Free Questions for NSE8_812 by dumpshq

Shared by Bryan on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

A customer is planning on moving their secondary data center to a cloud-based IaaS. They want to place all the Oracle-based systems Oracle Cloud, while the other systems will be on Microsoft Azure with ExpressRoute service to their main data center.

They have about 200 branches with two internet services as their only WAN connections. As a security consultant you are asked to design an architecture using Fortinet products with security, redundancy and performance as a priority.

Which two design options are true based on these requirements? (Choose two.)

Options:

A- Systems running on Azure will need to go through the main data center to access the services on Oracle Cloud.

B- Use FortiGate VM for IPSEC over ExpressRoute, as traffic is not encrypted by Azure.

C- Branch FortiGate devices must be configured as VPN clients for the branches' internal network to be able to access Oracle services without using public IPs.

D- Two ExpressRoute services to the main data center are required to implement SD-WAN between a FortiGate VM in Azure and a FortiGate device at the data center edge

Answer:

A, C

Explanation:

a) Systems running on Azure will need to go through the main data center to access the services on Oracle Cloud. This is because the Oracle Cloud is not directly connected to the Azure Cloud. The traffic will need to go through the main data center in order to reach the Oracle Cloud.

c) Branch FortiGate devices must be configured as VPN clients for the branches' internal network to be able to access Oracle services without using public IPs. This is because the Oracle Cloud does not allow direct connections from the internet. The traffic will need to go through the FortiGate devices in order to reach the Oracle Cloud.

The other options are not correct.

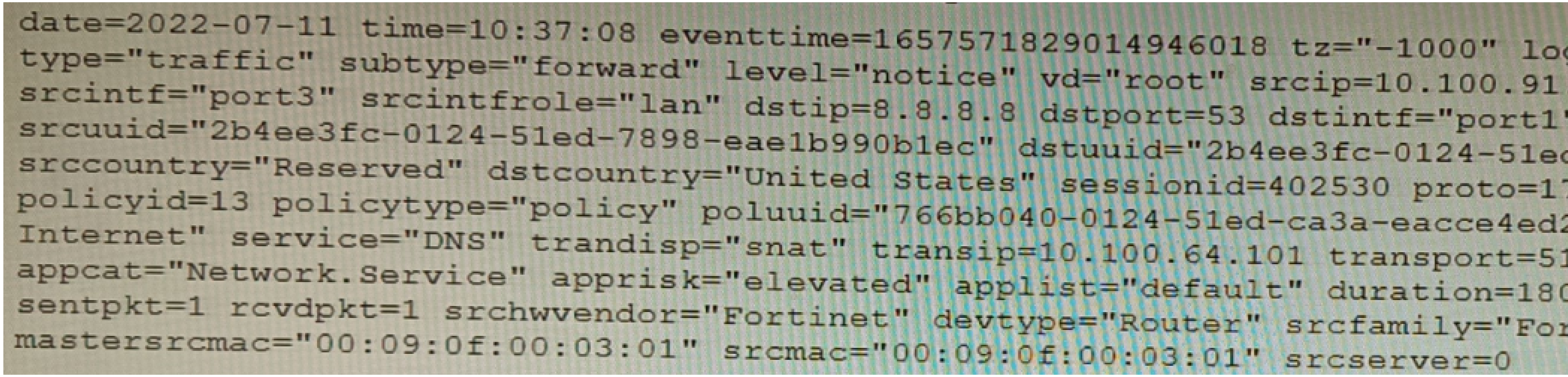
b) Use FortiGate VM for IPSEC over ExpressRoute, as traffic is not encrypted by Azure. This is not necessary. Azure does encrypt traffic over ExpressRoute.

d) Two ExpressRoute services to the main data center are required to implement SD-WAN between a FortiGate VM in Azure and a FortiGate device at the data center edge. This is not necessary. A single ExpressRoute service can be used to implement SD-WAN between a FortiGate VM in Azure and a FortiGate device at the data center edge.

Question 2

Question Type: **MultipleChoice**

You must analyze an event that happened at 20:37 UTC. One log relevant to the event is extracted from FortiGate logs:



```
date=2022-07-11 time=10:37:08 eventtime=1657571829014946018 tz="-1000" lo
type="traffic" subtype="forward" level="notice" vd="root" srcip=10.100.91
srcintf="port3" srcintfrole="lan" dstip=8.8.8.8 dstport=53 dstintf="port1"
srcuuid="2b4ee3fc-0124-51ed-7898-eae1b990b1ec" dstuuid="2b4ee3fc-0124-51e
srccountry="Reserved" dstcountry="United States" sessionid=402530 proto=1
policyid=13 policytype="policy" poluuid="766bb040-0124-51ed-ca3a-eacce4ed
Internet" service="DNS" trandisp="snat" transip=10.100.64.101 transport=5
appcat="Network.Service" apprisk="elevated" applist="default" duration=18
sentpkt=1 rcvdpkt=1 srchwvendor="Fortinet" devtype="Router" srcfamily="Fo
mastersrcmac="00:09:0f:00:03:01" srcmac="00:09:0f:00:03:01" srcserver=0
```

The devices and the administrator are all located in different time zones Daylight savings time (DST) is disabled

* The FortiGate is at GMT-1000.

* The FortiAnalyzer is at GMT-0800

* Your browser local time zone is at GMT-03.00

You want to review this log on FortiAnalyzer GUI, what time should you use as a filter?

Options:

A- 20:37:08

B- 10:37:08

C- 17:37:08

D- 12.37:08

Answer:

C

Explanation:

To review this log on FortiAnalyzer GUI, the administrator should use the time filter that matches the local time zone of FortiAnalyzer, which is GMT-0800. Since the log was generated at 20:37 UTC (GMT+0000), the corresponding time in GMT-0800 is 20:37 - 8 hours = 12:37. However, since DST is disabled on FortiAnalyzer, the administrator should add one hour to account for daylight saving time difference, resulting in 12:37 + 1 hour = 13:37. Therefore, the time filter to use is 13:37:08. References: https://docs.fortinet.com/document/fortianalyzer/6.4.0/administration-guide/103664/time-zone-and-daylight-saving-time

Question 3

Question Type: MultipleChoice

You are migrating the branches of a customer to FortiGate devices. They require independent routing tables on the LAN side of the network.

After reviewing the design, you notice the firewall will have many BGP sessions as you have two data centers (DC) and two ISPs per DC while each branch is using at least 10 internal segments.

Based on this scenario, what would you suggest as the more efficient solution, considering that in the future the number of internal segments, DCs or internet links per DC will increase?

Options:

A- No change in design is needed as even small FortiGate devices have a large memory capacity.

B- Acquire a FortiGate model with more capacity, considering the next 5 years growth.

C- Implement network-id, neighbor-group and increase the advertisement-interval

D- Redesign the SD-WAN deployment to only use a single VPN tunnel and segment traffic using VRFs on BGP

Answer:

D

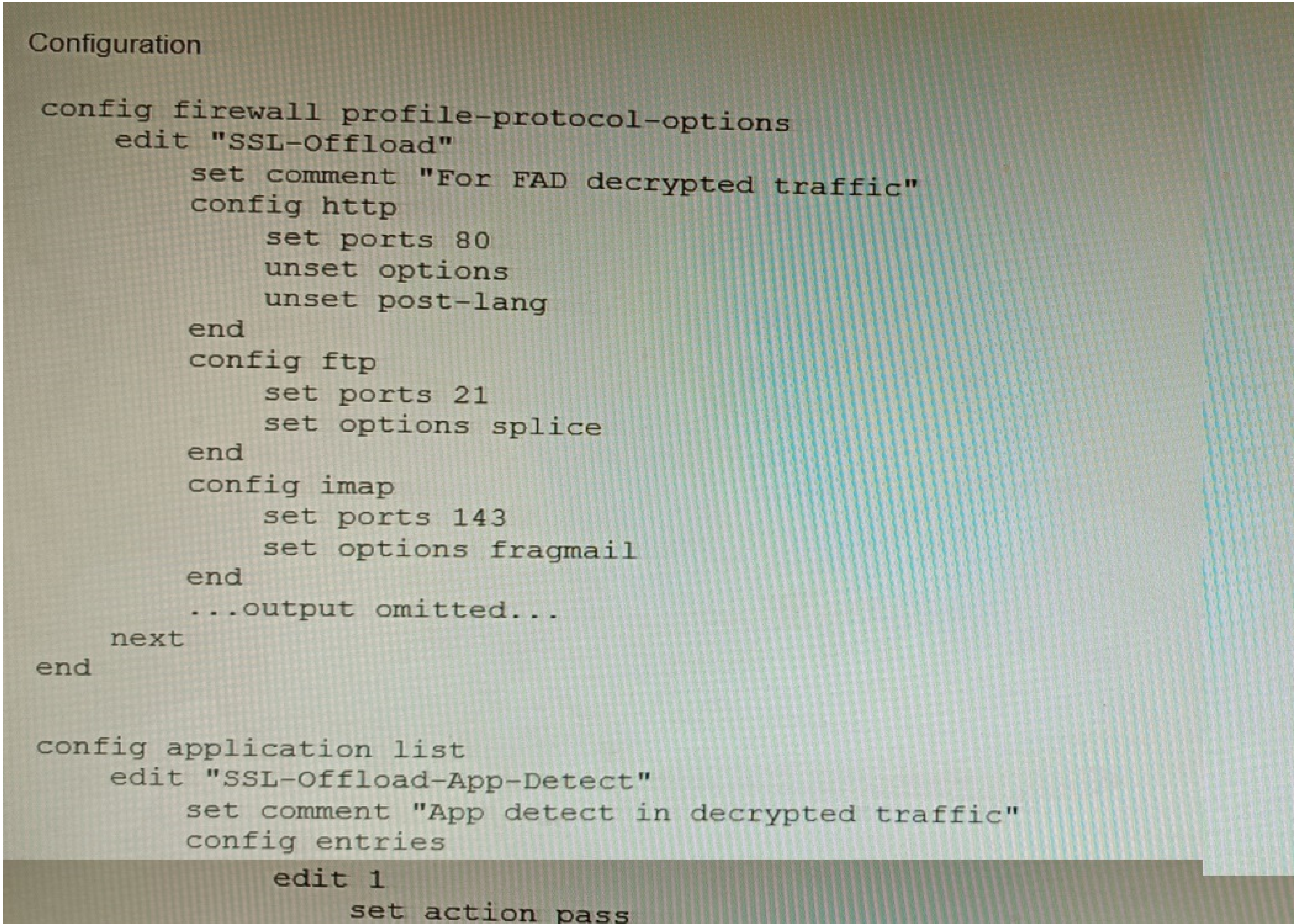
Explanation:

Using multiple VPN tunnels and BGP sessions for each internal segment is not scalable and efficient, especially when the number of segments, DCs or internet links per DC increases. A better solution is to use a single VPN tunnel per branch and segment traffic using virtual routing and forwarding (VRF) instances on BGP. This way, each VRF can have its own routing table and BGP session, while sharing the same VPN tunnel. References: https://docs.fortinet.com/document/fortigate/6.4.0/cookbook/103439/sd-wan-with-vrf-and-bgp

Question 4

Question Type: MultipleChoice

Refer to the exhibits.



Configuration

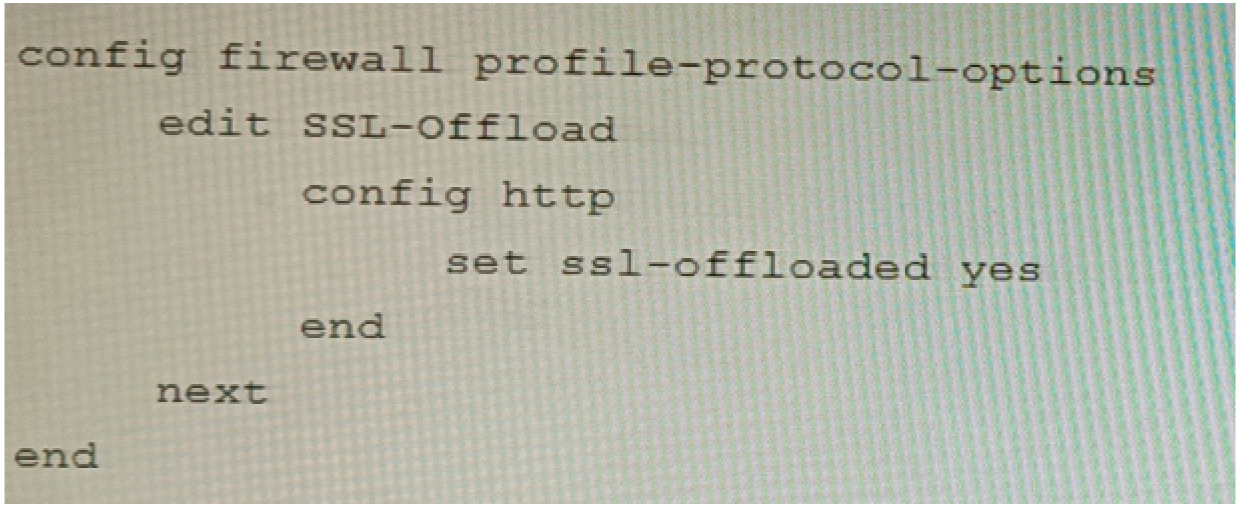
```
config firewall profile-protocol-options
    edit "SSL-Offload"
        set comment "For FAD decrypted traffic"
        config http
            set ports 80
            unset options
            unset post-lang
        end
        config ftp
            set ports 21
            set options splice
        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
```

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.

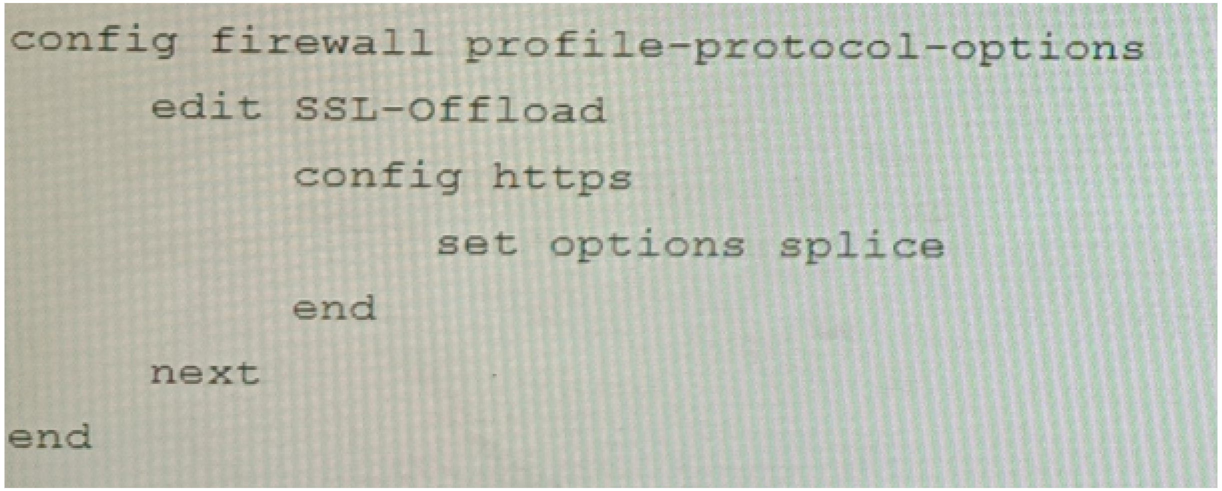
Given this scenario, which two configuration tasks must the administrator perform on CL-1? (Choose two.)

A)

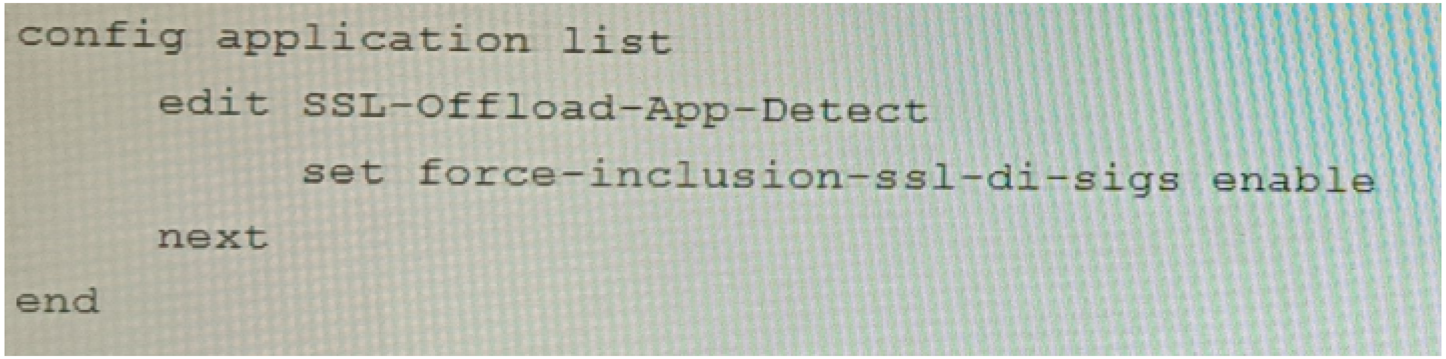


```
config firewall profile-protocol-options
    edit SSL-Offload
        config http
            set ssl-offloaded yes
        end
    next
end
```

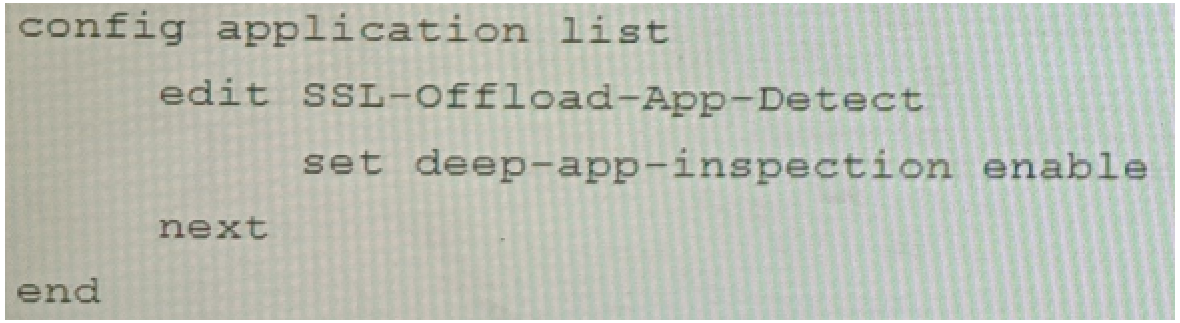
B)



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



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



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

Options:

A- Option A

B- Option B

C- Option C

D- Option D

Answer:

B, C

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:

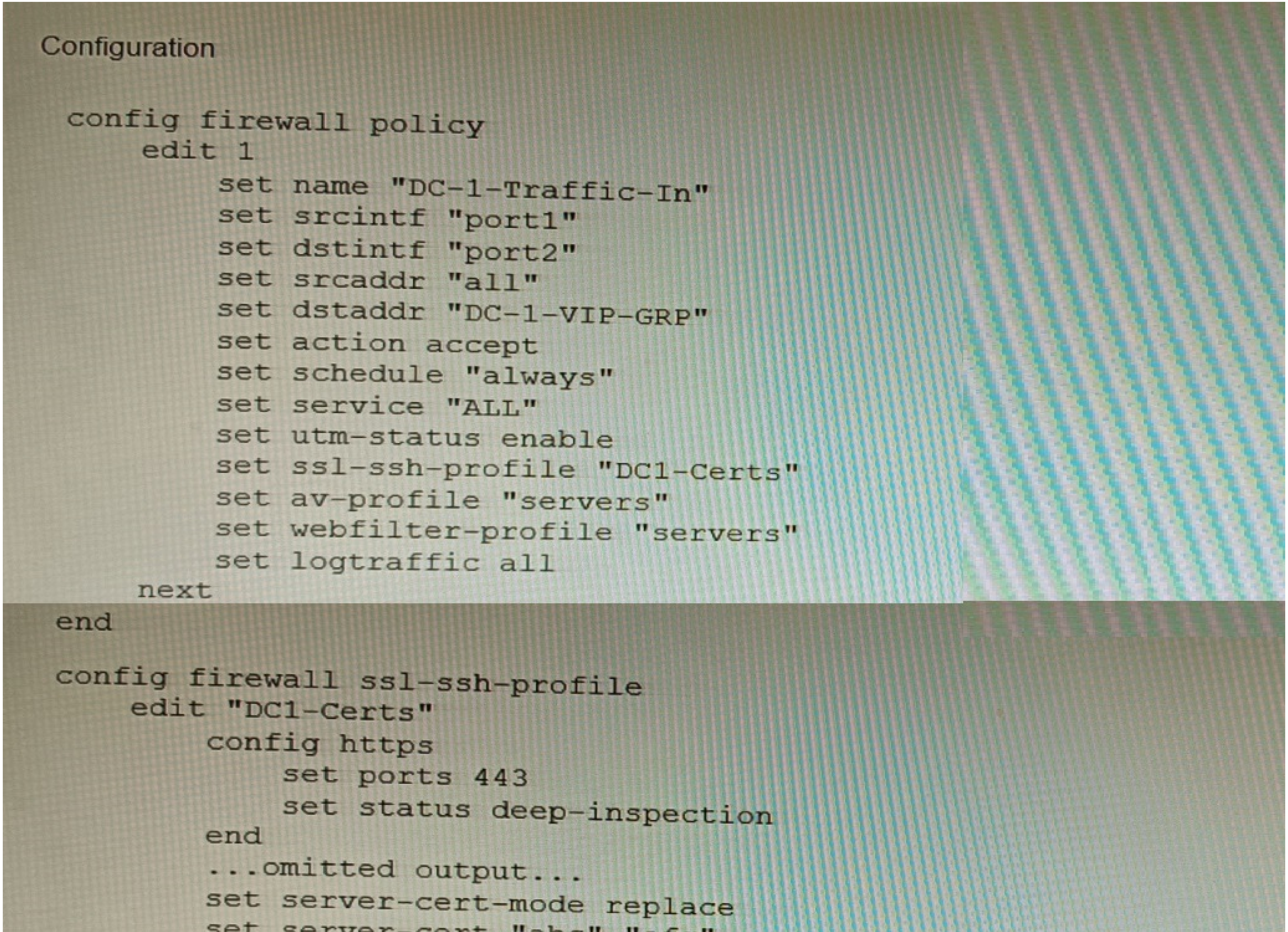
Enable SSL offloading in the firewall policy and select the SSL-Offload protocol options profile.

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

Question Type: MultipleChoice

Refer to the exhibits, which show a firewall policy configuration and a network topology.



Configuration

```
config firewall policy
    edit 1
        set name "DC-1-Traffic-In"
        set srcintf "port1"
        set dstintf "port2"
        set srcaddr "all"
        set dstaddr "DC-1-VIP-GRP"
        set action accept
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set ssl-ssh-profile "DC1-Certs"
        set av-profile "servers"
        set webfilter-profile "servers"
        set logtraffic all
    next
end

config firewall ssl-ssh-profile
    edit "DC1-Certs"
        config https
            set ports 443
            set status deep-inspection
        end
        ...omitted output...
        set server-cert-mode replace
        set server-cert "abc" "xfs"
```

An administrator has configured an inbound SSL inspection profile on a FortiGate device (FG-1) that is protecting a data center hosting multiple web pages-Given the scenario shown in the exhibits, which certificate will FortiGate use to handle requests to xyz.com?

Options:

A- FortiGate will fall-back to the default Fortinet_CA_SSL certificate.

B- FortiGate will reject the connection since no certificate is defined.

C- FortiGate will use the Fortinet_CA_Untrusted certificate for the untrusted connection,

D- FortiGate will use the first certificate in the server-cert list---the abc.com certificate

Answer:

A

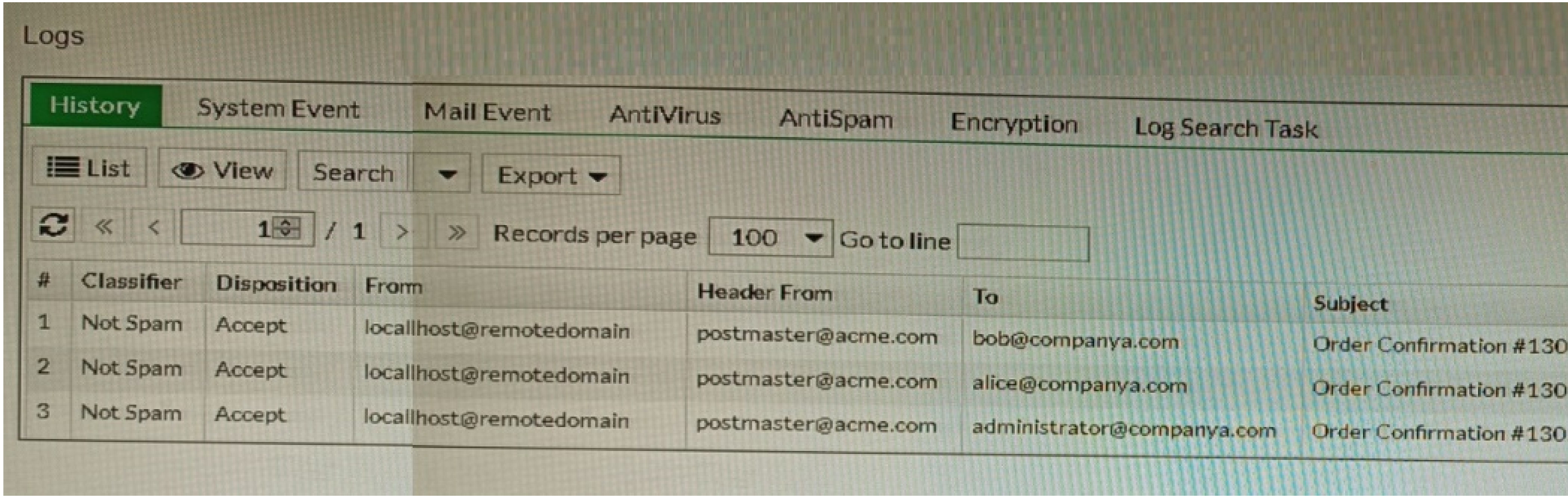
Explanation:

When using inbound SSL inspection, FortiGate needs to present a certificate to the client that matches the requested domain name. If no matching certificate is found in the server-cert list, FortiGate will fall-back to the default Fortinet_CA_SSL certificate, which is self-signed and may trigger a warning on the client browser. References:
https://docs.fortinet.com/document/fortigate/6.4.0/cookbook/103437/inbound-ssl-inspection

Question 6

Question Type: MultipleChoice

Refer to the exhibit showing the history logs from a FortiMail device.



#	Classifier	Disposition	From	Header From	To	Subject
1	Not Spam	Accept	localhost@remotedomain	postmaster@acme.com	bob@companya.com	Order Confirmation #130
2	Not Spam	Accept	localhost@remotedomain	postmaster@acme.com	alice@companya.com	Order Confirmation #130
3	Not Spam	Accept	localhost@remotedomain	postmaster@acme.com	administrator@companya.com	Order Confirmation #130

Which FortiMail email security feature can an administrator enable to treat these emails as spam?

Options:

A- DKIM validation in a session profile

B- Sender domain validation in a session profile

C- Impersonation analysis in an antispam profile

D- Soft fail SPF validation in an antispam profile

Answer:

C

Explanation:

Impersonation analysis is a feature that detects emails that attempt to impersonate a trusted sender, such as a company executive or a well-known brand, by using spoofed or look-alike email addresses. This feature can help prevent phishing and business email compromise (BEC) attacks. Impersonation analysis can be enabled in an antispam profile and applied to a firewall policy. References: https://docs.fortinet.com/document/fortimail/6.4.0/administration-guide/103663/impersonation-analysis

Question 7

Question Type: **MultipleChoice**

You want to use the MTA adapter feature on FortiSandbox in an HA-Cluster. Which statement about this solution is true?

Options:

A- The configuration of the MTA Adapter Local Interface is different than on port1.

B- The MTA adapter is only available in the primary node.

C- The MTA adapter mode is only detection mode.

D- The configuration is different than on a standalone device.

Answer:

B

Explanation:

The MTA adapter feature on FortiSandbox is a feature that allows FortiSandbox to act as a mail transfer agent (MTA) that can receive, inspect, and forward email messages from external sources. The MTA adapter feature can be used to integrate FortiSandbox with third-party email security solutions that do not support direct integration with FortiSandbox, such as Microsoft Exchange Server or Cisco Email Security Appliance (ESA). The MTA adapter feature can also be used to enhance email security by adding an additional layer of inspection and filtering before delivering email messages to the final destination. The MTA adapter feature can be enabled on FortiSandbox in an HA-Cluster, which is a configuration that allows two FortiSandbox units to synchronize their settings and data and provide high availability and load balancing for sandboxing services. However, one statement about this solution that is true is that the MTA adapter is only available in the primary node. This means that only one FortiSandbox unit in the HA-Cluster can act as an MTA and receive email messages from external sources, while the other unit acts as a backup node that can take over the MTA role if the primary

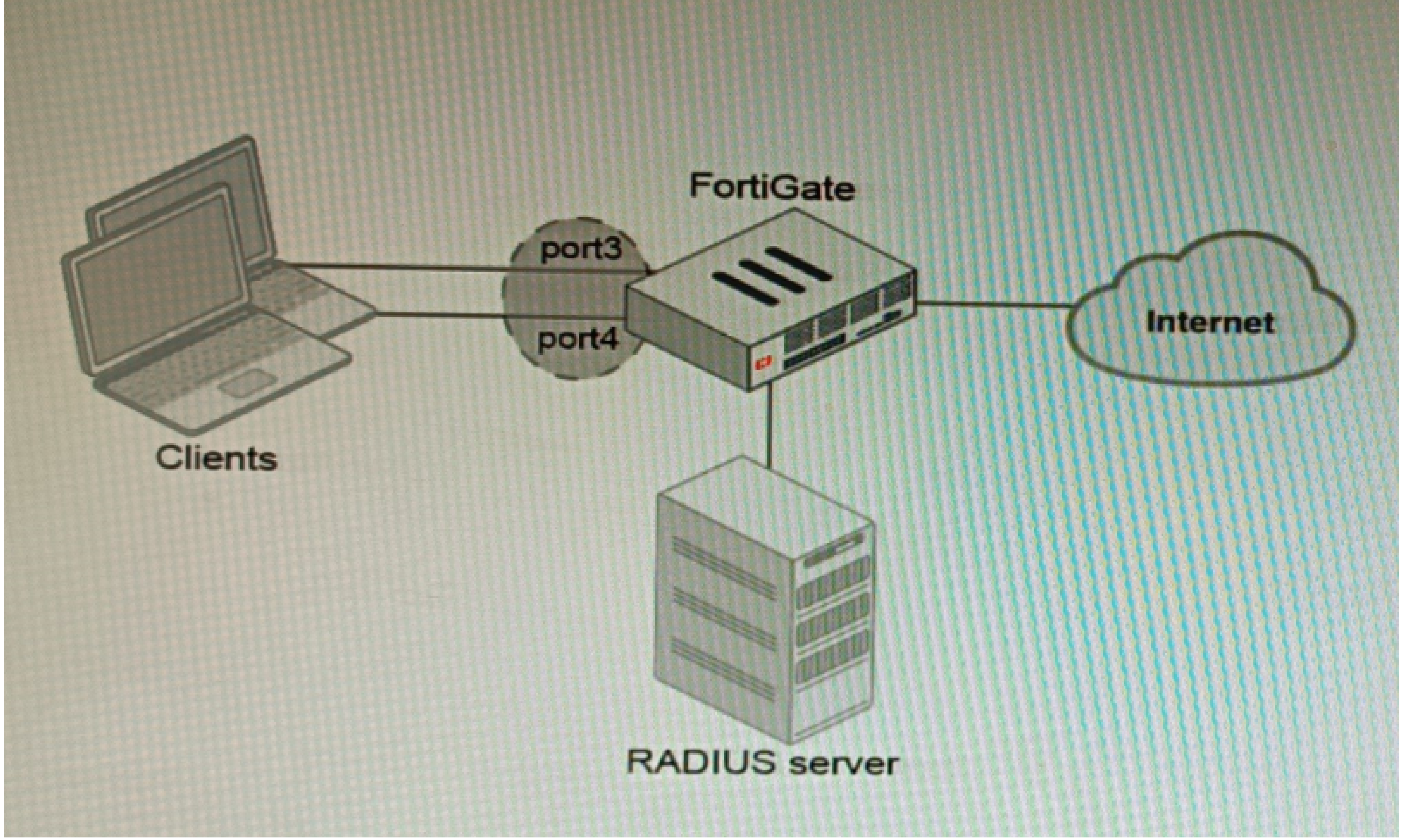
node fails or loses connectivity. This also means that only one IP address or FQDN can be used to configure the external sources to send email messages to the FortiSandbox MTA, which is the IP address or FQDN of the primary node. References:
https://docs.fortinet.com/document/fortisandbox/3.2.0/administration-guide/19662/mail-transfer-agent-mta
https://docs.fortinet.com/document/fortisandbox/3.2.0/administration-guide/19662/high-availability-ha

Question 8

Question Type: MultipleChoice

Refer to the exhibits.

Exhibit A



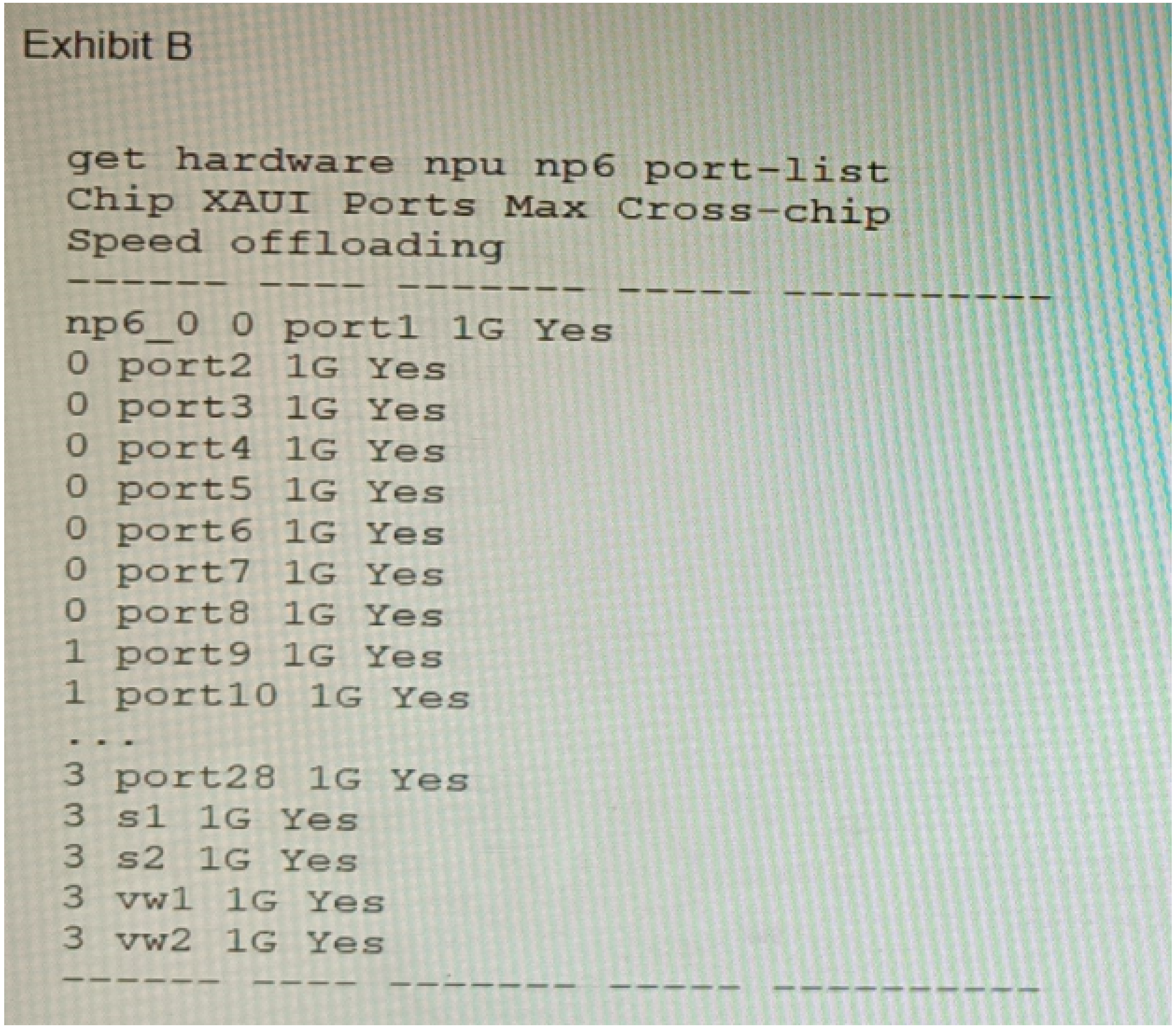


Exhibit B

```
get hardware npu np6 port-list
Chip XAUI Ports Max Cross-chip
Speed offloading
------ ---- ------- ----- ----------
np6_0 0 port1 1G Yes
0 port2 1G Yes
0 port3 1G Yes
0 port4 1G Yes
0 port5 1G Yes
0 port6 1G Yes
0 port7 1G Yes
0 port8 1G Yes
1 port9 1G Yes
1 port10 1G Yes
...
3 port28 1G Yes
3 s1 1G Yes
3 s2 1G Yes
3 vw1 1G Yes
3 vw2 1G Yes
------ ---- ------- ----- ----------
```

A customer is looking for a solution to authenticate the clients connected to a hardware switch interface of a FortiGate 400E.

Referring to the exhibits, which two conditions allow authentication to the client devices before assigning an IP address? (Choose two.)

Options:

A- FortiGate devices with NP6 and hardware switch interfaces cannot support 802.1X authentication.

B- Devices connected directly to ports 3 and 4 can perform 802 1X authentication.

C- Ports 3 and 4 can be part of different switch interfaces.

D- Client devices must have 802 1X authentication enabled

Answer:

B, D

Explanation:

The customer wants to deploy a solution to authenticate the clients connected to a hardware switch interface of a FortiGate 400E device. A hardware switch interface is an interface that combines multiple physical interfaces into one logical interface, allowing them to act as a single switch with one IP address and one set of security policies. The customer wants to use 802.1X authentication for this solution, which is a standard protocol for port-based network access control (PNAC) that authenticates clients based on their credentials before granting them access to network resources. One condition that allows authentication to the client devices before assigning an IP address is that devices connected directly to ports 3 and 4 can perform 802.1X authentication. This is because ports 3 and 4 are part of the hardware switch interface named "lan", which has an IP address of 10.10.10.254/24 and an inbound SSL inspection profile named "ssl-inspection". The inbound SSL inspection profile enables the FortiGate device to intercept and inspect SSL/TLS traffic from clients before forwarding it to servers, which allows it to apply security policies and features such as antivirus, web filtering, application control, etc. However, before performing SSL inspection, the FortiGate device needs to authenticate the clients using 802.1X authentication, which requires the clients to send their credentials (such as username and password) to the FortiGate device over a secure EAP (Extensible Authentication Protocol) channel. The FortiGate device then verifies the credentials with an authentication server (such as RADIUS or LDAP) and grants or denies access to the clients based on the authentication result. Therefore, devices connected directly to ports 3 and 4 can perform 802.1X authentication before assigning an IP address. Another condition that allows authentication to the client devices before assigning an IP address is that client devices must have 802.1X authentication enabled. This is because 802.1X authentication is a mutual process that requires both the client devices and the FortiGate device to support and enable it. The client devices must have 802.1X authentication enabled in their network settings, which allows them to initiate the authentication process when they connect to the hardware switch interface of the FortiGate device. The client devices must also have an 802.1X supplicant software installed, which is a program that runs on the client devices and handles the communication with the FortiGate device using EAP messages. The client devices must also have a trusted certificate installed, which is used to verify the identity of the FortiGate device and establish a secure EAP channel. Therefore, client devices must have 802.1X authentication enabled before assigning an IP address. References: https://docs.fortinet.com/document/fortigate/7.0.0/administration-guide/19662/hardware-switch-interfaces https://docs.fortinet.com/document/fortigate/7.0.0/administration-guide/19662/802-1x-authentication

Question 9

Question Type: **MultipleChoice**

Refer to the exhibits.

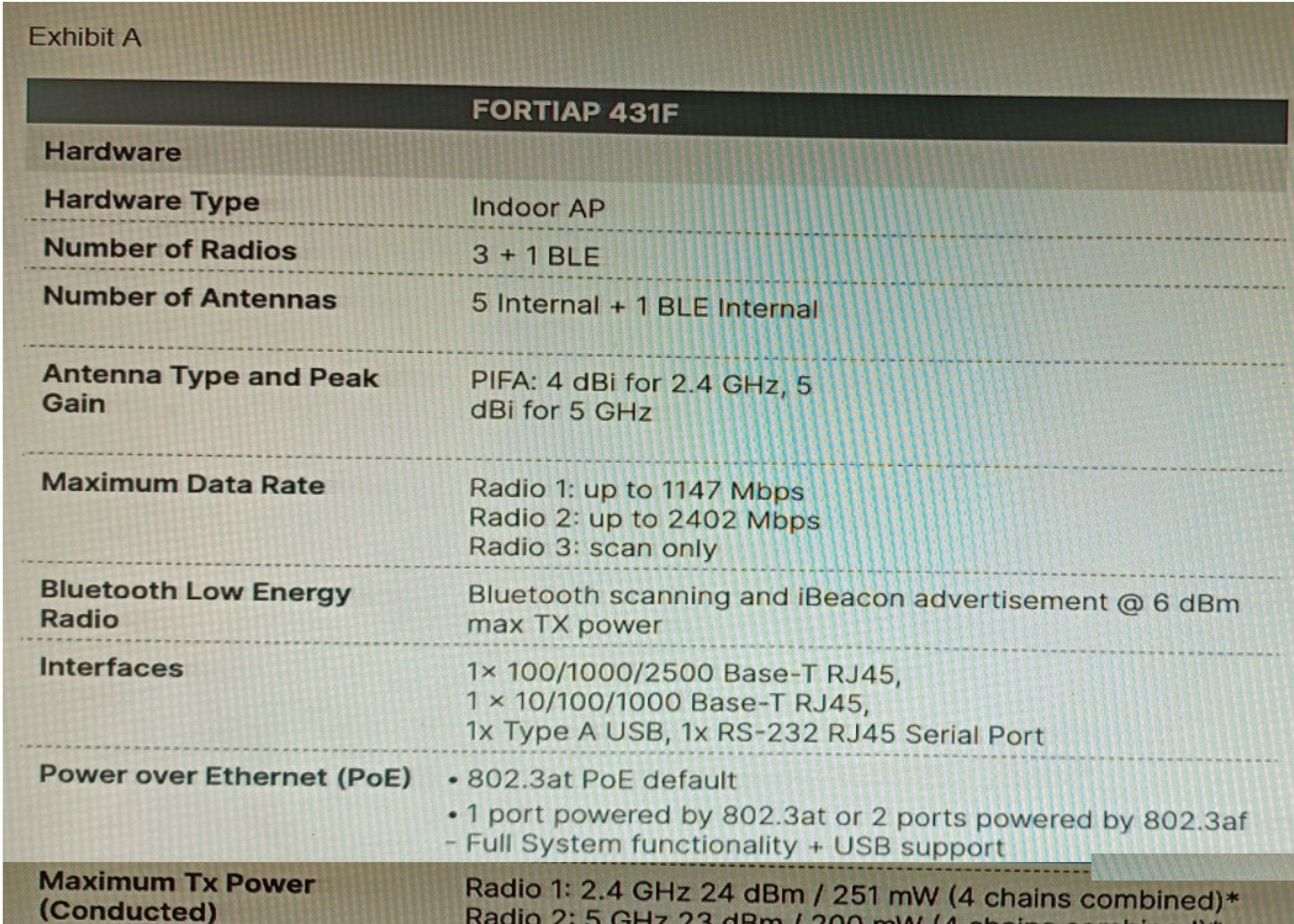


Exhibit A

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)*

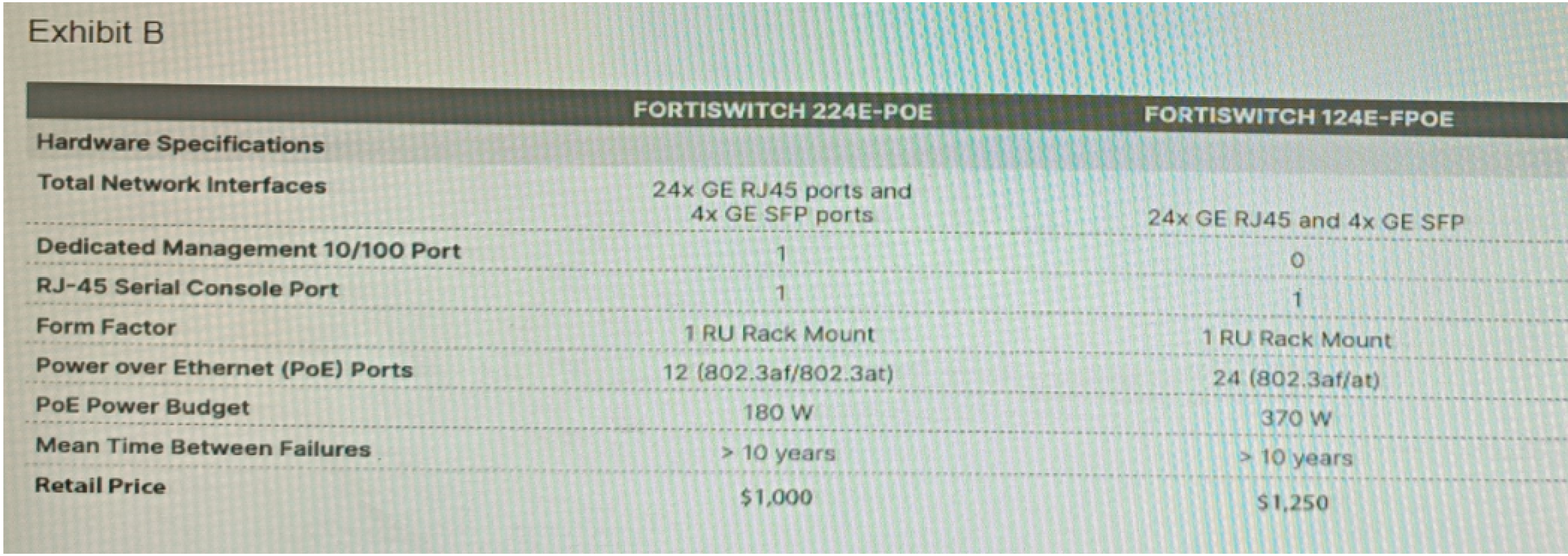


Exhibit B

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

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?

Options:

A- 1x FortiSwitch 248EFPOE

B- 2x FortiSwitch 224E-POE

C- 2x FortiSwitch 248E-FPOE

D- 2x FortiSwitch 124E-FPOE

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 power budget 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.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiAP_400_Series.pdf

Question 10

Question Type: **MultipleChoice**

You are deploying a FortiExtender (FEX) on a FortiGate-60F. The FEX will be managed by the FortiGate. You anticipate high utilization. The requirement is to minimize the overhead on the device for WAN traffic.

Which action achieves the requirement in this scenario?

Options:

A- Add a switch between the FortiGate and FEX.

B- Enable CAPWAP connectivity between the FortiGate and the FortiExtender.

C- Change connectivity between the FortiGate and the FortiExtender to use VLAN Mode

D- Add a VLAN under the FEX-WAN interface on the FortiGate.

Answer:

C

Explanation:

VLAN Mode is a more efficient way to connect a FortiExtender to a FortiGate than CAPWAP Mode. This is because VLAN Mode does not require the FortiExtender to send additional control traffic to the FortiGate.

The other options are not correct.

a) Add a switch between the FortiGate and FEX. This will add overhead to the network, as the switch will need to process the traffic.

b) Enable CAPWAP connectivity between the FortiGate and the FortiExtender. This will increase the overhead on the FortiGate, as it will need to process additional control traffic.

d) Add a VLAN under the FEX-WAN interface on the FortiGate. This will not affect the overhead on the FortiGate.