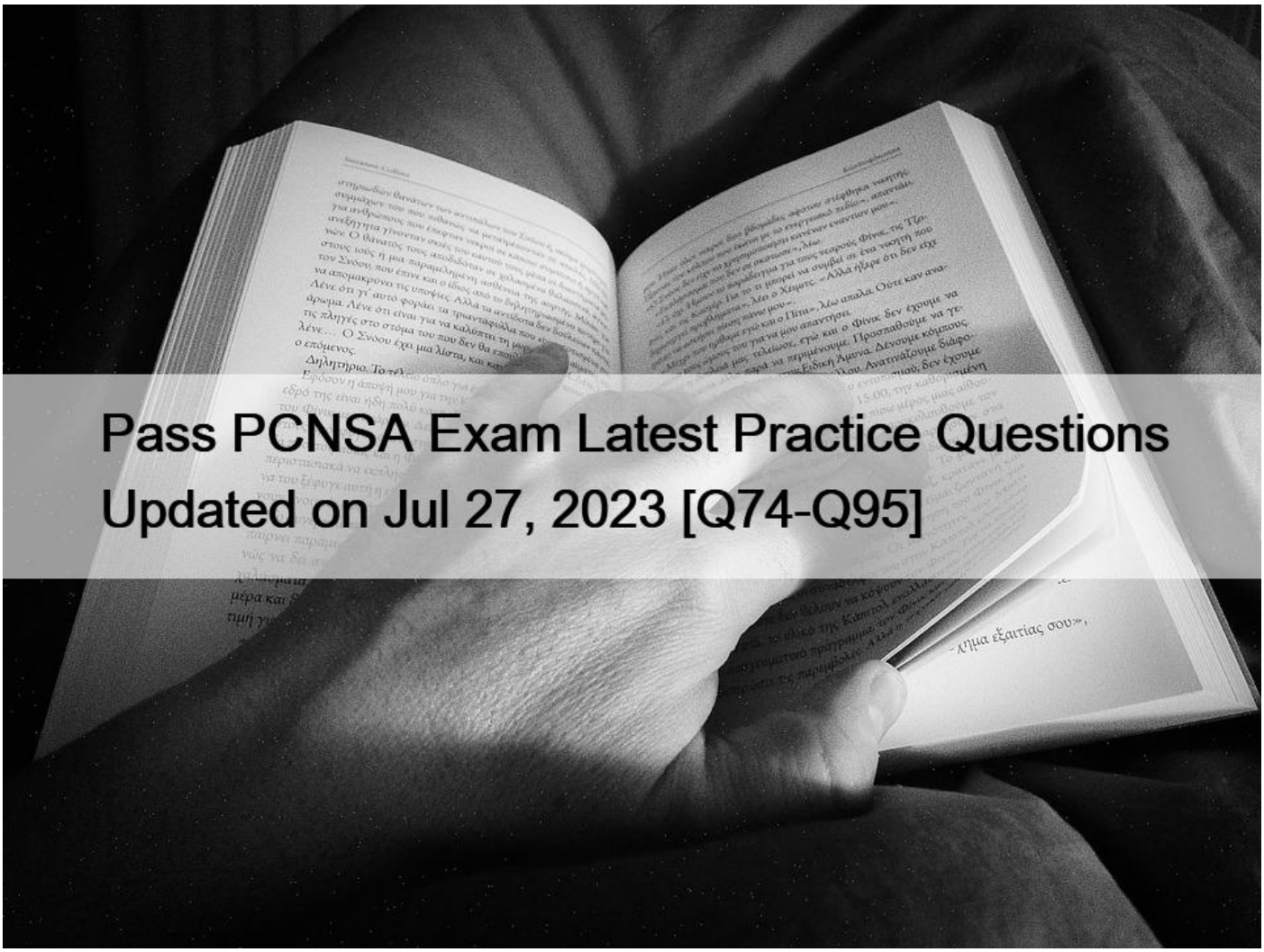
# Pass PCNSA Exam Latest Practice Questions Updated on Jul 27, 2023 [Q74-Q95




**Pass PCNSA Exam Latest Practice Questions Updated on Jul 27, 2023 Palo Alto Networks PCNSA Study Guide Archives**

Palo Alto Networks PCNSA Certification Exam is targeted at network security administrators, network engineers, and other IT professionals who are responsible for deploying and managing Palo Alto Networks firewalls in their organizations. Candidates for this certification exam should have a good understanding of network security concepts and protocols, as well as hands-on experience in configuring and managing firewalls.

**NO.74** Complete the statement. A security profile can block or allow traffic.
* on unknown-tcp or unknown-udp traffic
* after it is evaluated by a security policy that allows traffic
* before it is evaluated by a security policy
* after it is evaluated by a security policy that allows or blocks traffic

**NO.75** An administrator wants to prevent hacking attacks through DNS queries to malicious domains.

Which two DNS policy actions can the administrator choose in the Anti-Spyware Security Profile?

(Choose two.)
* deny
* block
* sinkhole
* override

**NO.76** What is the Anti-Spyware Security profile default action?
* Sinkhole
* Reset-client
* Drop
* Reset-both

https://docs.paloaltonetworks.com/network-security/security-policy/security-profiles/security- profile-anti-spyware

**NO.77** The firewall sends employees an application block page when they try to access Youtube.

Which Security policy rule is blocking the youtube application?

| | | | 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 |



* intrazone-default
* Deny Google
* allowed-security services
* interzone-default

**NO.78** Which operations are allowed when working with App-ID application tags?
* Predefined tags may be deleted.
* Predefined tags may be augmented by custom tags.
* Predefined tags may be modified.
* Predefined tags may be updated by WildFire dynamic updates.

**NO.79** Four configuration choices are listed, and each could be used to block access to a specific URL. If you configured each choice to block the same URL then which choice would be the last to block access to the URL?
* EDL in URL Filtering Profile
* Custom URL category in URL Filtering Profile
* Custom URL category in Security policy rule
* PAN-DB URL category in URL Filtering Profile

**NO.80** Which statement is true regarding a Best Practice Assessment?
* The BPA tool can be run only on firewalls
* It provides a percentage of adoption for each assessment area
* The assessment, guided by an experienced sales engineer, helps determine the areas of greatest risk where you should focus prevention activities
* It provides a set of questionnaires that help uncover security risk prevention gaps across all areas of network and security architecture

Explanation/Reference: https://docs.paloaltonetworks.com/best-practices/8-1/data-center-best-practices/data-center-best-practice-security-policy/use-palo-alto-networks-assessment-and-review-tools

**NO.81** Given the screenshot, what are two correct statements about the logged traffic? (Choose two.)

| TYPE | FROM ZONE | TO ZONE | INGRESS I/F | SOURCE | NAT APPLIED | EGRESS I/F | DESTINATION | TO PORT | APPLICATION | ACTION | SE RE |
|---|---|---|---|---|---|---|---|---|---|---|---|
| end | LAN | Internet | ethernet1/2 | 192.168.200.100 | yes | ethernet1/5 | 198.54.12.97 | 443 | web-browsing | allow | thr |



* The web session was unsuccessfully decrypted.
* The traffic was denied by security profile.
* The traffic was denied by URL filtering.
* The web session was decrypted.

The session was decrypted because you can see web-browsing over port 443 The traffic was denied by a security profile.

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000HCQlCAO

**NO.82** Which two features can be used to tag a username so that it is included in a dynamic user group?

(Choose two.)
* GlobalProtect agent
* XML API
* User-ID Windows-based agent
* log forwarding auto-tagging

Usernames also can be tagged and untagged using the autotagging feature in a Log Forwarding Profile. You also can program another utility to invoke PAN-OS XML API commands to tag or untag usernames. In the web interface you can use logical AND or OR operators with the tags to better filter or match against. You can configure a timeout value that determines when a username will be untagged automatically.

https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/datasheets/education/pcns e-study-guide.pdf

**NO.83** 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?


* Translation Type
* Interface
* Address Type
* IP Address

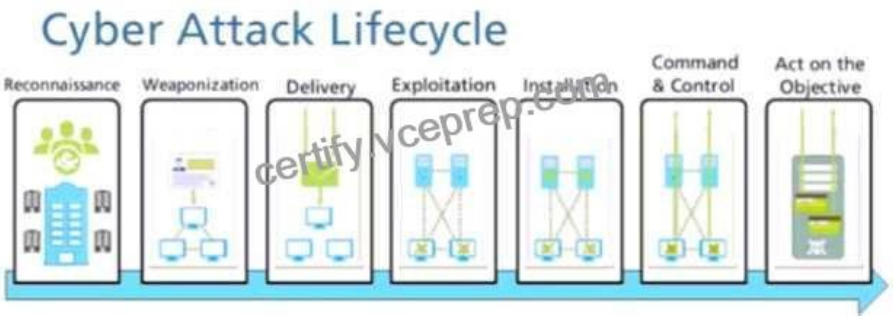
**NO.84** An administrator needs to add capability to perform real-time signature lookups to block or sinkhole all known malware domains.

Which type of single unified engine will get this result?
* User-ID
* App-ID
* Security Processing Engine
* Content-ID

Content-IDTM combines a real-time threat prevention engine with a comprehensive URL database and elements of application identification to limit unauthorized data and file transfers and detect and block a wide range of exploits, malware, dangerous web surfing as well as targeted and unknown threats.

https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/tech-briefs/techbrief- content-id.pdf

**NO.85** Given the cyber-attack lifecycle diagram identify the stage in which the attacker can run malicious code against a vulnerability in a targeted machine.




* Exploitation
* Installation
* Reconnaissance

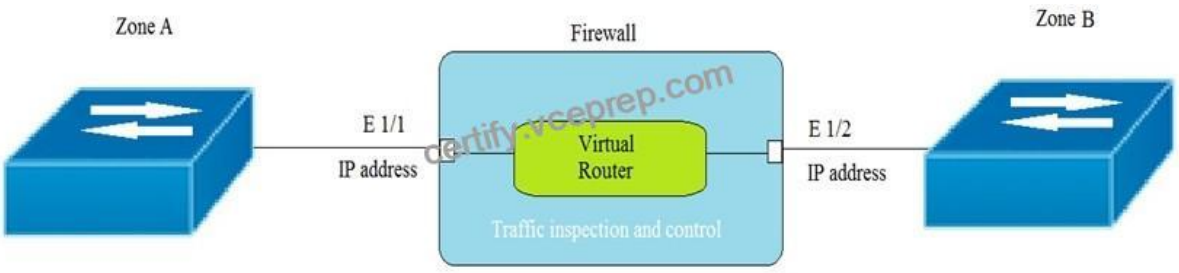
* Act on the Objective

**NO.86** What is considered best practice with regards to committing configuration changes?
* Disable the automatic commit feature that prioritizes content database installations before committing
* Validate configuration changes prior to committing
* Wait until all running and pending jobs are finished before committing
* Export configuration after each single configuration change performed

**NO.87** An administrator would like to override the default deny action for a given application, and instead would like to block the traffic.

Which security policy action causes this?
* Drop
* Drop, send ICMP Unreachable
* Reset both
* Reset client

**NO.88** Given the topology, which zone type should zone A and zone B to be configured with?




* Layer3
* Tap
* Layer2
* Virtual Wire

**NO.89** 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?
* Traffic is being denied on the interzone-default policy.
* The Log Forwarding profile is not configured on the policy.
* The interzone-default policy is disabled by default
* Logging on the interzone-default policy is disabled

**NO.90** Based on the show security policy rule would match all FTP traffic from the inside zone to the outside zone?

| | Name | Type | Source Zone | Source Address | Destination Zone | Destination Address | Application | Service | Action |
|---|---|---|---|---|---|---|---|---|---|
| 1 | inside-portal | universal | inside | any | outside | 203.0.113.20 | any | any | Allow |
| 2 | internal-inside-dmz | universal | inside | any | dmz | any | ftp<br>ssh<br>ssl<br>web-browsing | application-default | Allow |
| 3 | egress-outside | universal | inside | any | outside | any | any | application-default | Allow |
| 4 | egress-outside-content-id | universal | inside | any | outside | any | any | application-default | Allow |
| 5 | danger-simulated-traffic | universal | danger | any | danger | any | any | application-default | Allow |
| 6 | intrazone-default | intrazone | any | any | (intrazone) | any | any | any | Allow |
| 7 | intrazone-default | intrazone | any | any | any | any | any | any | Deny |



* internal-inside-dmz
* engress outside
* inside-portal
* intercone-default

**NO.91** An administrator would like to silently drop traffic from the internet to a ftp server.

Which Security policy action should the administrator select?
* Reset-server
* Block
* Deny
* Drop

**NO.92** Which three statements describe the operation of Security policy rules and Security Profiles?

(Choose three.)
* Security policy rules inspect but do not block traffic.
* Security Profile should be used only on allowed traffic.
* Security Profile are attached to security policy rules.
* Security Policy rules are attached to Security Profiles.
* Security Policy rules can block or allow traffic.

**NO.93** An administrator would like to block access to a web server, while also preserving resources and minimizing half-open sockets. What are two security policy actions the administrator can select? (Choose two.)
* Reset server
* Reset both
* Drop
* Deny

**NO.94** Which option shows the attributes that are selectable when setting up application filters?
* Category, Subcategory, Technology, and Characteristic
* Category, Subcategory, Technology, Risk, and Characteristic
* Name, Category, Technology, Risk, and Characteristic
* Category, Subcategory, Risk, Standard Ports, and Technology

https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-web-interface-help/objects/objects-application-filters

**NO.95** Which type of policy allows an administrator to both enforce rules and take action?
* Authentication

* Security
* NAT
* Decryption

The PCNSA certification exam covers a wide range of topics related to Palo Alto Networks next-generation firewalls. PCNSA exam tests the candidate's knowledge of network security architecture, firewall configuration, security policies, VPNs, user identification, and application control. PCNSA exam also assesses the candidate's ability to troubleshoot common network security issues and perform basic administrative tasks using the Palo Alto Networks firewall management interface.

**PCNSA Questions Prepare with Learning Information:** https://www.vceprep.com/PCNSA-latest-vce-prep.html]