QUESTION 81
How would an administrator monitor/capture traffic on the managementinterface of the Palo Alto Networks NGFW?

A. Use the debug dataplane packet-diag set capture stage firewall file command.
B. Enable all four stages of traffic capture (TX, RX, DROP, Firewall).
C. Use the debug dataplane packet-diag set capture stage management file command.
D. Use the tcpdump command.

Correct Answer: D
Explanation:
https://live.paloaltonetworks.com/t5/Learning-Articles/How-to-Run-a-Packet-Capture/ta-p/62390

QUESTION 82
Which three authentication services can administrator use to authenticate admins into the Palo Alto Networks NGFW without defining a corresponding admin account on the local firewall? (Choose three.)

A. Kerberos
B. PAP
C. SAML
D. TACACS+
E. RADIUS
F. LDAP

Correct Answer: DEF

QUESTION 83
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 thestack.
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.

Correct Answer: B
Explanation:
https://www.paloaltonetworks.com/documentation/80/panorama/panorama_adminguide/manage-firewalls/manage-templates-and-template-stacks/configure-a-template-stack

QUESTION 84
Which three options are supported in HA Lite? (Choose three.)

A. Virtual link
B. Active/passive deployment
C. Synchronization of IPsec security associations
D. Configuration synchronization
E. Sessionsynchronization

Correct Answer: BCD
Explanation:
https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/device/device-high-availability/ha-lite

QUESTION 85
During the packet flow process, which two processes are performed in application identification? (Choose two.)

A. Pattern based application identification
B. Application override policy match
C. Application changed from content inspection
D. Session application identified.

Correct Answer: BD

QUESTION 86
Which method does an administrator use to integrate all non-native MFA platforms in PAN-OS® software?

A. Okta
B. DUO
C. RADIUS
D. PingID

Correct Answer: C

QUESTION 87
What is exchanged through the HA2 link?

A. hello heartbeats
B. User-ID information
C. sessionsynchronization
D. HA state information

Correct Answer: C
Explanation:
https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/high-availability/ha-links-and-backup-links

QUESTION 88
An administrator just submitted a newlyfound piece of spyware for WildFire analysis. The spyware passively monitors behavior without the user's knowledge. What is the expected verdict from WildFire?

A. Gray ware
B. Malware
C. Spyware

D. Phishing

Correct Answer: A

QUESTION 89
If the firewall has the link monitoringconfiguration, what will cause a failover?
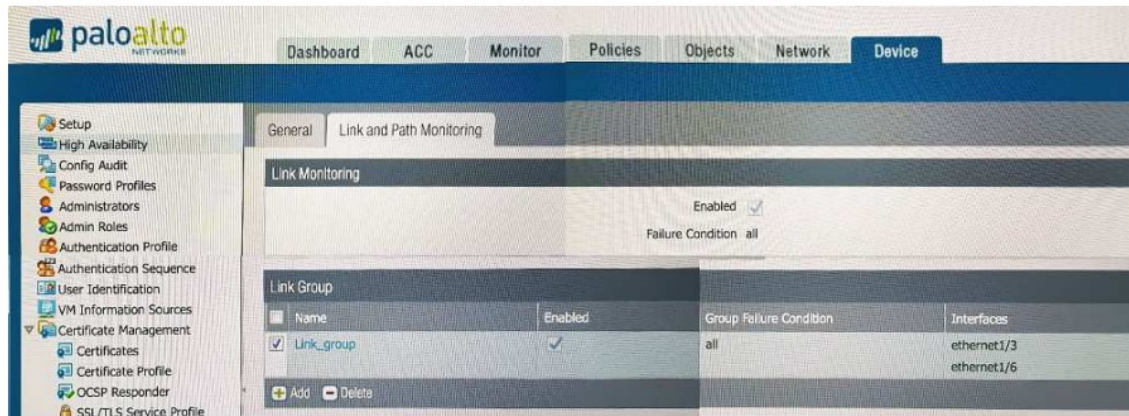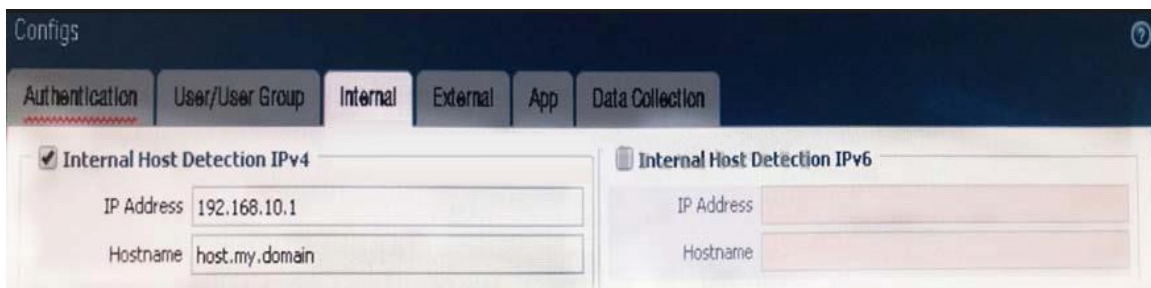

A. ethernet1/3 and ethernet1/6 going down
B. ethernet1/3 going down
C. ethernet1/3 or Ethernet1/6 going down
D. ethernet1/6 going down

Correct Answer: A

QUESTION 90
View the GlobalProtect configuration screen capture. What is the purpose of this configuration?

A. It configures the tunnel address of all internal clients to an IP address range starting at 192.168.10.1.
B. It forces an internal client to connect to an internal gateway at IP address 192.168.10.1.
C. It enables a client to perform a reverse DNS lookup on 192.168.10.1 to detect that it is an internal client.
D. It forces the firewall to perform a dynamic DNS update, which adds the internal gateway's hostname and IP address to the DNS server.

Correct Answer: C

Explanation:
https://www.paloaltonetworks.com/documentation/80/globalprotect/globalprotect-admin-guide/globalprotect-portals/define-the-globalprotect-client-authentication-configurations/define-the-globalprotect-agent-configurations

QUESTION 91
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 certificatefrom an HSM

Correct Answer: A
Explanation:
https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/decryption/configure-ssl-inbound-inspection

QUESTION 92
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 routein the virtual router.

Correct Answer: C

QUESTION 93
Where can an administrator see both the management plane and data plane CPU utilization in the WebUI?

A. System log
B. CPU Utilization widget
C. Resources widget
D. System Utilization log

Correct Answer: C

QUESTION 94
What are the differences between using a service versus using an application for Security Policy match?

A. Use of a "service" enables the firewall to take action after enough packets allow for App-ID identification
B. Use of a "service" enables the firewall to take immediate action with the first observed packet based on port numbers Use ofan "application" allows the firewall to take action after enough

packets allow for App-ID identification regardless of the portsbeing used.

C. There are no differences between "service" or "application" Use of an "application" simplifies configuration by allowing use ofa friendly application name instead of port numbers.

D. Use of a "service" enables the firewall to take immediate action with thefirst observed packet based on port numbers. Use ofan "application" allows the firewall to take immediate action it the port being used is a member of the application standardport list

Correct Answer: B

QUESTION 95
Refer to the exhibit. Which will be the egress interface if the traffic's ingress interface is ethernet 1/7 sourcing from 192.168.111.3 and to the destination 10.46.41.113?

```
###############################
admin@Lab33-111-PA-3060(active)>show routing fib
```

id	destination	nexthop	flags	interface	mtu
47	0.0.0.0/0	10.46.40.1	ug	ethernet1/3	1500
46	10.46.40.0/23	0.0.0.0	u	ethernet1/3	1500
45	10.46.41.111/32	0.0.0.0	uh	ethernet1/3	1500
70	10.46.41.113/32	10.46.40.1	ug	ethernet1/3	1500
51	192.168.111.0/24	0.0.0.0	u	ethernet1/6	1500
50	192.168.111.2/32	0.0.0.0	uh	ethernet1/6	1500

```
-----------------------------------------------------------------
###############################

admin@Lab33-111-PA-3060(active)>show virtual-wire all

total virtual-wire shown:
flags:  m-multicast firewalling
        p= link state pass-through
        s- vlan sub-interface
        i- ip+vlan sub-interface
        t-tenant sub-interface
```

name	interface1	interface2	flags	allowed-tags
VW-1	ethernet1/7	ethernet1/5	p	

```
###############################
```