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

Correct Answer: B
Explanation:
https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/getting-started/enable-autofocus-threat-intelligence

QUESTION 42
Which protection feature is available only in a Zone Protection Profile?

A. SYN Flood Protection using SYN Flood Cookies
B. ICMP Flood Protection
C. Port Scan Protection
D. UDP Flood Protections

Correct Answer: A

QUESTION 43
An administratorpushes 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

Correct Answer: C

QUESTION 44
Which GlobalProtect Client connect method requires the distribution and use of machine certificates?

A. User-logon (Always on)
B. At-boot
C. On-demand
D. Pre-logon

Correct Answer: D

QUESTION 45
The administrator has enabled BGP on a virtual router on the Palo Alto Networks NGFW, but new routes do not seem to be populating the virtual router. Which two options would help the administrator troubleshoot this issue? (Choose two.)

A. View the System logs and look for the error messages about BGP.

B. Perform a traffic pcap on the NGFW to see any BGP problems.
C. View the Runtime Stats and look for problems with BGP configuration.
D. View the ACC tab to isolate routing issues.

Correct Answer: CD

QUESTION 46
Which menu item enables a firewall administrator to see details about traffic that is currently
active through the NGFW?

A. App Scope
B. ACC
C. Session Browser
D. System Logs

Correct Answer: C

QUESTION 47
An administrator has users accessing network resources through Citrix XenApp 7 x. Which User-
ID mapping solution will map multiple users who are using Citrix to connect to the network and
access resources?

A. Client Probing
B. Terminal Services agent
C. GlobalProtect
D. Syslog Monitoring

Correct Answer: B

QUESTION 48
An administrator wants to upgrade an NGFW from PAN-OS® 7.1. 2 to PAN-OS® 8.0.2 The
firewall is not a part of an HA pair. What needs to be updated first?

A. XML Agent
B. Applications and Threats
C. WildFire
D. PAN-OS?Upgrade Agent

Correct Answer: B

QUESTION 49
Which logs enable a firewall administrator to determine whether a session was decrypted?

A. Correlated Event
B. Traffic
C. Decryption
D. Security Policy

Correct Answer: B

QUESTION 50
VPN traffic intended for an administrator's Palo Alto Networks NGFW is being maliciously intercepted and retransmitted by the interceptor. When creating a VPN tunnel, which protection profile can be enabled to prevent this malicious behavior?

A. Zone Protection
B. DoS Protection
C. Web Application
D. Replay

Correct Answer: A

QUESTION 51
An administrator has been asked to create 100 virtual firewalls in a local, on-premise lab environment (not in "the cloud"). Bootstrapping is the most expedient way to perform this task. Which option describes deployment of a bootstrap package in an on-premise virtual environment?

A. Use config-drive on a USB stick.
B. Use an S3 bucket with an ISO.
C. Create and attach a virtual hard disk (VHD).
D. Use a virtual CD-ROM with an ISO.

Correct Answer: D
Explanation:
https://www.paloaltonetworks.com/documentation/71/pan-os/newfeaturesguide/management-features/bootstrapping-firewalls-for-rapid-deployment.html

QUESTION 52
A customer has an applicationthat is being identified as unknown-top for one of their custom PostgreSQL database connections. Which two configuration options can be used to correctly categorize their custom database application? (Choose two.)

A. Application Override policy.
B. Securitypolicy to identify the custom application.
C. Custom application.
D. Custom Service object.

Correct Answer: BD

QUESTION 53
The firewall determines if a packet is the first packet of a new session or if a packet is part of an existing session using which kind of match?

A. 5-tuple match
    Source IP Address, Destination IP Address, Source Port, Destination Port, Protocol
B. 7-tuple match
    Source IP Address, Destination IP Address, Source Port, Destination Port ,Source User, URLCategory and Source Security Zone.
C. 6-tuple match

Source IP Address, Destination IP Address, Source Port, Destination Port, Protocol and Source Security Zone
D. 9-tuple match
Source IP Address, Destination IP Address, Source Port, Destination Port, Source User, Source Security Zone, Destination Security Zone, Application and URL Category

Correct Answer: A

QUESTION 54
Which processing order will be enabled when a Panorama administrator selects the setting "Objects defined in ancestors will take higher precedence"?

A. Descendant objects will take precedence over other descendant objects.
B. Descendant objects will take precedence over ancestor objects.
C. Ancestor objects will have precedence over descendant objects.
D. Ancestor objects will have precedence over other ancestor objects.

Correct Answer: C
Explanation:
https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/device/device-setup-management

QUESTION 55
Which CLI command can be used to export the tcpdumpcapture?

A. scp export tcpdump from mgmt.pcap to <username@host:path>
B. scp extract mgmt-pcap from mgmt.pcap to <username@host:path>
C. scp export mgmt-pcap from mgmt.pcap to <username@host:path>
D. download mgmt.-pcap

Correct Answer: C
Explanation:
https://live.paloaltonetworks.com/t5/Management-Articles/How-To-Packet-Capture-tcpdump-On-Management-Interface/ta-p/55415

QUESTION 56
Anadministrator using an enterprise PKI needs to establish a unique chain of trust to ensure mutual authentication between Panorama and the managed firewalls and Log Collectors. How would the administrator establish the chain of trust?

A. Use custom certificates
B. Enable LDAP or RADIUS integration
C. Set up multi-factor authentication
D. Configure strong password authentication

Correct Answer: A
Explanation:
https://www.paloaltonetworks.com/documentation/80/panorama/panorama_adminguide/panorama-overview/plan-your-panorama-deployment

QUESTION 57

An administrator needs to upgrade a Palo Alto Networks NGFW to the most current version of PAN-OS® software. The firewall hasinternet connectivity through an Ethernet interface, but no internet connectivity from the management interface. The Security policy has the default security rules and a rule that allows all web-browsing traffic from any to any zone. What must the administrator configure so that the PAN-OS® software can be upgraded?

A.   Security policy rule
B.   CRL
C.   Service route
D.   Scheduler

Correct Answer: A

QUESTION 58
VPN traffic intended for an administrator's Palo Alto Networks NGFW is being maliciously intercepted and retransmitted by the interceptor. When creating a VPN tunnel, which protection profile can be enabled to prevent this malicious behavior?

A.   Zone Protection
B.   Replay
C.   Web Application
D.   DoS Protection

Correct Answer: A

QUESTION 59
Which CLI command is used to simulate traffic goingthrough 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

Correct Answer: C
Explanation:
http://www.shanekillen.com/2014/02/palo-alto-useful-cli-commands.html

QUESTION 60
A client is concerned about resource exhaustion because of denial-of-service attacks against their DNS servers. Which option will protect theindividual servers?

A.   Enable packet buffer protection on the Zone Protection Profile.
B.   Apply an Anti-Spyware Profile with DNS sinkholing.
C.   Use the DNS App-ID with application-default.
D.   Apply a classified DoS Protection Profile.

Correct Answer: A

QUESTION 61