

Palo Alto Networks Certified Network Security Engineer

1. Which CLI command is used to simulate traffic going through the firewall and determine which Security policy rule, NAT translation, static route, or PBF rule will be triggered by the traffic?

A. check

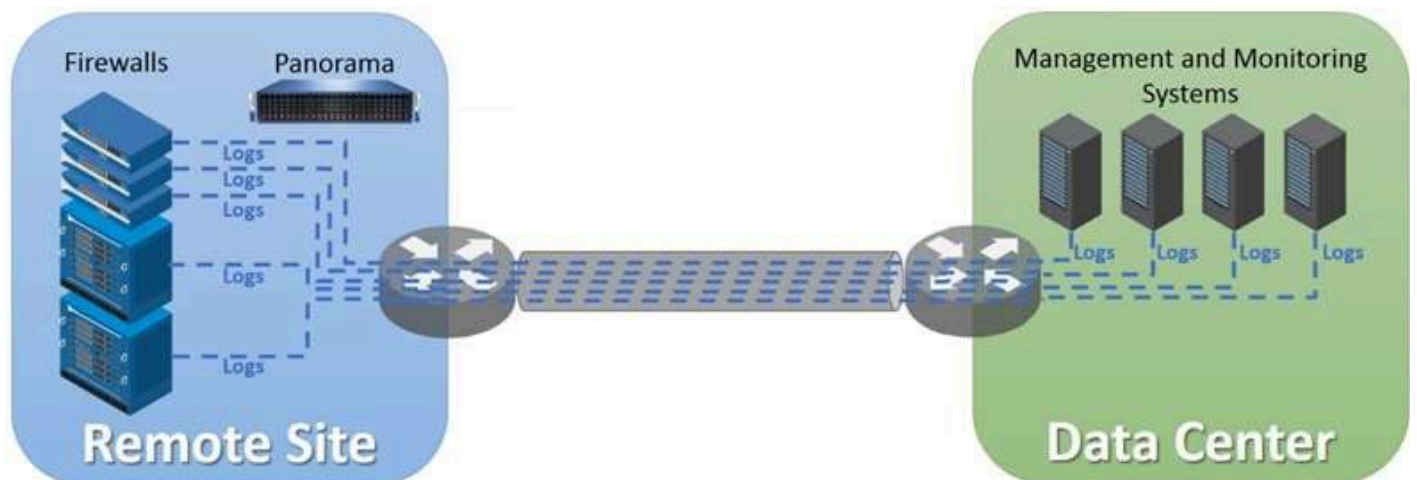
B. find

C. test

D. sim

Answer(s): C

2. Refer to the exhibit.



An organization has Palo Alto Networks NGFWs that send logs to remote monitoring and security management platforms. The network team has reported excessive traffic on the corporate WAN. How could the Palo Alto Networks NGFW administrator reduce WAN traffic while maintaining support for all the existing monitoring/security platforms?

A. Forward logs from firewalls only to Panorama and have Panorama forward logs to other external services.

B. Forward logs from external sources to Panorama for correlation, and from Panorama send them to the NGFW.

C. Configure log compression and optimization features on all remote firewalls.

D. Any configuration on an M-500 would address the insufficient bandwidth concerns.

Answer(s): A

3. A customer wants to set up a VLAN interface for a Layer 2 Ethernet port.

Which two mandatory options are used to configure a VLAN interface? (Choose two.)

A. Virtual router

B. Security zone

C. ARP entries

D. Netflow Profile

Answer(s): A B

4. An administrator has been asked to configure a Palo Alto Networks NGFW to provide protection against worms and trojans.

Which Security Profile type will protect against worms and trojans?

A. Anti-Spyware

B. Instruction Prevention

C. File Blocking

D. Antivirus

Answer(s): D

5. A company needs to preconfigure firewalls to be sent to remote sites with the least amount of preconfiguration. Once deployed, each firewall must establish secure tunnels back to multiple regional data centers to include the future regional data centers.

Which VPN configuration would adapt to changes when deployed to the future site?

A. Preconfigured GlobalProtect satellite

B. Preconfigured GlobalProtect client

C. Preconfigured IPsec tunnels

D. Preconfigured PPTP Tunnels

Answer(s): A

6. An administrator has been asked to configure active/passive HA for a pair of Palo Alto Networks NGFWs. The administrator assigns priority 100 to the active firewall. Which priority is correct for the passive firewall?

A. 0

B. 99

C. 1

D. 255

Answer(s): D

7. An administrator pushes a new configuration from Panorama to a pair of firewalls that are configured as an active/passive HA pair. Which NGFW receives the configuration from Panorama?

A. The passive firewall, which then synchronizes to the active firewall

B. The active firewall, which then synchronizes to the passive firewall

C. Both the active and passive firewalls, which then synchronize with each other

D. Both the active and passive firewalls independently, with no synchronization afterward

Answer(s): D

8. An administrator cannot see any Traffic logs from the Palo Alto Networks NGFW in Panorama reports. The configuration problem seems to be on the firewall. Which settings, if configured incorrectly, most likely would stop only Traffic logs from being sent from the firewall to Panorama?

A.

B.

C.

D.

Answer(s): B

9. When configuring a GlobalProtect Portal, what is the purpose of specifying an Authentication Profile?

- A. To enable Gateway authentication to the Portal
- B. To enable Portal authentication to the Gateway
- C. To enable user authentication to the Portal
- D. To enable client machine authentication to the Portal

Answer(s): C

10. If a template stack is assigned to a device and the stack includes three templates with overlapping settings, which settings are published to the device when the template stack is pushed?

- A. The settings assigned to the template that is on top of the stack.
- B. The administrator will be promoted to choose the settings for that chosen firewall.
- C. All the settings configured in all templates.
- D. Depending on the firewall location, Panorama decides with settings to send.

Answer(s): A

11. Which method will dynamically register tags on the Palo Alto Networks NGFW?

- A. Restful API or the VMware API on the firewall or on the User-ID agent or the ready-only domain controller(RODC)
- B. Restful API or the VMware API on the firewall or on the User-ID agent
- C. XML API or the VMware API on the firewall or on the User-ID agent or the CLI
- D. XML API or the VM Monitoring agent on the NGFW or on the User-ID agent

Answer(s): D

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

A. Configure the option for "Threshold".

B. Disable automatic updates during weekdays.

C. Automatically "download only" and then install Applications and Threats later, after the administrator approves the update.

D. Automatically "download and install" but with the "disable new applications" option used.

Answer(s): A

13. To connect the Palo Alto Networks firewall to AutoFocus, which setting must be enabled?

A. Device>Setup>Services>AutoFocus

B. Device> Setup>Management >AutoFocus

C. AutoFocus is enabled by default on the Palo Alto Networks NGFW

D. Device>Setup>WildFire>AutoFocus

E. Device>Setup> Management> Logging and Reporting Settings

Answer(s): B

14. An administrator encountered problems with inbound decryption. Which option should the administrator investigate as part of triage?

A. Security policy rule allowing SSL to the target server

B. Firewall connectivity to a CRL

C. Root certificate imported into the firewall with "Trust" enabled

D. Importation of a certificate from an HSM

Answer(s): A

15. Which two virtualization platforms officially support the deployment of Palo Alto Networks VM-Series firewalls? (Choose two.)

A. Red Hat Enterprise Virtualization (RHEV)

B. Kernel Virtualization Module (KVM)

C. Boot Strap Virtualization Module (BSVM)

D. Microsoft Hyper-V

Answer(s): B D

16. Which User-ID method maps IP addresses to usernames for users connecting through an 802.1x-enabled wireless network device that has no native integration with PAN-OS® software?

A. XML API

B. Port Mapping

C. Client Probing

D. Server Monitoring

Answer(s): A

17. Decrypted packets from the website <https://www.microsoft.com> will appear as which application and service within the Traffic log?

A. web-browsing and 443

B. SSL and 80

C. SSL and 443

D. web-browsing and 80

Answer(s): A

18. Which PAN-OS® policy must you configure to force a user to provide additional credentials before he is allowed to access an internal application that contains highly-sensitive business data?

A. Security policy

B. Decryption policy

C. Authentication policy

D. Application Override policy

Answer(s): C

19. A Security policy rule is configured with a Vulnerability Protection Profile and an action of “Deny”. Which action will this cause configuration on the matched traffic?

A. The configuration is invalid. The Profile Settings section will be grayed out when the Action is set to “Deny”.

B. The configuration will allow the matched session unless a vulnerability signature is detected. The “Deny” action will supersede the per-severity defined actions defined in the associated Vulnerability Protection Profile.

C. The configuration is invalid. It will cause the firewall to skip this Security policy rule. A warning will be displayed during a commit.

D. The configuration is valid. It will cause the firewall to deny the matched sessions. Any configured Security Profiles have no effect if the Security policy rule action is set to “Deny”.

Answer(s): D

20. A user's traffic traversing a Palo Alto Networks NGFW sometimes can reach <http://www.company.com>. At other times the session times out. The NGFW has been configured with a PBF rule that the user's traffic matches when it goes to <http://www.company.com>.

How can the firewall be configured automatically disable the PBF rule if the next hop goes down?

A. Create and add a Monitor Profile with an action of Wait Recover in the PBF rule in question.

B. Create and add a Monitor Profile with an action of Fail Over in the PBF rule in question.

C. Enable and configure a Link Monitoring Profile for the external interface of the firewall.

D. Configure path monitoring for the next hop gateway on the default route in the virtual router.

Answer(s): B
