answer: A

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

QUESTION 15

A website is unexpectedly allowed due to miscategorization.

What are two ways to resolve this issue for a proper response? (Choose two.)

A. Identify the URL category being assigned to the website. Edit the active URL Filtering profile and update that category\\'s site access settings to block.

B. Create a URL category and assign the affected URL. Update the active URL Filtering profile site access setting for the custom URL category to block.

C. Review the categorization of the website on https://urlfiltering.paloaltonetworks.com. Submit for "request change*, identifying the appropriate categorization, and wait for confirmation before testing again.

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

Correct Answer: BC

Latest PCNSA Dumps PCNSA Practice Test PCNSA Braindumps