Latest Version: 39.0

Question: 1

An administrator is defining protection settings on the Palo Alto Networks NGFW to guard against resource exhaustion. When platform utilization is considered, which steps must the administrator take to configure and apply packet buffer protection?

A. Enable and configure the Packet Buffer protection thresholds.Enable Packet Buffer Protection per ingress zone.
B. Enable and then configure Packet Buffer thresholdsEnable Interface Buffer protection.
C. Create and Apply Zone Protection Profiles in all ingress zones.Enable Packet Buffer Protection per ingress zone.
D. Configure and apply Zone Protection Profiles for all egress zones.Enable Packet Buffer Protection pre egress zone.
E. Enable per-vsys Session Threshold alerts and triggers for Packet Buffer Limits.Enable Zone Buffer Protection per zone.

Answer: A

Question: 2

Which feature can provide NGFWs with User-ID mapping information?

A. Web Captcha
B. Native 802.1q authentication
C. GlobalProtect
D. Native 802.1x authentication

Answer: C

Question: 3

What are the two behavior differences between Highlight Unused Rules and the Rule Usage Hit counter when a firewall is rebooted? (Choose two.)

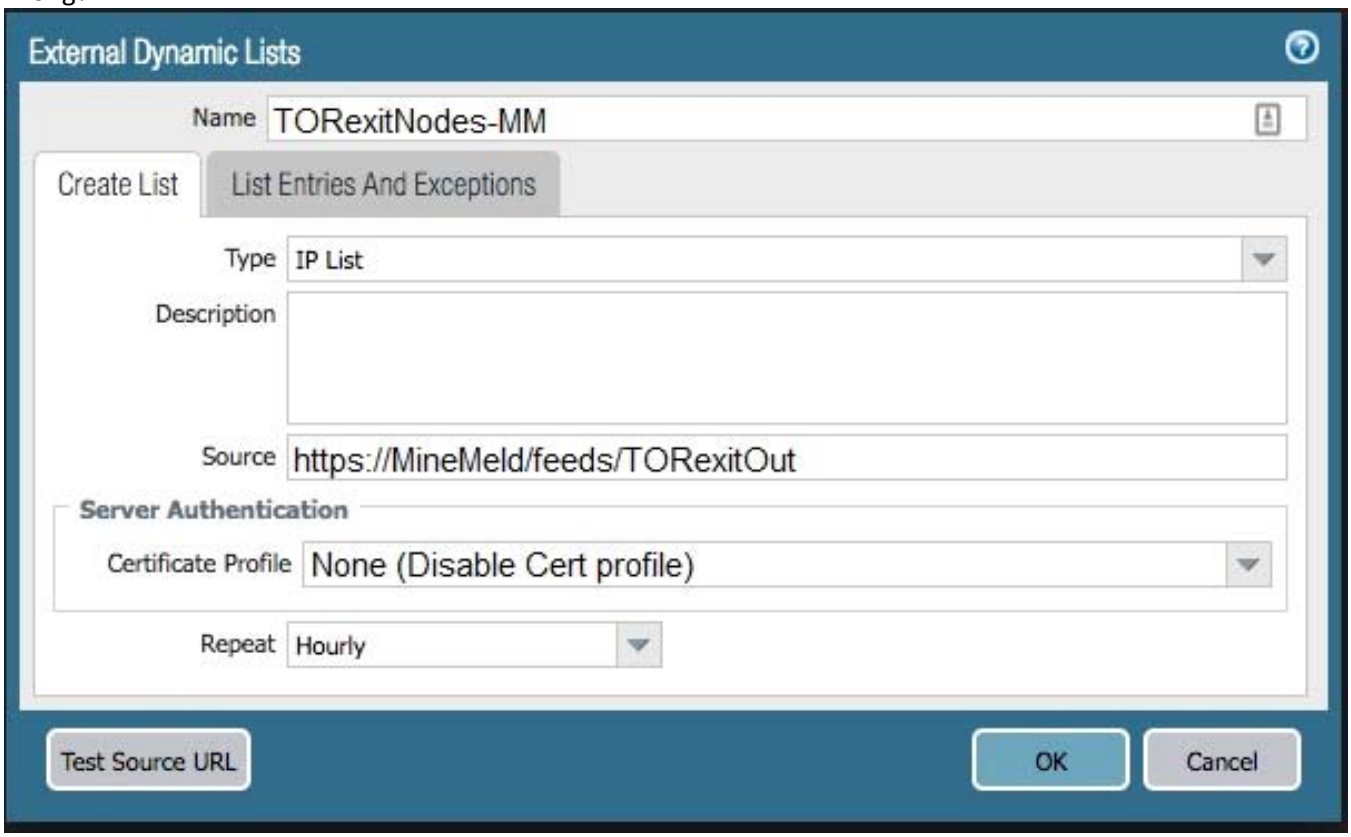
A. Rule Usage Hit counter will not be reset
B. Highlight Unused Rules will highlight all rules.
C. Highlight Unused Rules will highlight zero rules.
D. Rule Usage Hit counter will reset.

Answer: A, B

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClVICA0
"Notice how the rules looks after selecting "Highlight Unused Rules." You can now see exactly what rules have and have not been used since the last reboot."

Question: 4

The firewall is not downloading IP addresses from MineMeld. Based, on the image, what most likely is wrong?



A. A Certificate Profile that contains the client certificate needs to be selected.
B. The source address supports only files hosted with an ftp://<address/file>.
C. External Dynamic Lists do not support SSL connections.
D. A Certificate Profile that contains the CA certificate needs to be selected.

Answer: D

"If the list source is secured with SSL (i.e. lists with an HTTPS URL), enable server authentication. Select a Certificate Profile or create a New Certificate Profile for authenticating the server that hosts the list. The certificate profile you select must have root certificate authority (CA) and intermediate CA certificates that match the certificates installed on the server you are authenticating."

Question: 5

Which is not a valid reason for receiving a decrypt-cert-validation error?

A. Unsupported HSM
B. Unknown certificate status
C. Client authentication
D. Untrusted issuer

Answer: A

Per the link https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-new-features/networking-features/ssl-ssh-session-end-reasons
, receiving the decrypt-cert-validation error is valid for the following conditions: expired, untrusted issuer, unknown status, or status verification time-out. "Unsupported HSM" is not a valid reason for receiving a decrypt-cert-validation error.

Question: 6

In the following image from Panorama, why are some values shown in red?

Device Name	Logging Rate (Log/sec)	Device	Session
		Throughput (KB/sec)	Count (Sessions)
uk3	781	209	40221
sg2	0	953	170
us3	291	0	67455

A. sg2 session count is the lowest compared to the other managed devices.
B. us3 has a logging rate that deviates from the administrator-configured thresholds.
C. uk3 has a logging rate that deviates from the seven-day calculated baseline.
D. sg2 has misconfigured session thresholds.

Answer: C

"The Deviating Devices tab displays devices that have any metrics that are deviating from their calculated baseline and displays those deviating metrics in red. A metric health baseline is determined by averaging the health performance for a given metric over seven days plus the standard deviation."
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface-help/panorama-web-interface/panorama-managed-devices-summary/panorama-managed-devices-health

Question: 7

What should an administrator consider when planning to revert Panorama to a pre-PAN-OS 8.1 version?

A. Panorama cannot be reverted to an earlier PAN-OS release if variables are used in templates or template stacks.
B. An administrator must use the Expedition tool to adapt the configuration to the pre-PAN-OS 8.1 state.
C. When Panorama is reverted to an earlier PAN-OS release, variables used in templates or template stacks will be removed automatically.
D. Administrators need to manually update variable characters to those used in pre-PAN-OS 8.1.

Answer: A

You are unable to downgrade from PAN-OS 8.1 to an earlier PAN-OS release if variables are used in your template or template stack configuration. Variables must be removed from the template and template stack configuration to downgrade.

Question: 8

Which two methods can be configured to validate the revocation status of a certificate? (Choose two.)

A. CRL
B. CRT
C. OCSP
D. Cert-Validation-Profile
E. SSL/TLS Service Profile

Answer: A, C

https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/certificate-management/certificate-revocation.html#idaa3aa4f6-4791-4dbb-b834-58c22e208be8

Question: 9

Which administrative authentication method supports authorization by an external service?

A. Certificates
B. LDAP
C. RADIUS
D. SSH keys

Answer: C

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/firewall-administration/manage-firewall-administrators/administrative-authentication

Question: 10

An administrator has been asked to configure active/active HA for a pair of Palo Alto Networks NGFWs. The firewall use Layer 3 interfaces to send traffic to a single gateway IP for the pair.
Which configuration will enable this HA scenario?

A. The two firewalls will share a single floating IP and will use gratuitous ARP to share the floating IP.
B. Each firewall will have a separate floating IP, and priority will determine which firewall has the primary IP.
C. The firewalls do not use floating IPs in active/active HA.
D. The firewalls will share the same interface IP address, and device 1 will use the floating IP if device 0 fails.

Answer: A

Each HA firewall interface has its own IP address and floating IP. The interface IP address remains local to the firewall, but the floating IP address moves between the firewalls upon firewall failure. You configure the end hosts to use a floating IP address as its default gateway, thus allowing you to load balance traffic to the two HA peers. You also can use external load balancers to load balance traffic.If a link or firewall fails or a path monitoring event causes a failover, the floating IP address and virtual MAC address move over to the functional firewall. (In the figure that follows, each firewall has two floating IP addresses and virtual MAC addresses; they all move over if the firewall fails.) The functioning firewall sends a gratuitous ARP to update the MAC tables of the connected switches to inform them of the change in floating IP address and MAC address ownership to redirect traffic to itself.