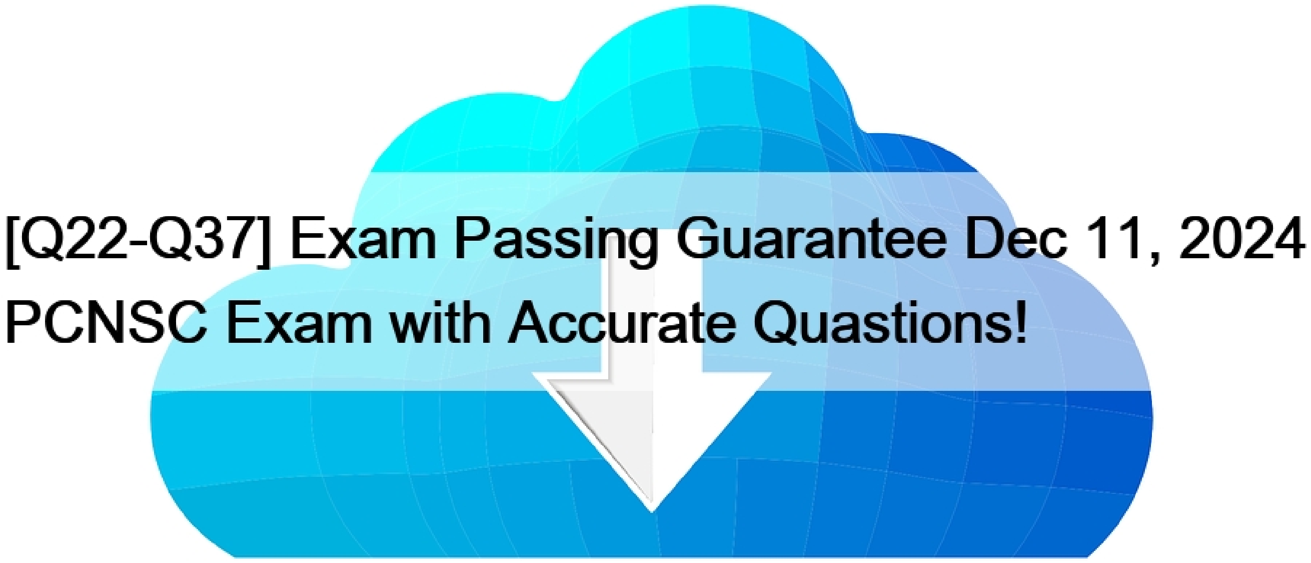
[Q22-Q37 Exam Passing Guarantee Dec 11, 2024 PCNSC Exam with Accurate Quastions!



Exam Passing Guarantee Dec 11, 2024 PCNSC Exam with Accurate Quastions!
Test Engine to Practice Test for PCNSC Valid and Updated Dumps

Q22. An administrator sees several inbound sessions identified as unknown tcp in the Traffic logs. The administrator determines that these sessions are from external users accessing the company&#8217;s propriety accounting application. The administrator wants to reliability identity this as their accounting application and to scan this traffic for threats.

Which option would achieve this result?
* Create an Application Override policy and a custom threat signature for the application.
* Create a custom App-ID and use the &#8220;ordered condition cheek box.
* Create an Application Override policy
* Create a custom App-ID and enable scanning on the advanced tab.

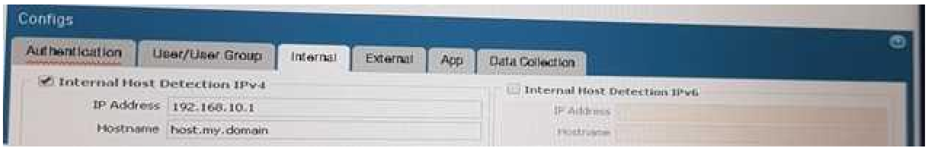
Q23. An administrator has enabled OSPF on a virtual router on the NGFW OSPF is not adding new routes to the virtual router.

Which two options enable the administrator top troubleshoot this issue? (Choose two.)
* Perform a traffic pcap at the routing stage.

* View System logs.
* Add a redistribution profile to forward as BGP updates.
* View Runtime Status virtual router.

Q24. View the GlobalProtect configuration screen capture.

What is the purpose of this configuration?



☑ Internal Host Detection IPv4
IP Address 192.168.10.1
Hostname host.my.domain

□ Internal Host Detection IPv6
IP Address
Hostname

* It forces an internal client to connect to an internal gateway at IP address 192 168 10 I.
* It configures the tunnel address of all internal clients lo an IP address range starting at 192 168 10 1.
* It forces the firewall to perform a dynamic DNS update, Which adds the internal gateway&#8217;s hostname and IP address to the DNS server.
* It enables a Client to perform a reverse DNS lookup on 192 .168. 10 .1. to delect it is an internal client.

Q25. Which three user authentication services can be modified in to provide the Palo Alto Networks NGFW with both username and role names? (Choose three.)
* PAP
* SAML
* LDAP
* TACACS+
* RADIUS
* Kerberos

Q26. What is the purpose of the WildFire Analysis Profile in a security policy?
* To specify which files are sent to WildFire for analysis
* To configure the WildFire subscription settings
* To enable WildFire to analyze all network traffic
* To define the action to be taken on files analyzed by WildFire

Q27. Which prerequisite must be satisfied before creating an SSH proxy Decryption policy?
* No prerequisites are required
* SSH keys must be manually generated
* Both SSH keys and SSL certificates must be generated
* SSL certificates must be generated

Q28. TAC has requested a PCAP on your Panorama lo see why the DNS app is having intermittent issues resolving FODN What is the appropriate CLI command1*
* tcp dump snaplen 53 filter &#8220;tcp 53&#8221;
* tcpdump snaplen 0 filter &#8220;port 53&#8221;
* tcp dump snap-en 0 filter &#8220;app dns&#8221;
* tcpdump snaplen 53 filter &#8220;port 53&#8221;

To capture a PCAP on your Panorama to troubleshoot DNS resolution issues, the appropriate CLI command is:

B:tcpdump snaplen 0 filter &#8220;port 53&#8221;

This command captures packets with no size limit (snaplen 0) and filters the traffic for port 53, which is used by DNS. This is the most straightforward and comprehensive way to capture all DNS traffic for analysis.

References:

* Palo Alto Networks &#8211; Using tcpdump on PAN-OS: https://knowledgebase.paloaltonetworks.com

* Palo Alto Networks &#8211; Troubleshooting Network Connectivity Issues: https://docs.paloaltonetworks.com

Q29. The firewall identified a popular application as a unknown-tcp. Which options are available to identify the application? (Choose two.)
* Create a Security policy to identify the customer application.
* Create a customer object for the customer application server to identify the custom application.
* Submit an App-ID request to Palo Alto Networks.
* Create a custom application.

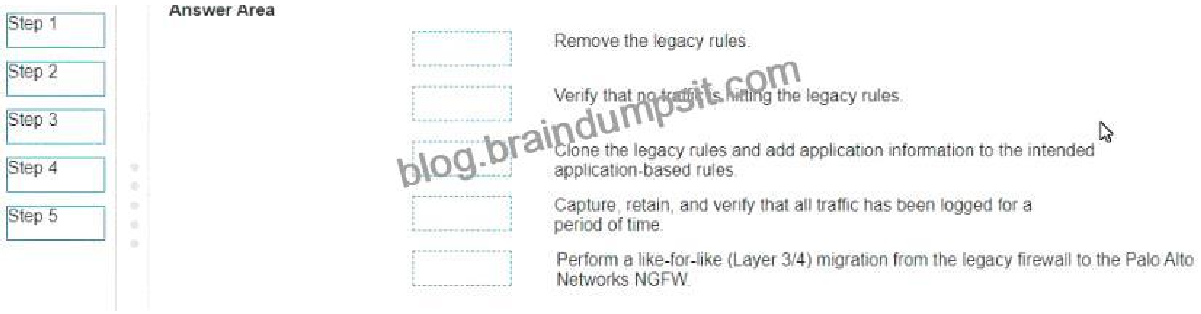
Q30. Which CLI command enables an administrator to view detail about the firewall including uptime. PAN -OS version, and serial number?
* debug system details
* Show system detail
* Show system info
* Show session info

Q31. Which Palo Alto Networks feature allows you to create dynamic security policies based on the behavior of the devices in your network?
* Behavioral Threat Detection
* Cortex XDR
* App-ID
* Dynamic Address Groups

Q32. An administrator pushes a new configuration from panorama to a pair of firewalls that are configured as active/passive HA pair.

Which NGFW receives the configuration from panorama?
* the active firewall, which then synchronizes to the passive firewall
* the passive firewall, which then synchronizes to the active firewall
* both the active and passive firewalls independently, with no synchronization afterward
* both the active and passive firewalls, which then synchronizes with each other

Q33. Match the App-ID adoption task with its order in the process.



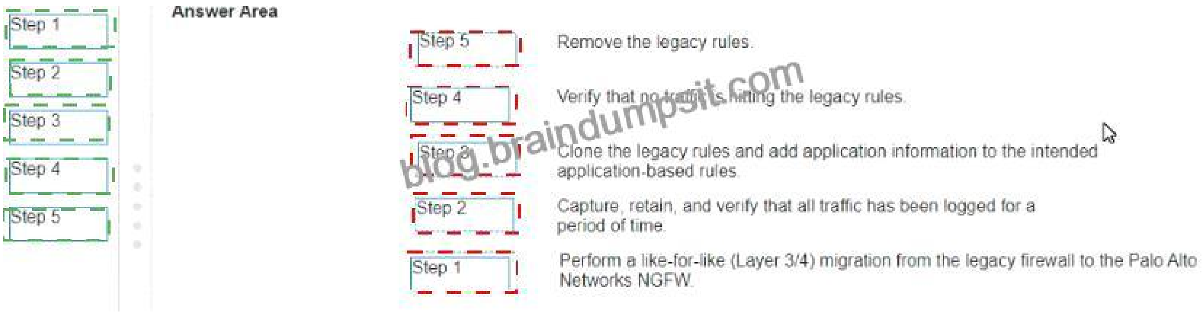
Remove the legacy rules.

Verify that no traffic is hitting the legacy rules.

Clone the legacy rules and add application information to the intended application-based rules.

Capture, retain, and verify that all traffic has been logged for a period of time.

Perform a like-for-like (Layer 3/4) migration from the legacy firewall to the Palo Alto Networks NGFW.



Step 1
Step 2
Step 3
Step 4
Step 5

Answer Area

Step 5	Remove the legacy rules.
Step 4	Verify that no traffic is hitting the legacy rules.
Step 3	Clone the legacy rules and add application information to the intended application-based rules.
Step 2	Capture, retain, and verify that all traffic has been logged for a period of time.
Step 1	Perform a like-for-like (Layer 3/4) migration from the legacy firewall to the Palo Alto Networks NGFW.

Explanation:

To match the App-ID adoption task with its order in the process, follow these steps:

* Perform a like-for-like (Layer 3/4) migration from the legacy firewall to the Palo Alto Networks NGFW.

* This is the initial step to ensure that the Palo Alto Networks NGFW is in place and functioning with the existing security policies.

* Capture, retain, and verify that all traffic has been logged for a period of time.

* This step involves enabling logging and monitoring traffic to understand the application usage and to ensure that all traffic is being logged.

* Clone the legacy rules and add application information to the intended application-based rules.

* This step involves creating copies of the existing rules and enhancing them with application-specific information using App-ID.

* Verify that no traffic is hitting the legacy rules.

* After creating application-based rules, ensure that traffic is now hitting these new rules instead of the legacy rules. This indicates that the transition to App-ID based policies is successful.

* Remove the legacy rules.

* Once it is confirmed that no traffic is hitting the legacy rules and the new App-ID based rules are effectively managing the traffic, the legacy rules can be safely removed.

Order in Process:

* Perform a like-for-like (Layer 3/4) migration from the legacy firewall to the Palo Alto Networks NGFW.

* Capture, retain, and verify that all traffic has been logged for a period of time.

* Clone the legacy rules and add application information to the intended application-based rules.

* Verify that no traffic is hitting the legacy rules.

* Remove the legacy rules.

References:

* Palo Alto Networks &#8211; App-ID Best Practices: https://docs.paloaltonetworks.com/best-practices

* Palo Alto Networks &#8211; Migration from Legacy Firewalls: https://docs.paloaltonetworks.com/migration

Q34. A web server is hosted in the DMZ and the server re configured to listen for income connections on TCP port

443. A Security policies rules allowing access from the Trust zone to the DMZ zone needs to be configured to allow web-browsing access. The web server host its contents over Traffic from Trust to DMZ is being decrypted with a Forward Proxy rule.

Which combination of service and application, and order of Security policy rules needs to be configured to allow cleaned web-browsing traffic to the server on tcp/443?
* Rule# 1 application: ssl; service application-default: action allow

Role # 2 application web browsing, service application default, action allow
* Rule #1application web-browsing, service service imp action allow

Rule #2 application ssl. service application -default, action allow
* Rule#1 application web-brows.no service application-default, action allow Rule #2 application ssl. Service application-default, action allow
* Rule#1application: web-biows.no; service service-https action allow

Rule#2 application ssl. Service application-default, action allow

Q35. Which category of Vulnerability Signatures is most likely to trigger false positive alerts?
* code-execution
* phishing
* info-leak
* brute-force
The category of Vulnerability Signatures that is most likely to trigger false positive alerts is:

C:info-leak

Information leakage signatures are designed to detect attempts to access or disclose sensitive information.

These signatures can be prone to false positives because benign activities or legitimate data transmissions can sometimes be mistakenly identified as information leaks.

References:

* Palo Alto Networks &#8211; Managing False Positives in Threat Prevention:

https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/threat-prevention/manage-false-positives-in-

* Palo Alto Networks &#8211; Vulnerability Protection:

https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/threat-prevention/vulnerability-protection

Q36. Which two action would be part of an automatic solution that would block sites with untrusted certificates without enabling SSL forward proxy? (Choose two.)
* Configure an EDL to pull IP Addresses of known sites resolved from a CRL.
* Create a Security Policy rule with vulnerability Security Profile attached.
* Create a no-decrypt Decryption Policy rule.
* Enable the &#8220;Block seasons with untrusted Issuers- setting.
* Configure a Dynamic Address Group for untrusted sites.

Q37. Which of the following is a primary use case for the Decryption Broker feature?
* Managing multiple decryption rules
* Sharing decrypted traffic with multiple security appliances
* Decrypting outbound SSL traffic
* Aggregating traffic logs from different sources

To be eligible for the PCNSC Exam, candidates must have a minimum of six months of experience working with Palo Alto Networks technologies. PCNSC exam consists of 75 multiple-choice questions and must be completed within 90 minutes. PCNSC exam is administered online and can be taken at any time. Upon passing the exam, candidates are awarded the PCNSC certification, which is valid for two years. Palo Alto Networks Certified Network Security Consultant certification provides a competitive edge in the job market and demonstrates the ability to effectively manage and secure a network using Palo Alto Networks technologies.

Exam Questions for PCNSC Updated Versions With Test Engine: https://www.braindumpsit.com/PCNSC_real-exam.html]