

➤ **Vendor: Palo Alto Networks**

➤ **Exam Code: PCNSA**

➤ **Exam Name: Palo Alto Networks Certified Network Security Administrator**

➤ **New Updated Questions from [Braindump2go](#) (Updated in [November/2021](#))**

[Visit Braindump2go and Download Full Version PCNSA Exam Dumps](#)

QUESTION 173

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

QUESTION 174

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

QUESTION 175

Starting with PAN-OS version 9.1, which new type of object is supported for use within the User field of a Security policy rule?

- A. remote username
- B. dynamic user group
- C. static user group
- D. local username

Answer: B

QUESTION 176

Which link in the web interface enables a security administrator to view the Security policy rules that match new application signatures?

[PCNSA Exam Dumps](#) [PCNSA Exam Questions](#) [PCNSA PDF Dumps](#) [PCNSA VCE Dumps](#)

<https://www.braindump2go.com/pcnsa.html>

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

Answer: D

QUESTION 177

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

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

Answer: D

Explanation:

<https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-admin/threat-prevention/best-practices-for-application-and-threat-content-updates#>

QUESTION 178

Which type of firewall configuration contains in-progress configuration changes?

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

Answer: B

QUESTION 179

Which three configuration settings are required on a Palo Alto Network firewall management interface? (Choose three.)

- A. hostname
- B. netmask
- C. default gateway
- D. auto-negotiation
- E. IP address

Answer: BCE

Explanation:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIN7CAK>

QUESTION 180

What is an advantage for using application tags?

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

Answer: B

[PCNSA Exam Dumps](#) [PCNSA Exam Questions](#) [PCNSA PDF Dumps](#) [PCNSA VCE Dumps](#)

<https://www.braindump2go.com/pcnsa.html>

QUESTION 181

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 Now in the Dynamic Update window
- B. after committing the firewall configuration
- C. after installing the update
- D. after downloading the update

Answer: D

Explanation:

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

QUESTION 182

You receive notification about a new malware that infects hosts. An infection results in the infected host attempting to contact a command-and-control server.

Which Security Profile detects and prevents this threat from establishing a command-and-control connection?

- A. Vulnerability Protection Profile applied to outbound Security policy rules.
- B. Anti-Spyware Profile applied to outbound security policies.
- C. Antivirus Profile applied to outbound Security policy rules
- D. Data Filtering Profile applied to outbound Security policy rules.

Answer: B

QUESTION 183

Which statement is true regarding a Best Practice Assessment?

- A. It runs only on firewalls.
- B. It shows how current configuration compares to Palo Alto Networks recommendations.
- C. When guided by an authorized sales engineer, it helps determine the areas of greatest risk where you should focus prevention activities.
- D. It provides a set of questionnaires that help uncover security risk prevention gaps across all areas of network and security architecture.

Answer: B

QUESTION 184

The PowerBall Lottery has reached an unusually high value this week. Your company has decided to raise morale by allowing employees to access the PowerBall Lottery website (www.powerball.com) for just this week. However, the company does not want employees to access any other websites also listed in the URL filtering "gambling" category. Which method allows the employees to access the PowerBall Lottery website but without unblocking access to the "gambling" URL category?

- A. Add just the URL www.powerball.com to a Security policy allow rule.
- B. Manually remove [powerball.com](http://www.powerball.com) from the gambling URL category.
- C. Add *.[powerball.com](http://www.powerball.com) to the URL Filtering allow list.
- D. Create a custom URL category, add *.[powerball.com](http://www.powerball.com) to it and allow it in the Security Profile.

Answer: CD

QUESTION 185

Which Palo Alto Networks service protects cloud-based applications such as Dropbox and Salesforce by monitoring permissions and shares and scanning files for sensitive information?

[PCNSA Exam Dumps](#) [PCNSA Exam Questions](#) [PCNSA PDF Dumps](#) [PCNSA VCE Dumps](#)

<https://www.braindump2go.com/pcnsa.html>

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

Answer: A

QUESTION 186

In a Security policy, what is the quickest way to reset all policy rule hit counters to zero?

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

Answer: C

Explanation:

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface-help/policies/policies-security/creating-and-managing-policies>

QUESTION 187

Based on the Security policy rules shown, SSH will be allowed on which port?

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

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

Answer: A

QUESTION 188

You receive notification about new malware that is being used to attack hosts. The malware exploits a software bug in 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 Protection Profile applied to inbound Security policy rules

Answer: B

QUESTION 189

Palo Alto Networks firewall architecture accelerates content inspection performance while minimizing latency using which two components? (Choose two.)

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

Answer: CD

QUESTION 190

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

Answer: C

Explanation:

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

QUESTION 191

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

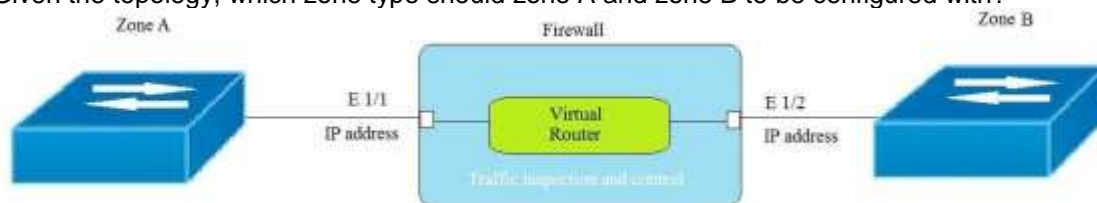
Answer: C

Explanation:

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

QUESTION 192

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



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

Answer: A

QUESTION 193

Assume a custom URL Category Object of "NO-FILES" has been created to identify a specific website? How can file uploading/downloading be restricted for the website while permitting general browsing access to that

[PCNSA Exam Dumps](#) [PCNSA Exam Questions](#) [PCNSA PDF Dumps](#) [PCNSA VCE Dumps](#)

<https://www.braindump2go.com/pcnsa.html>

website?

- A. Create a Security policy with a URL Filtering profile that references the site access setting of block to NO-FILES.
- B. Create a Security policy that references NO-FILES as a URL Category qualifier with an appropriate File Blocking profile.
- C. Create a Security policy with a URL Filtering profile that references the site access setting of continue to NO-FILES.
- D. Create a Security policy that references NO-FILES as a URL Category qualifier with an appropriate Data Filtering profile.

Answer: A

Explanation:

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/threat-prevention/set-up-file-blocking>

QUESTION 194

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

Answer: D

Explanation:

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

QUESTION 195

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

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

Answer: C