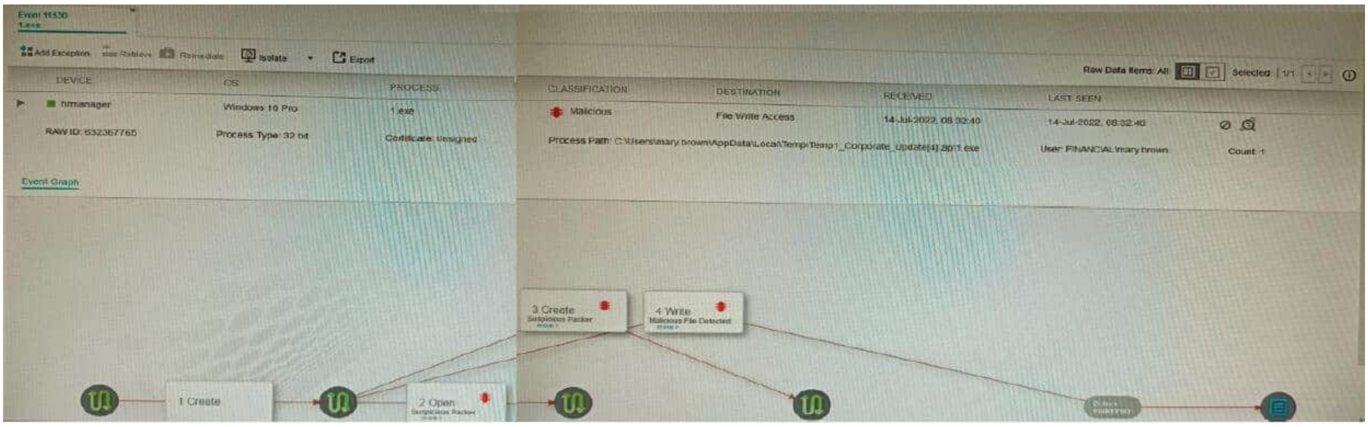
NSE8_812$^{Q\&As}$

Network Security Expert 8 Written Exam

QUESTION 1

Refer to the exhibit.



DEVICE	OS	PROCESS	CLASSIFICATION	DESTINATION	RECEIVED	LAST SEEN	
hrmanager	Windows 10 Pro	1.exe	Malicious	File Write Access	14-Jul-2022, 08:32:40	14-Jul-2022, 08:32:40	
RAW ID: 532367765	Process Type: 32 bit	Certificate: Unsigned	Process Path: C:\Users\mary.brown\AppData\Local\Temp\Temp1_Corporate_Update[4].zip\1.exe			User: FINANCIAL\mary.brown	Count: 1

The exhibit shows the forensics analysis of an event detected by the FortiEDR core

In this scenario, which statement is correct regarding the threat?

A. This is an exfiltration attack and has been stopped by FortiEDR.

B. This is an exfiltration attack and has not been stopped by FortiEDR

C. This is a ransomware attack and has not been stopped by FortiEDR.

D. This is a ransomware attack and has been stopped by FortiEDR

Correct Answer: B

Explanation: The exhibit shows that the FortiEDR core has detected an exfiltration attack. The attack is attempting to copy files from the device to an external location. The FortiEDR core has blocked the attack, and the files have not been

exfiltrated. The exhibit also shows that the attack is using the Cobalt Strike beacon. Cobalt Strike is a penetration testing tool that can be used for both legitimate and malicious purposes. In this case, the Cobalt Strike beacon is being used to

exfiltrate files from the device. The other options are incorrect. Option A is incorrect because the attack has not been stopped. Option C is incorrect because the attack is not a ransomware attack. Option D is incorrect because the FortiEDR

core has not stopped the attack.

References:

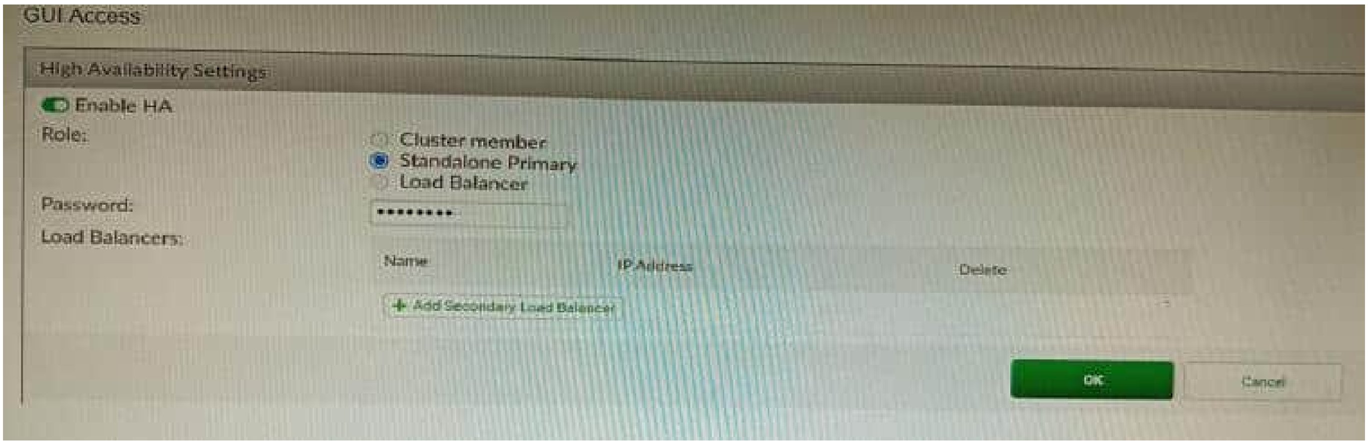
FortiEDR Forensics:

https://docs.fortinet.com/document/fortiedr/6.0.0/administration- guide/733983/forensics

Cobalt Strike: https://www.cobaltstrike.com/

QUESTION 2

Refer to the exhibit, which shows the high availability configuration for the FortiAuthenticator (FAC1).



GUI Access

High Availability Settings

Enable HA

Role:

○ Cluster member

● Standalone Primary

○ Load Balancer

Password: •••••••••

Load Balancers:

Name	IP Address	Delete

Based on this information, which statement is true about the next FortiAuthenticator (FAC2) member that will join an HA cluster with this FortiAuthenticator (FAC1)?

A. FAC2 can only process requests when FAC1 fails.

B. FAC2 can have its HA interface on a different network than FAC1.

C. The FortiToken license will need to be installed on the FAC2.

D. FSSO sessions from FAC1 will be synchronized to FAC2.

Correct Answer: D

Explanation: When FortiAuthenticator operates in cluster mode, it provides active-passive failover and synchronization of all configuration and data, including FSSO sessions, between the cluster members. Therefore, if FAC1 is the active unit and FAC2 is the standby unit, any FSSO sessions from FAC1 will be synchronized to FAC2. If FAC1 fails, FAC2 will take over the active role and continue to process the FSSO sessions. References:https://docs.fortinet.com/document/fortiauthenticator/6.1.2/administration- guide/122076/high-availability

QUESTION 3

Refer to the exhibits.

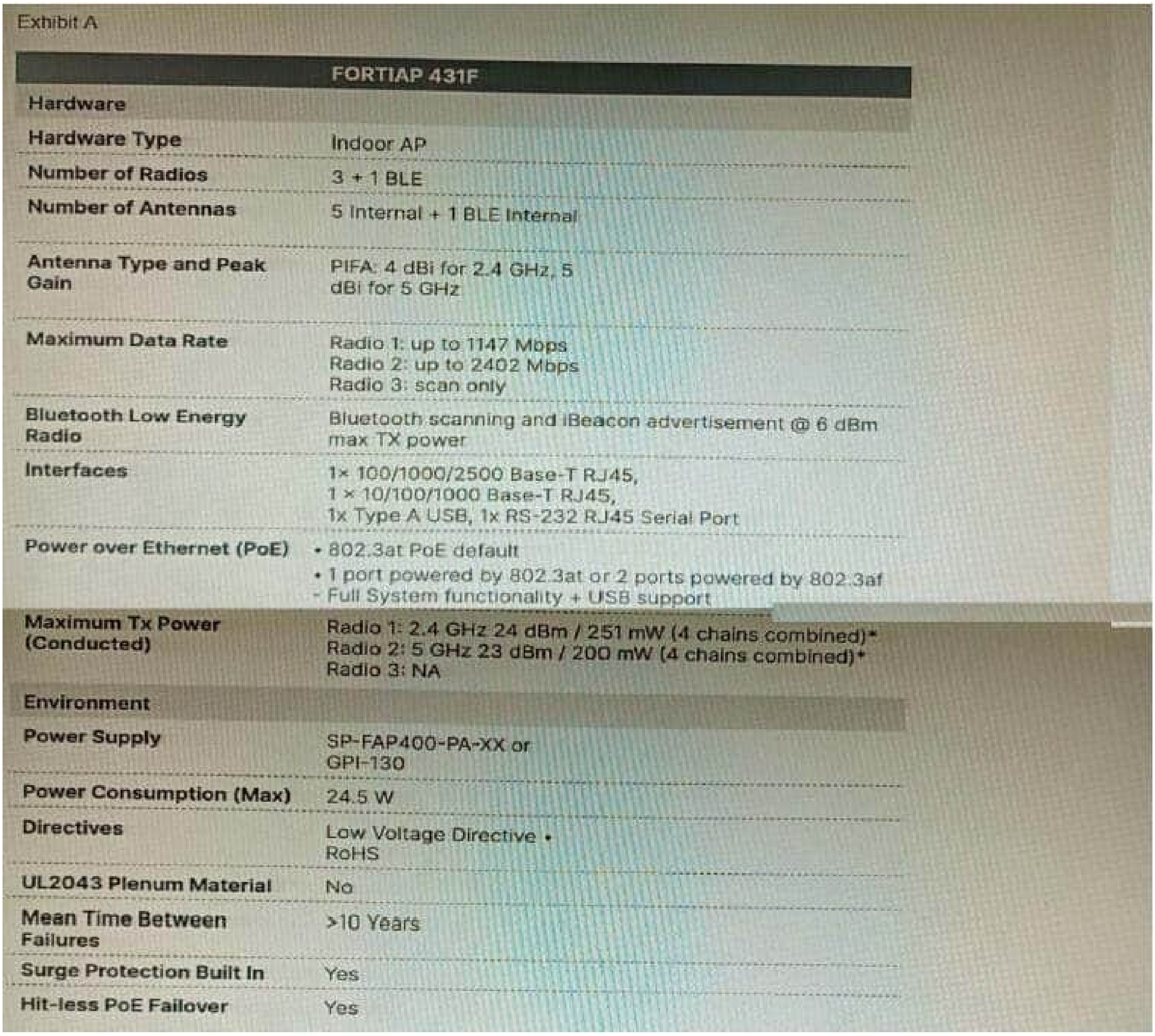


Exhibit A

FORTIAP 431F	
Hardware	
Hardware Type	Indoor AP
Number of Radios	3 + 1 BLE
Number of Antennas	5 Internal + 1 BLE Internal
Antenna Type and Peak Gain	PIFA: 4 dBi for 2.4 GHz, 5 dBi for 5 GHz
Maximum Data Rate	Radio 1: up to 1147 Mbps Radio 2: up to 2402 Mbps Radio 3: scan only
Bluetooth Low Energy Radio	Bluetooth scanning and iBeacon advertisement @ 6 dBm max TX power
Interfaces	1× 100/1000/2500 Base-T RJ45, 1 × 10/100/1000 Base-T RJ45, 1x Type A USB, 1x RS-232 RJ45 Serial Port
Power over Ethernet (PoE)	• 802.3at PoE default • 1 port powered by 802.3at or 2 ports powered by 802.3af - Full System functionality + USB support
Maximum Tx Power (Conducted)	Radio 1: 2.4 GHz 24 dBm / 251 mW (4 chains combined)* Radio 2: 5 GHz 23 dBm / 200 mW (4 chains combined)* Radio 3: NA
Environment	
Power Supply	SP-FAP400-PA-XX or GPI-130
Power Consumption (Max)	24.5 W
Directives	Low Voltage Directive • RoHS
UL2043 Plenum Material	No
Mean Time Between Failures	>10 Years
Surge Protection Built In	Yes
Hit-less PoE Failover	Yes

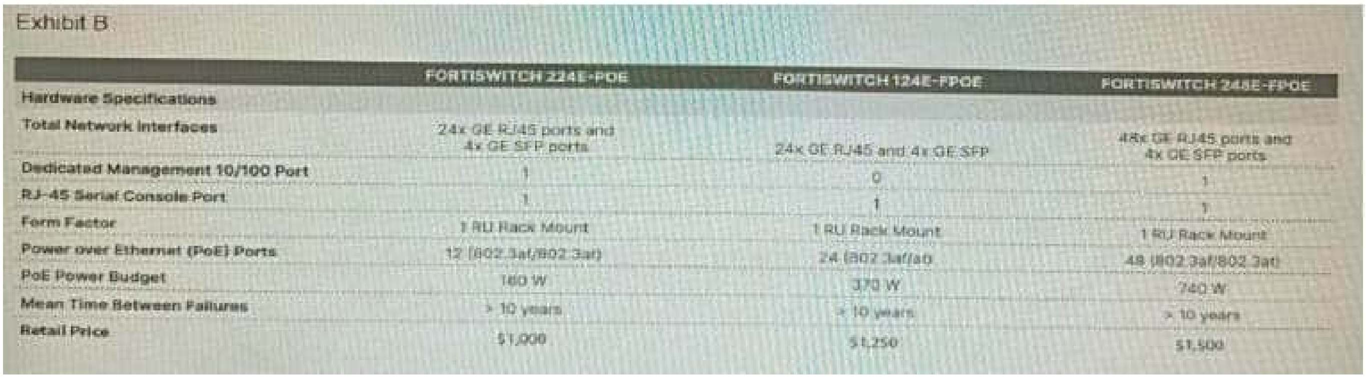


Exhibit B

	FORTISWITCH 224E-POE	FORTISWITCH 124E-FPOE	FORTISWITCH 248E-FPOE
Hardware Specifications			
Total Network Interfaces	24x GE RJ45 ports and 4x GE SFP ports	24x GE RJ45 and 4x GE SFP	48x GE RJ45 ports and 4x GE SFP ports
Dedicated Management 10/100 Port	1	0	1
RJ-45 Serial Console Port	1	1	1
Form Factor	1 RU Rack Mount	1 RU Rack Mount	1 RU Rack Mount
Power over Ethernet (PoE) Ports	12 (802.3af/802.3at)	24 (802.3af/at)	48 (802.3af/802.3at)
PoE Power Budget	180 W	370 W	740 W
Mean Time Between Failures	> 10 years	> 10 years	> 10 years
Retail Price	$1,000	$1,250	$1,500

A customer wants to deploy 12 FortiAP 431F devices on high density conference center, but they do not currently have any PoE switches to connect them to. They want to be able to run them at full power while having network redundancy From the FortiSwitch models and sample retail prices shown in the exhibit, which build of materials would have the lowest cost, while fulfilling the customer\\'s requirements?

A. 1x FortiSwitch 248EFPOE

B. 2x FortiSwitch 224E-POE

C. 2x FortiSwitch 248E-FPOE

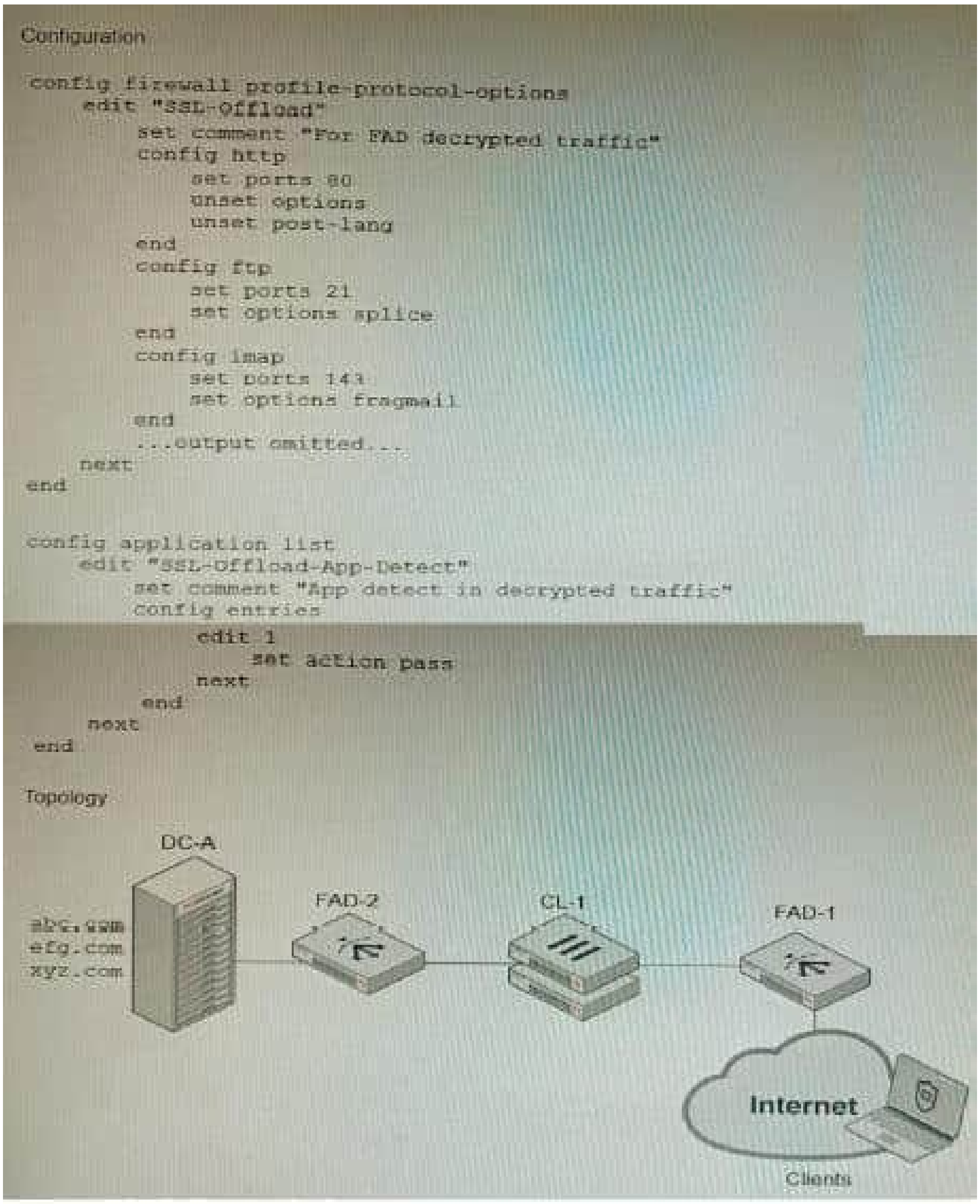
D. 2x FortiSwitch 124E-FPOE

Correct Answer: C

Explanation: The customer wants to deploy 12 FortiAP 431F devices on a high density conference center, but they do not have any PoE switches to connect them to. They want to be able to run them at full power while having network redundancy. PoE switches are switches that can provide both data and power to connected devices over Ethernet cables, eliminating the need for separate power adapters or outlets. PoE switches are useful for deploying devices such as wireless access points, IP cameras, and VoIP phones in locations where power outlets are scarce or inconvenient. The FortiAP 431F is a wireless access point that supports PoE+ (IEEE 802.3at) standard, which can deliver up to 30W of power per port. The FortiAP 431F has a maximum power consumption of 25W when running at full power. Therefore, to run 12 FortiAP 431F devices at full power, the customer needs PoE switches that can provide at least 300W of total PoE power budget (25W x 12). The customer also needs network redundancy, which means that they need at least two PoE switches to connect the FortiAP devices in case one switch fails or loses power. From the FortiSwitch models and sample retail prices shown in the exhibit, the build of materials that has the lowest cost while fulfilling the customer\\'s requirements is 2x FortiSwitch 248E- FPOE. The FortiSwitch 248E-FPOE is a PoE switch that has 48 GE ports with PoE+ capability and a total PoE power budget of 370W. It also has 4x 10 GE SFP+ uplink ports for high-speed connectivity. The sample retail price of the FortiSwitch 248E-FPOE is $1,995, which means that two units will cost $3,990. This is the lowest cost among the other options that can meet the customer\\'s requirements. Option A is incorrect because the FortiSwitch 248EFPOE is a non-PoE switch that has no PoE capability or power budget. It cannot provide power to the FortiAP devices over Ethernet cables. Option B is incorrect because the FortiSwitch 224E-POE is a PoE switch that has only 24 GE ports with PoE+ capability and a total PoE powerbudget of 185W. It cannot provide enough ports or power to run 12 FortiAP devices at full power. Option D is incorrect because the FortiSwitch 124E-FPOE is a PoE switch that has only 24 GE ports with PoE+ capability and a total PoE power budget of 185W. It cannot provide enough ports or power to run 12 FortiAP devices at full power. References: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSwitch_Secure_Access_Series.pdfhttps://www.fortinet.com/content/dam/fortine t/assets/data-sheets/FortiAP_400_Series.pdf

QUESTION 4

Refer to the exhibits.



Configuration

```
config firewall profile-protocol-options
    edit "SSL-Offload"
        set comment "For FAD decrypted traffic"
        config http
            set ports 80
            unset options
            unset post-lang
        end
        config ftp
            set ports 21
            set options splice
        end
        config imap
            set ports 143
            set options fragmail
        end
        ...output omitted...
    next
end

config application list
    edit "SSL-Offload-App-Detect"
        set comment "App detect in decrypted traffic"
        config entries
            edit 1
                set action pass
            next
        end
    next
end
```

Topology

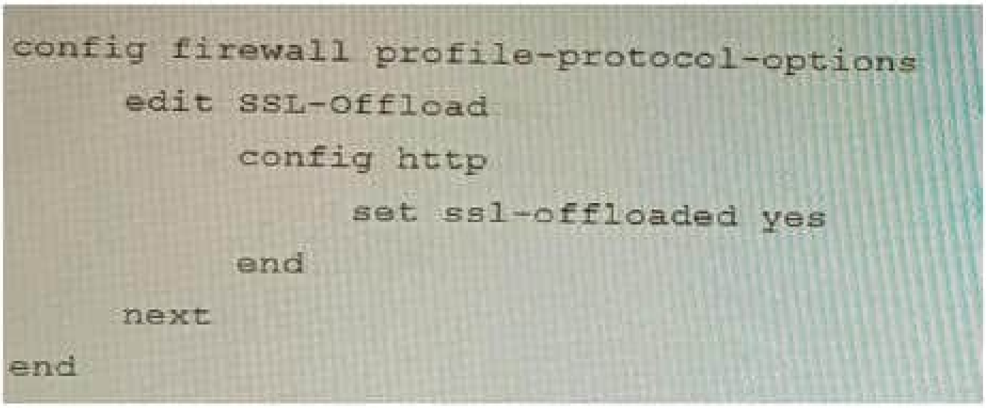
A FortiGate cluster (CL-1) protects a data center hosting multiple web applications. A pair of FortiADC devices are already configured for SSL decryption (FAD-1), and re-encryption (FAD-2). CL-1 must accept unencrypted traffic from FAD-1,

perform application detection on the plain-text traffic, and forward the inspected traffic to FAD-2.

The SSL-Offload-App-Detect application list and SSL-Offload protocol options profile are applied to the firewall policy handling the web application traffic on CL-1.

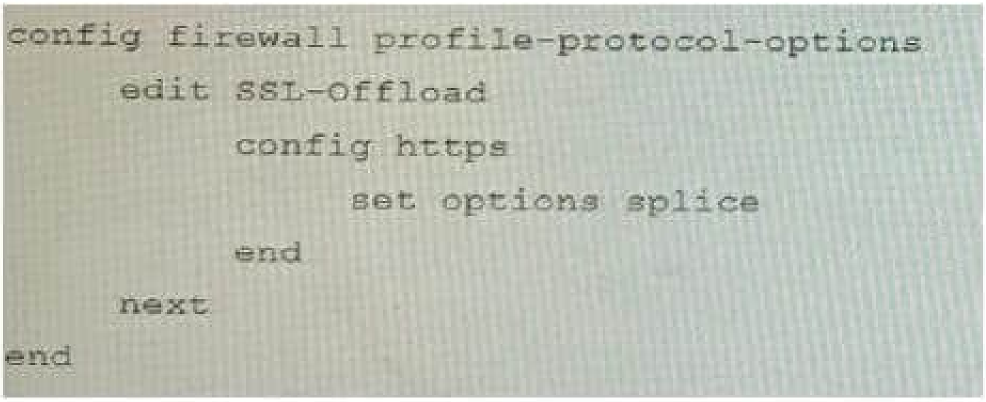
Given this scenario, which two configuration tasks must the administrator perform on CL-1? (Choose two.)

A)



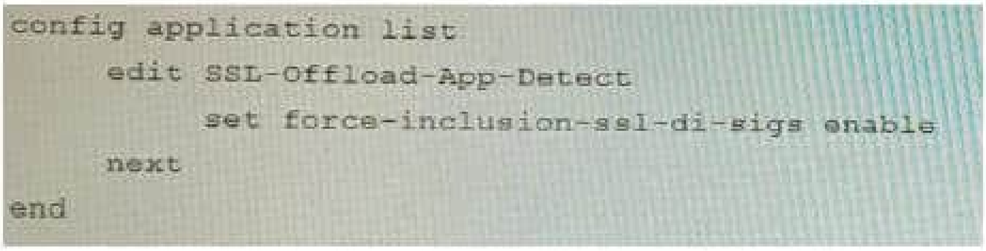
```
config firewall profile-protocol-options
    edit SSL-Offload
        config http
            set ssl-offloaded yes
        end
    next
end
```

B)



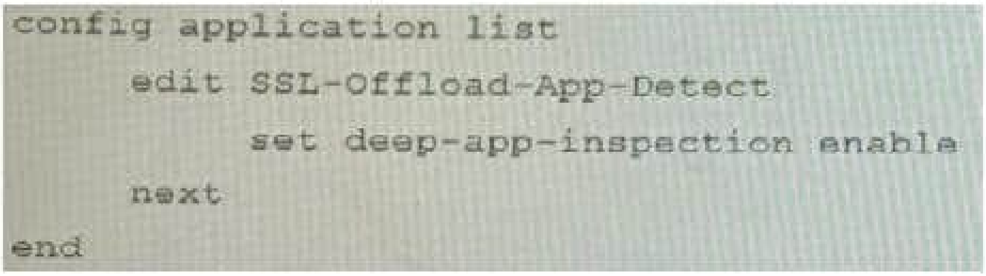
```
config firewall profile-protocol-options
    edit SSL-Offload
        config https
            set options splice
        end
    next
end
```

C)



```
config application list
    edit SSL-Offload-App-Detect
        set force-inclusion-ssl-di-sigs enable
    next
end
```

D)



```
config application list
    edit SSL-Offload-App-Detect
        set deep-app-inspection enable
    next
end
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: BC

Explanation: To enable application detection on plain-text traffic that has been decrypted by FortiADC, the administrator must perform two configuration tasks on CL-1:

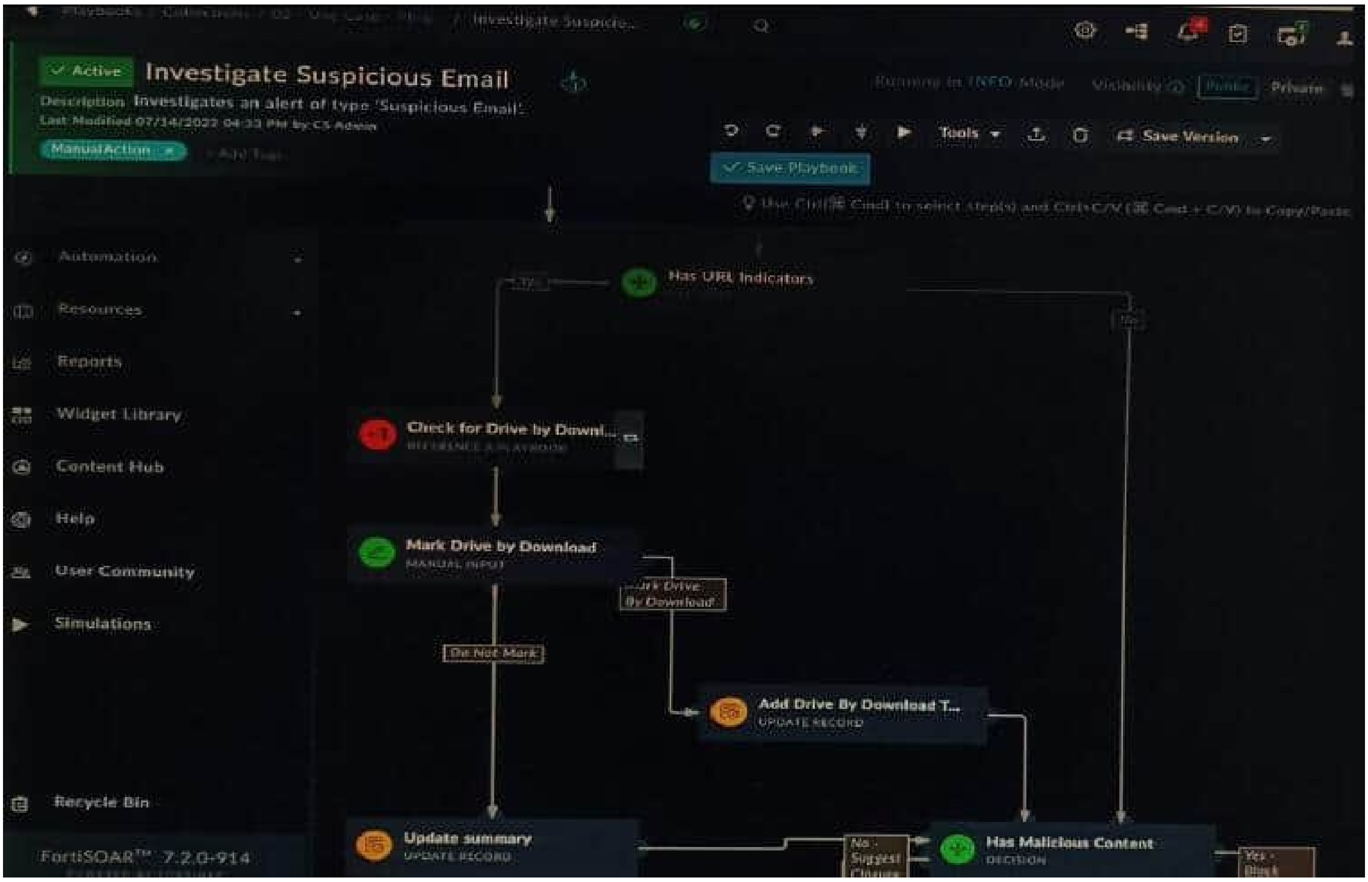
Enable SSL offloading in the firewall policy and select the SSL-Offload protocol options profile.

Enable application control in the firewall policy and select the SSL-Offload-App- Detect application list. References:

https://docs.fortinet.com/document/fortigate/6.4.0/cookbook/103438/application- detection-on-ssl-offloaded-traffic

QUESTION 5

Refer to the exhibit showing a FortiSOAR playbook.



You are investigating a suspicious e-mail alert on FortiSOAR, and after reviewing the executed playbook, you can see that it requires intervention.

What should be your next step?

A. Go to the Incident Response tasks dashboard and run the pending actions

B. Click on the notification icon on FortiSOAR GUI and run the pending input action

C. Run the Mark Drive by Download playbook action

D. Reply to the e-mail with the requested Playbook action

Correct Answer: A

Explanation: The exhibited playbook requires intervention, which means that the playbook has reached a point where it needs a human operator to take action. The next step should be to go to the Incident Response tasks dashboard and run

the pending actions. This will allow you to see the pending actions that need to be taken and to take those actions. The other options are not correct. Option B will only show you the notification icon, but it will not allow you to run the pending

input action. Option C will run the Mark Drive by Download playbook action, but this is not the correct action to take in this case. Option D is not a valid option.

Here are some additional details about pending actions in FortiSOAR:

Pending actions are actions that need to be taken by a human operator. Pending actions are displayed in the Incident Response tasks dashboard. Pending actions can be run by clicking on the action in the dashboard.