Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.

Palo-Alto

PCNSE

Palo Alto Networks Certified Security Engineer (PCNSE) PAN-OS 10

Question: 48

Which CLI command is used to determine how much disk space is allocated to logs?
A. show logging-status
B. show system info
C. debug log-receiver show
D. show system logdfo-quota

Answer: D

Question: 49

Which Panorama feature protects logs against data loss if a Panorama server fails?
A. Panorama HA automatically ensures that no logs are lost if a server fails inside the HA Cluster.
B. Panorama Collector Group with Log Redundancy ensures that no logs are lost if a server fails inside the Collector Group.
C. Panorama HA with Log Redundancy ensures that no logs are lost if a server fails inside the HA Cluster.
D. Panorama Collector Group automatically ensures that no logs are lost if a server fails inside the Collector Group

Answer: A

Question: 50

A network security engineer wants to prevent resource-consumption issues on the firewall.

Which strategy is consistent with decryption best practices to ensure consistent performance?
A. Use RSA in a Decryption profile tor higher-priority and higher-risk traffic, and use less processor-intensive decryption methods for lower-risk traffic
B. Use PFS in a Decryption profile for higher-priority and higher-risk traffic, and use less processor-intensive decryption methods for tower-risk traffic
C. Use Decryption profiles to downgrade processor-intensive ciphers to ciphers that are less processor-intensive
D. Use Decryption profiles to drop traffic that uses processor-intensive ciphers

Answer: B

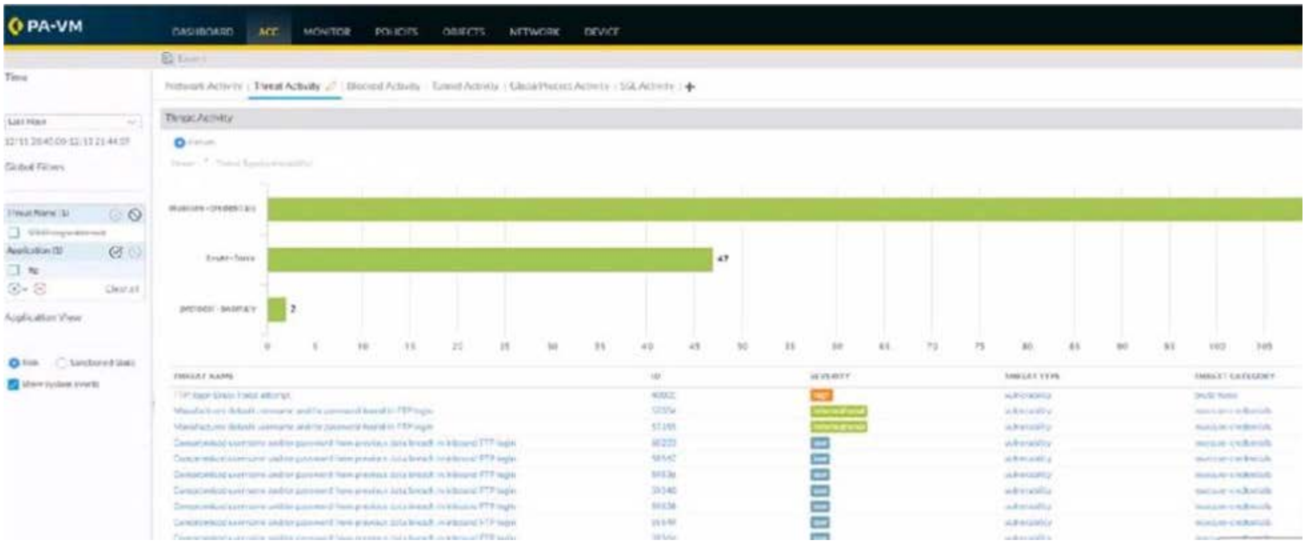
Question: 51

Using multiple templates in a stack to manage many firewalls provides which two advantages? (Choose two.)
A. inherit address-objects from templates
B. define a common standard template configuration for firewalls
C. standardize server profiles and authentication configuration across all stacks
D. standardize log-forwarding profiles for security polices across all stacks

Answer: B, C

Question: 52

In the screenshot above which two pieces ot information can be determined from the ACC configuration shown? (Choose two)



A. The Network Activity tab will display all applications, including FTP.
B. Threats with a severity of "high" are always listed at the top of the Threat Name list
C. Insecure-credentials, brute-force and protocol-anomaly are all a part of the vulnerability Threat Type
D. The ACC has been filtered to only show the FTP application

Answer: C, D

Question: 53

A company is using wireless controllers to authenticate users.

Which source should be used for User-ID mappings?
A. Syslog
B. XFF headers
C. server monitoring
D. client probing

Answer: A

Question: 54

Which statement regarding HA timer settings is true?
A. Use the Recommended profile for typical failover timer settings
B. Use the Moderate profile for typical failover timer settings
C. Use the Aggressive profile for slower failover timer settings.
D. Use the Critical profile for faster failover timer settings.

Answer: A

Question: 55

An administrator is seeing one of the firewalls in a HA active/passive pair moved to ‘suspended" state due to Non-functional loop.

Which three actions will help the administrator troubleshool this issue? (Choose three.)
A. Use the CLI command show high-availability flap-statistics
B. Check the HA Link Monitoring interface cables.
C. Check the High Availability > Link and Path Monitoring settings.
D. Check High Availability > Active/Passive Settings > Passive Link State
E. Check the High Availability > HA Communications > Packet Forwarding settings.

Answer: A,B,D

Question: 56

An administrator has 750 firewalls. The administrator’s central-management Panorama instance deploys dynamic updates to the firewalls. The administrator notices that the dynamic updates from Panorama do not appear on some of the firewalls.

If Panorama pushes the configuration of a dynamic update schedule to managed firewalls, but the configuration does not appear, what is the root cause?
A. Panorama does not have valid licenses to push the dynamic updates.
B. Panorama has no connection to Palo Alto Networks update servers.
C. No service route is configured on the firewalls to Palo Alto Networks update servers.
D. Locally-defined dynamic update settings take precedence over the settings that Panorama pushed.

Answer: D

Question: 57

A client wants to detect the use of weak and manufacturer-default passwords for loT devices.

Which option will help the customer?
A. Configure a Data Filtering profile with alert mode.
B. Configure an Antivirus profile with alert mode.
C. Configure a Vulnerability Protection profile with alert mode
D. Configure an Anti-Spyware profile with alert mode.

Answer: C

Question: 58

An administrator needs to evaluate a recent policy change that was committed and pushed to a firewall device group.

How should the administrator identify the configuration changes?
A. review the configuration logs on the Monitor tab

B. click Preview Changes under Push Scope
C. use Test Policy Match to review the policies in Panorama
D. context-switch to the affected firewall and use the configuration audit tool

Answer: A

Explanation:

https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface-help/panorama-web-interface/panorama-commit-operations.html

Question: 59

A network administrator troubleshoots a VPN issue and suspects an IKE Crypto mismatch between peers.

Where can the administrator find the corresponding logs after running a test command to initiate the VPN?
A. Configuration logs
B. System logs
C. Traffic logs
D. Tunnel Inspection logs

Answer: B

Question: 60

An administrator has configured a pair of firewalls using high availability in Active/Passive mode. Path Monitoring has been enabled with a Failure Condition of "any." A path group is configured with Failure Condition of "all" and contains a destination IP of 8.8.8.8 and 4.2.2.2 with a Ping Interval of 500ms and a Ping count of 3.

Which scenario will cause the Active firewall to fail over?
A. IP address 8.8.8.8 is unreachable for 1 second.
B. IP addresses 8.8.8.8 and 4.2.2.2 are unreachable for 1 second.
C. IP addresses 8.8.8.8 and 4.2.2.2 are unreachable for 2 seconds
D. IP address 4.2.2.2 is unreachable for 2 seconds.

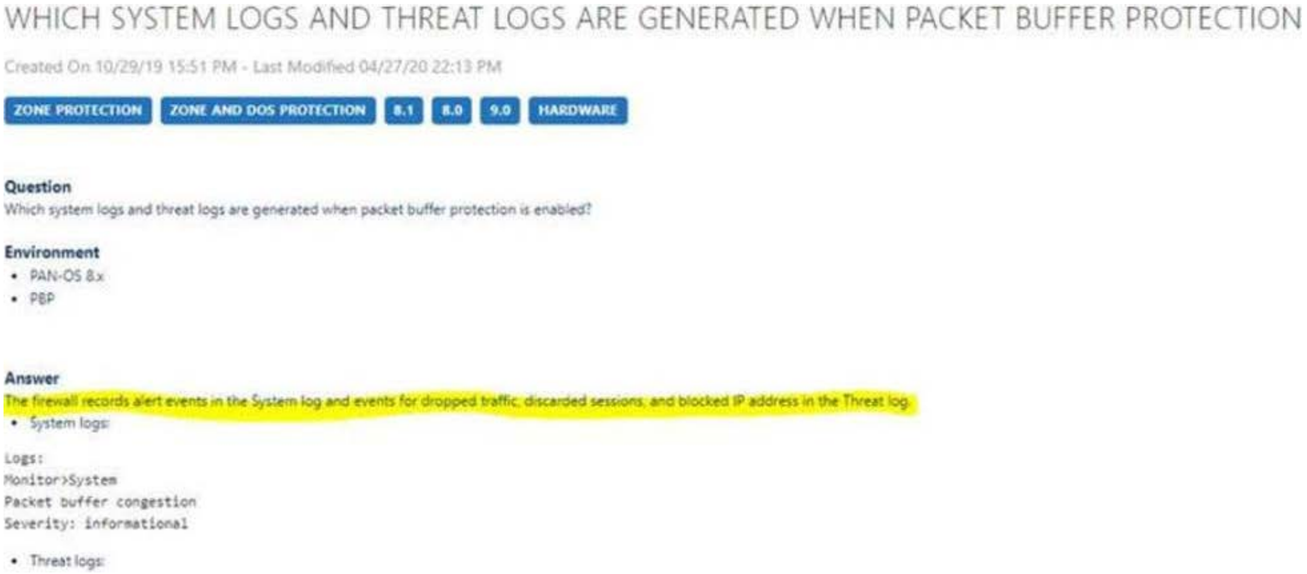
Answer: C

Question: 61

Where is information about packet buffer protection logged?
A. Alert entries are in the Alarms log. Entries for dropped traffic, discarded sessions, and blocked IP address are in the Threat log
B. All entries are in the System log
C. Alert entries are in the System log. Entries for dropped traffic, discarded sessions and blocked IP addresses are in the Threat log
D. All entries are in the Alarms log

Answer: C

Explanation:



WHICH SYSTEM LOGS AND THREAT LOGS ARE GENERATED WHEN PACKET BUFFER PROTECTION

Created On 10/29/19 15:51 PM - Last Modified 04/27/20 22:13 PM

ZONE PROTECTION | ZONE AND DOS PROTECTION | 8.1 | 8.0 | 9.0 | HARDWARE

Question

Which system logs and threat logs are generated when packet buffer protection is enabled?

Environment

- PAN-OS 8.x
- PBP

Answer

The firewall records alert events in the System log and events for dropped traffic, discarded sessions, and blocked IP address in the Threat log.

- System logs:

```
Logs:
Monitor>System
Packet buffer congestion
Severity: informational
```

- Threat logs:

Graphical user interface, text,

application

Description automatically generated

Question: 62

The administrator for a small company has recently enabled decryption on their Palo Alto Networks firewall using a self-signed root certificate. They have also created a Forward Trust and Forward Untrust certificate and set them as such.

The admin has not yet installed the root certificate onto client systems

What effect would this have on decryption functionality?
A. Decryption will function and there will be no effect to end users
B. Decryption will not function because self-signed root certificates are not supported
C. Decryption will not function until the certificate is installed on client systems
D. Decryption will function but users will see certificate warnings for each SSL site they visit

Answer: D

Question: 63

A firewall administrator notices that many Host Sweep scan attacks are being allowed through the firewall sourced from the outside zone.

What should the firewall administrator do to mitigate this type of attack?
A. Create a DOS Protection profile with SYN Flood protection enabled and apply it to all rules allowing traffic from the outside zone
B. Enable packet buffer protection in the outside zone.

C. Create a Security rule to deny all ICMP traffic from the outside zone.
D. Create a Zone Protection profile, enable reconnaissance protection, set action to Block, and apply it to the outside zone.

Answer: D

Question: 64

An engineer is tasked with configuring a Zone Protection profile on the untrust zone.

Which three settings can be configured on a Zone Protection profile? (Choose three.)
A. Ethernet SGT Protection
B. Protocol Protection
C. DoS Protection
D. Reconnaissance Protection
E. Resource Protection

Answer: A, B, D

Explanation:

B. Protocol Protection: is used to protect against known protocol vulnerabilities, such as buffer overflows and malformed packets.

C. DoS Protection: is used to protect against denial-of-service (DoS) attacks, such as SYN floods and ICMP floods.

D. Reconnaissance Protection: is used to protect against reconnaissance attacks, such as

port scans and ping sweeps.

Question: 65

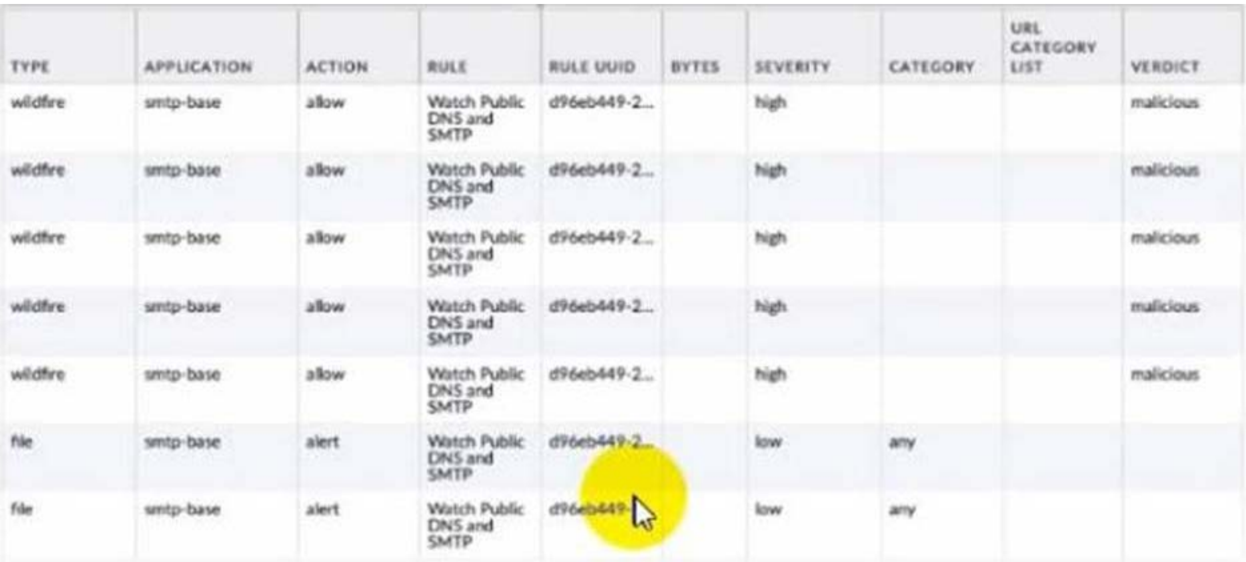
A firewall should be advertising the static route 10.2.0.0/24 Into OSPF. The configuration on the neighbor is correct, but the route is not in the neighbor’s routing table.

Which two configurations should you check on the firewall? (Choose two.)
A. In the OSFP configuration, ensure that the correct redistribution profile is selected in the OSPF Export Rules section.
B. Within the redistribution profile ensure that Redist is selected.
C. Ensure that the OSPF neighbor state Is "2-Way."
D. In the redistribution profile check that the source type is set to "ospf."

Answer: A,B

Question: 66

Given the following snippet of a WildFire submission log. did the end-user get access to the requested information and why or why not?



TYPE	APPLICATION	ACTION	RULE	RULE UUID	BYTES	SEVERITY	CATEGORY	URL CATEGORY LIST	VERDICT
wildfire	smtp-base	allow	Watch Public DNS and SMTP	d96eb449-2...		high			malicious
wildfire	smtp-base	allow	Watch Public DNS and SMTP	d96eb449-2...		high			malicious
wildfire	smtp-base	allow	Watch Public DNS and SMTP	d96eb449-2...		high			malicious
wildfire	smtp-base	allow	Watch Public DNS and SMTP	d96eb449-2...		high			malicious
wildfire	smtp-base	allow	Watch Public DNS and SMTP	d96eb449-2...		high			malicious
file	smtp-base	alert	Watch Public DNS and SMTP	d96eb449-2...		low	any		
file	smtp-base	alert	Watch Public DNS and SMTP	d96eb449-		low	any		

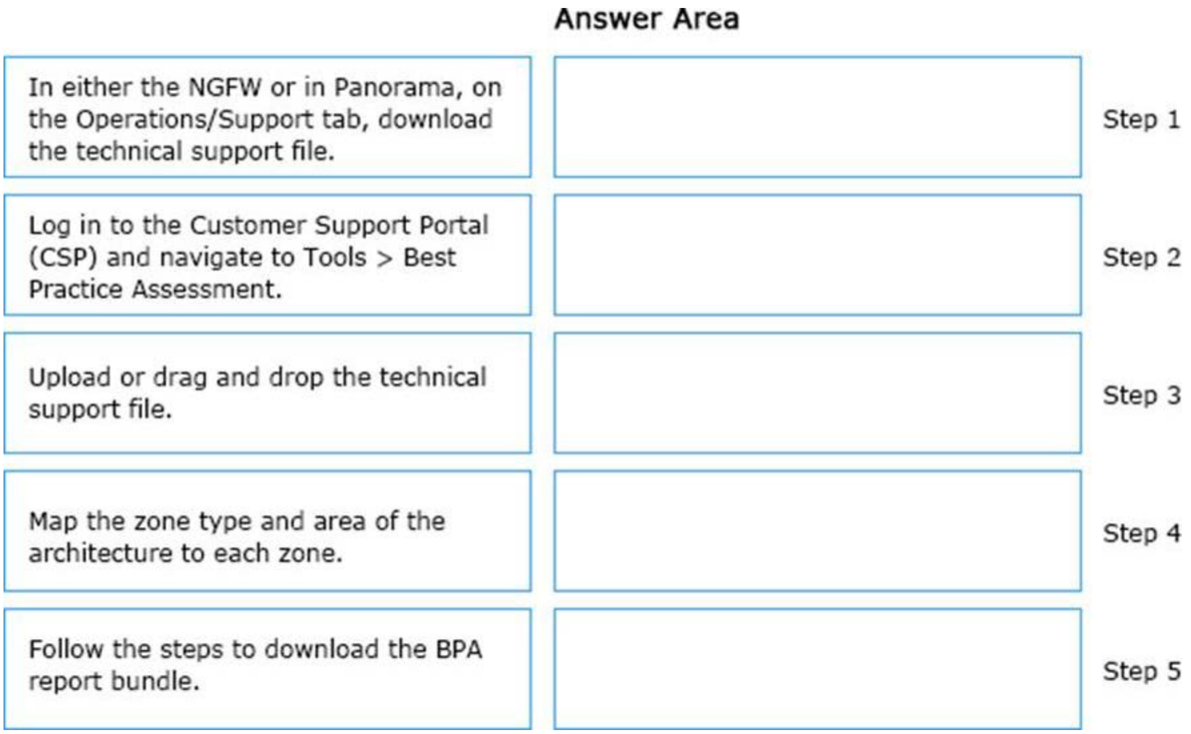
A. Yes. because the action is set to "allow ”
B. No because WildFire categorized a file with the verdict "malicious"
C. Yes because the action is set to "alert"
D. No because WildFire classified the seventy as "high."

Answer: C

Question: 67

DRAG DROP

Below are the steps in the workflow for creating a Best Practice Assessment in a firewall and Panorama configuration Place the steps in order.



Answer Area

In either the NGFW or in Panorama, on the Operations/Support tab, download the technical support file.

Log in to the Customer Support Portal (CSP) and navigate to Tools > Best Practice Assessment.

Upload or drag and drop the technical support file.

Map the zone type and area of the architecture to each zone.

Follow the steps to download the BPA report bundle.

Step 1

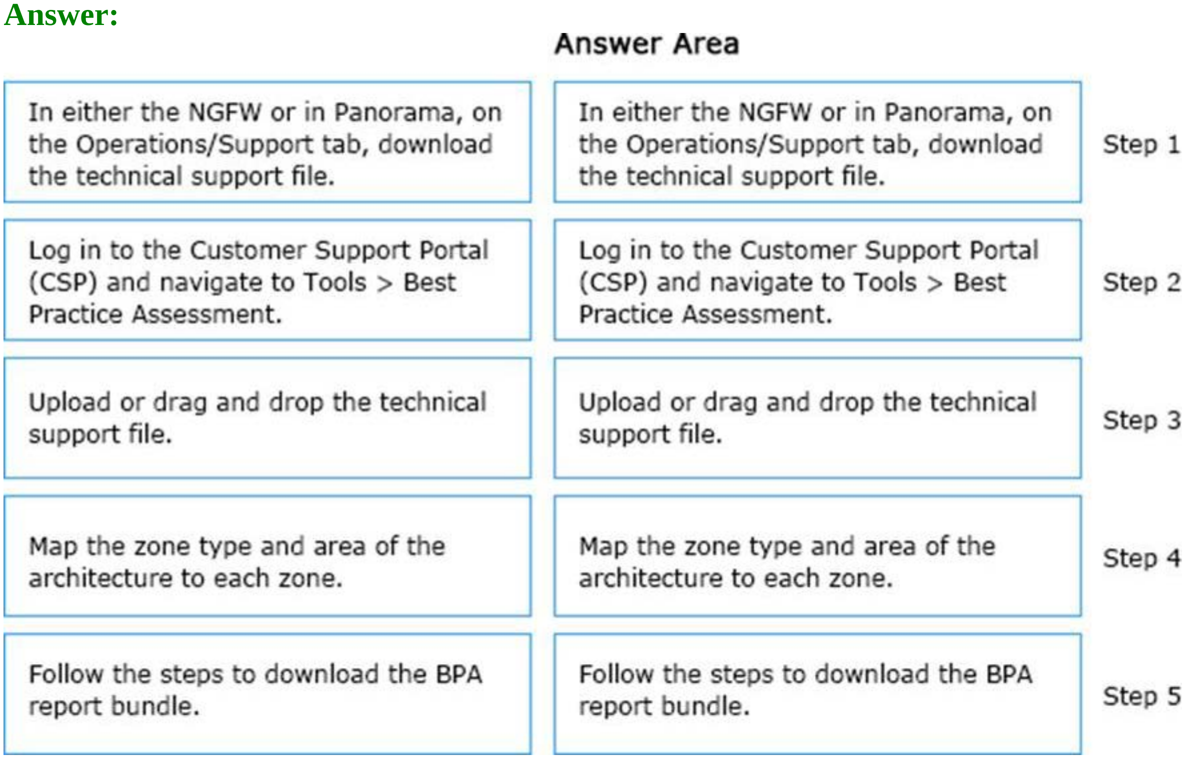
Step 2

Step 3

Step 4

Step 5

Answer:



Answer Area

In either the NGFW or in Panorama, on the Operations/Support tab, download the technical support file.	In either the NGFW or in Panorama, on the Operations/Support tab, download the technical support file.	Step 1
Log in to the Customer Support Portal (CSP) and navigate to Tools > Best Practice Assessment.	Log in to the Customer Support Portal (CSP) and navigate to Tools > Best Practice Assessment.	Step 2
Upload or drag and drop the technical support file.	Upload or drag and drop the technical support file.	Step 3
Map the zone type and area of the architecture to each zone.	Map the zone type and area of the architecture to each zone.	Step 4
Follow the steps to download the BPA report bundle.	Follow the steps to download the BPA report bundle.	Step 5

Explanation:

Step 1. In either the NGFW or in Panorama, on the Operations/Support tab, download the technical support file.

Step 2. Log in to the Customer Support Portal (CSP) and navigate to Tools > Best Practice Assessment.

Step 3. Upload or drag and drop the technical support file.

Step 4. Map the zone type and area of the architecture to each zone.

Step 5. Follow the steps to download the BPA report bundle.

Question: 68

You have upgraded Panorama to 10.2 and need to upgrade six Log Collectors.

When upgrading Log Collectors to 10.2, you must do what?
A. Upgrade the Log Collectors one at a time.
B. Add Panorama Administrators to each Managed Collector.
C. Add a Global Authentication Profile to each Managed Collector.
D. Upgrade all the Log Collectors at the same time.

Answer: D

Question: 69

How would an administrator configure a Bidirectional Forwarding Detection profile for BGP after enabling the Advance Routing Engine run on PAN-OS 10.2?

A. create a BFD profile under Network > Network Profiles > BFD Profile and then select the BFD profile under Network > Virtual Router > BGP > BFD
B. create a BFD profile under Network > Routing > Routing Profiles > BFD and then select the BFD profile under Network > Virtual Router > BGP > General > Global BFD Profile
C. create a BFD profile under Network > Routing > Routing Profiles > BFD and then select the BFD profile under Network > Routing > Logical Routers > BGP > General > Global BFD Profile
D. create a BFD profile under Network > Network Profiles > BFD Profile and then select the BFD profile under Network > Routing > Logical Routers > BGP > BFD

Answer: A