NSE8_812$^{Q\&As}$

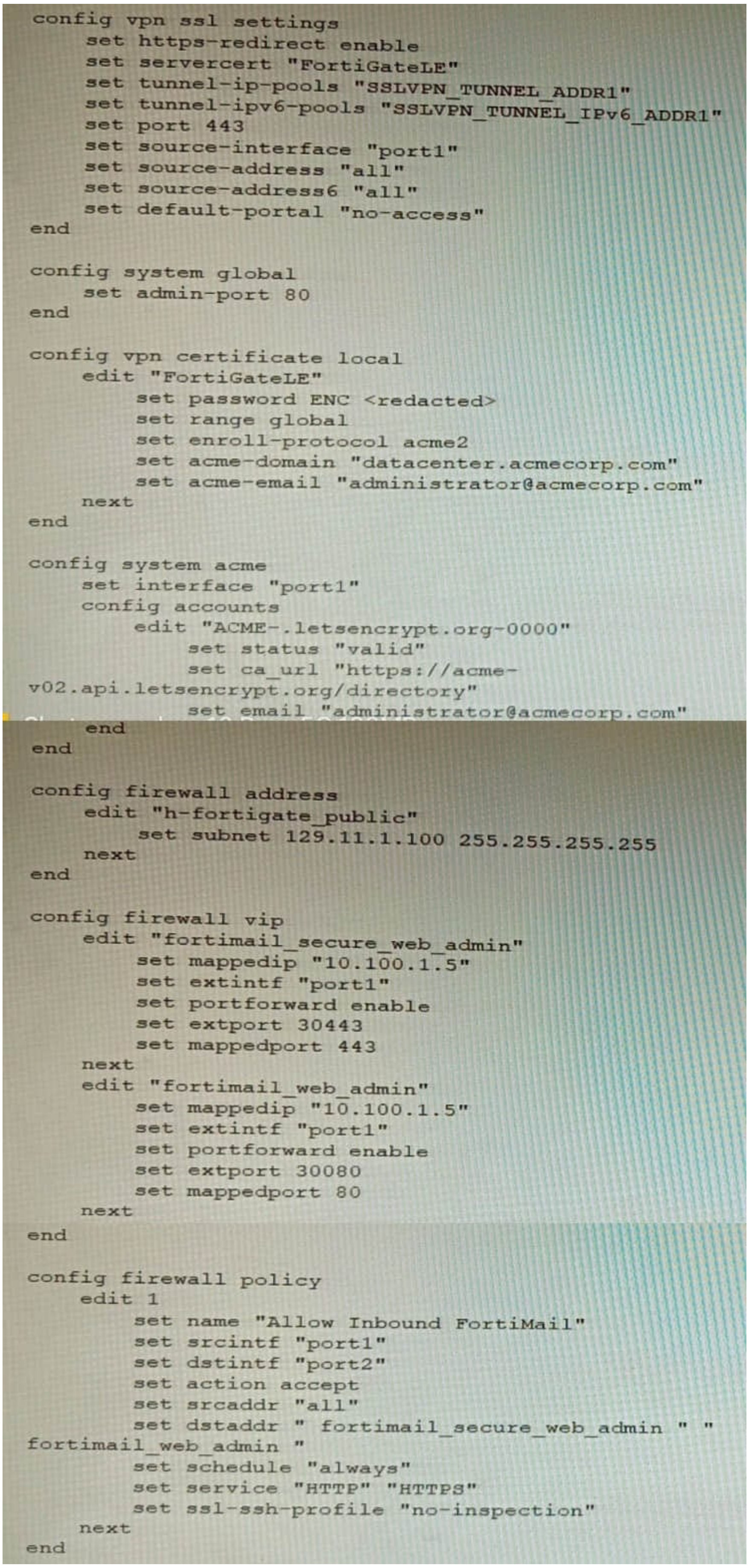
Network Security Expert 8 Written Exam

Pass Fortinet NSE8_812 Exam with 100% Guarantee

Following Questions and Answers are all new published by Fortinet Official Exam Center

QUESTION 1

Refer to the exhibit containing the configuration snippets from the FortiGate. Customer requirements: SSLVPN Portal must be accessible on standard HTTPS port (TCP/443) Public IP address (129.11.1.100) is assigned to portl Datacenter.acmecorp.com resolves to the public IP address assigned to portl

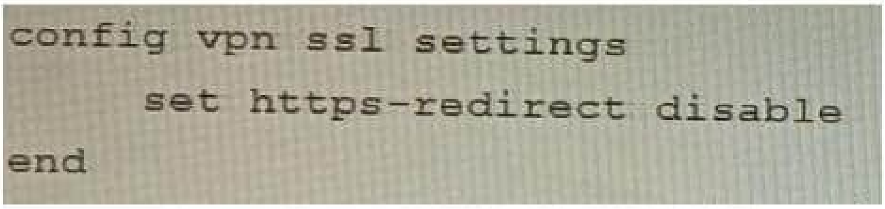


```
config vpn ssl settings
    set https-redirect enable
    set servercert "FortiGateLE"
    set tunnel-ip-pools "SSLVPN_TUNNEL_ADDR1"
    set tunnel-ipv6-pools "SSLVPN_TUNNEL_IPv6_ADDR1"
    set port 443
    set source-interface "port1"
    set source-address "all"
    set source-address6 "all"
    set default-portal "no-access"
end

config system global
    set admin-port 80
end

config vpn certificate local
    edit "FortiGateLE"
        set password ENC <redacted>
        set range global
        set enroll-protocol acme2
        set acme-domain "datacenter.acmecorp.com"
        set acme-email "administrator@acmecorp.com"
    next
end

config system acme
    set interface "port1"
    config accounts
        edit "ACME-.letsencrypt.org-0000"
            set status "valid"
            set ca_url "https://acme-
v02.api.letsencrypt.org/directory"
            set email "administrator@acmecorp.com"
    end
end

config firewall address
    edit "h-fortigate_public"
        set subnet 129.11.1.100 255.255.255.255
    next
end

config firewall vip
    edit "fortimail_secure_web_admin"
        set mappedip "10.100.1.5"
        set extintf "port1"
        set portforward enable
        set extport 30443
        set mappedport 443
    next
    edit "fortimail_web_admin"
        set mappedip "10.100.1.5"
        set extintf "port1"
        set portforward enable
        set extport 30080
        set mappedport 80
    next
end

config firewall policy
    edit 1
        set name "Allow Inbound FortiMail"
        set srcintf "port1"
        set dstintf "port2"
        set action accept
        set srcaddr "all"
        set dstaddr " fortimail_secure_web_admin " "
fortimail_web_admin "
        set schedule "always"
        set service "HTTP" "HTTPS"
        set ssl-ssh-profile "no-inspection"
    next
end
```

The customer has a Let\\'s Encrypt certificate that is going to expire soon and it reports that subsequent attempts to renew that certificate are failing.

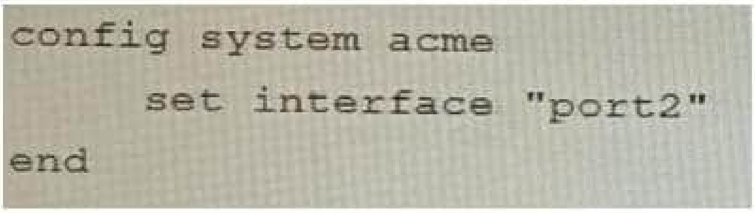
Reviewing the requirement and the exhibit, which configuration change below will resolve this issue?

○ A.



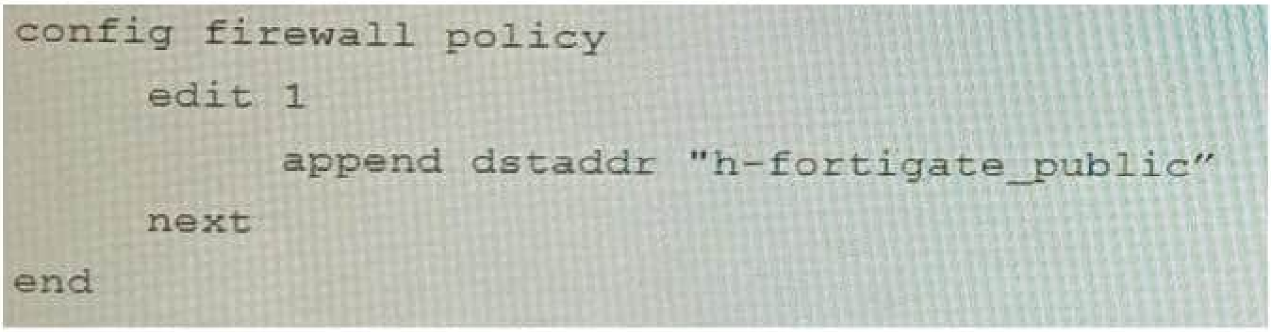
```
config vpn ssl settings
     set https-redirect disable
end
```

○ B.



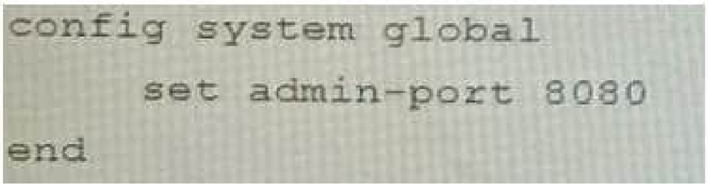
```
config system acme
     set interface "port2"
end
```

○ C.



```
config firewall policy
     edit 1
          append dstaddr "h-fortigate_public"
     next
end
```

○ D.



```
config system global
     set admin-port 8080
end
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: B

Explanation: The customer\\'s SSLVPN Portal is currently configured to use a self-signed certificate. This means that the certificate is not trusted by any browsers, and users will have to accept a security warning before they can connect to the

portal. To resolve this issue, the customer needs to configure the FortiGate to use a Let\\'s Encrypt certificate. Let\\'s Encrypt is a free certificate authority that provides trusted certificates for websites and other applications.

The configuration change in option B will configure the FortiGate to use a Let\\'s Encrypt certificate for the SSLVPN Portal. This will allow users to connect to the portal without having to accept a security warning.

The other configuration changes are not necessary to resolve the issue. Option A will configure the FortiGate to use a different port for the SSLVPN Portal, but this will not resolve the issue with the self-signed certificate. Option C will

configure the FortiGate to use a different DNS name for the SSLVPN Portal, but this will also not resolve the issue with the self-signed certificate. Option D will configure the FortiGate to use a different certificate authority for the SSLVPN

Portal, but this will also not resolve the issue because the customer still needs to use a trusted certificate.

References:

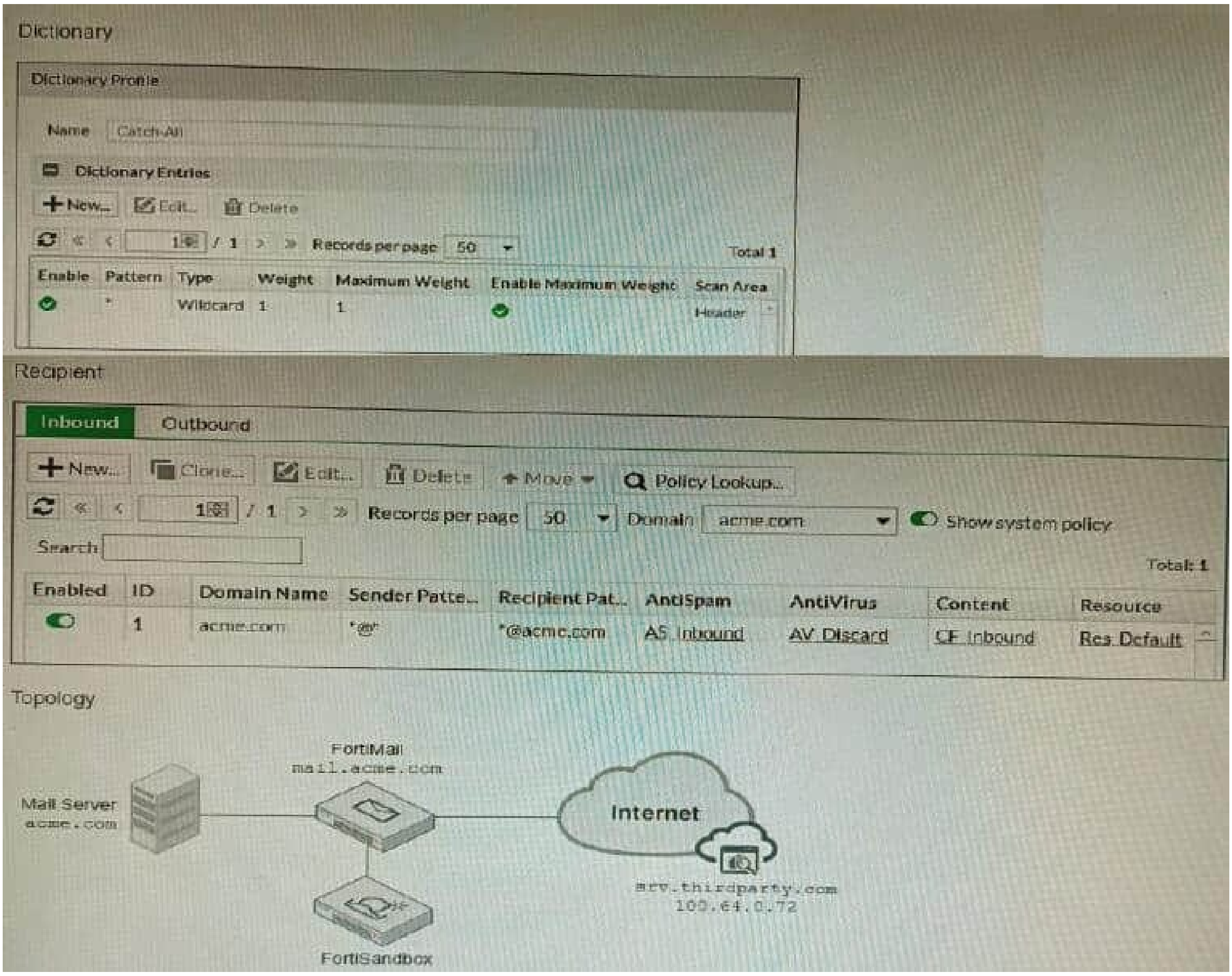
Configuring SSLVPN with Let\\'s Encrypt:

https://docs.fortinet.com/document/fortigate/7.0.0/administration- guide/822087/acme-certificate-support

Let\\'s Encrypt: https://letsencrypt.org/

QUESTION 2

Refer to the exhibits.



Dictionary

Dictionary Profile

Name: Catch-All

Dictionary Entries

Enable	Pattern	Type	Weight	Maximum Weight	Enable Maximum Weight	Scan Area
✓	*	Wildcard	1	1	✓	Header

Records per page: 50 — Total 1

Recipient

Inbound | Outbound

Records per page: 50 — Domain: acme.com — Show system policy

Search:

Total: 1

Enabled	ID	Domain Name	Sender Patte...	Recipient Pat...	AntiSpam	AntiVirus	Content	Resource
●	1	acme.com	*@*	*@acme.com	AS_Inbound	AV_Discard	CF_Inbound	Res_Default

Topology

The exhibits show a FortiMail network topology, Inbound configuration settings, and a Dictionary Profile.

You are required to integrate a third-party\\'s host service (srv.thirdparty.com) into the e-mail processing path.

All inbound e-mails must be processed by FortiMail antispam and antivirus with FortiSandbox integration. If the email is clean, FortiMail must forward it to the third-party service, which will send the email back to FortiMail for final delivery, FortiMail must not scan the e-mail again.

Which three configuration tasks must be performed to meet these requirements? (Choose three.)

A. Change the scan order in FML-GW to antispam-sandbox-content.

B. Apply the Catch-Ail profile to the CFInbound profile and configure a content action profile to deliver to the srv. thirdparty. com FQDN

C. Create an access receive rule with a Sender value of srv. thirdparcy.com, Recipient value of *@acme.com, and action value of Safe

D. Apply the Catch-AII profile to the ASinbound profile and configure an access delivery rule to deliver to the 100.64.0.72 host.

E. Create an IP policy with a Source value of 100. 64 .0.72/32, enable precedence, and place the policy at the top of the list.

Correct Answer: ABE

A is correct because the scan order must be changed to antispam-sandbox- content in order for FortiMail to scan the email for spam and viruses before forwarding it to the third-party service.

B is correct because the Catch-All profile must be applied to the CFInbound profile in order for FortiMail to forward clean emails to the third-party service. E is correct because an IP policy must be created with a Source value of 100.64.0.72/32

in order to allow emails from the third-party service to be delivered to FortiMail.

The other options are not necessary to meet the requirements. Option C is not necessary because the access receive rule will already allow emails from the third-party service to be received by FortiMail. Option D is not necessary because

the Catch-All profile already allows emails to be delivered to any destination. Here are some additional details about integrating a third-party service into the FortiMail email processing path:

The third-party service must be able to receive emails from FortiMail and send them back to FortiMail.

The third-party service must be able to communicate with FortiMail using the SMTP protocol.

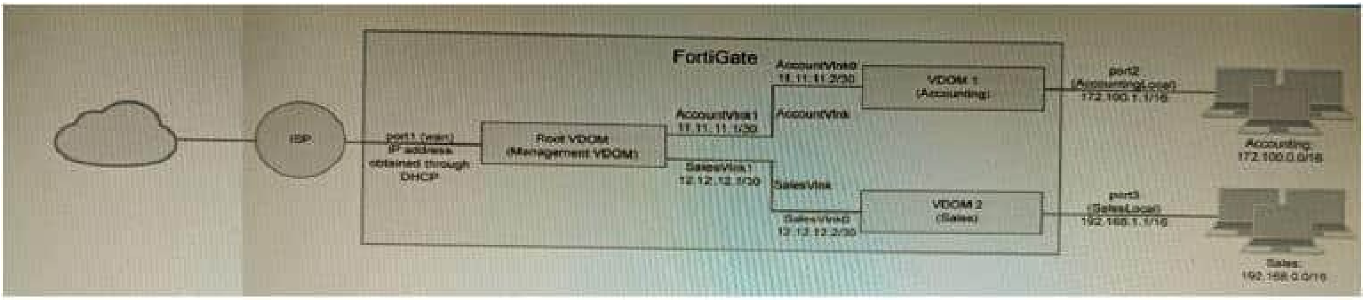
The third-party service must be able to authenticate with FortiMail using the SMTP AUTH protocol.

Once the third-party service is integrated into the FortiMail email processing path, all inbound emails will be processed by FortiMail as usual. If the email is clean, FortiMail will forward it to the third-party service. The third-party service will then

send the email back to FortiMail for final delivery. FortiMail will not scan the email again.

QUESTION 3

Refer to the exhibit.



A customer has deployed a FortiGate 300E with virtual domains (VDOMs) enabled in the multi-VDOM mode. There are three VDOMs: Root is for management and internet access, while VDOM 1 and VDOM 2 are used for segregating internal traffic. AccountVInk and SalesVInk are standard VDOM links in Ethernet mode.

Given the exhibit, which two statements below about VDOM behavior are correct? (Choose two.)

A. You can apply OSPF routing on the VDOM link in either PPP or Ethernet mode

B. Traffic on AccountVInk and SalesVInk will not be accelerated.

C. The VDOM links are in Ethernet mode because they have IP addressed assigned on both sides.

D. Root VDOM is an Admin type VDOM, while VDOM 1 and VDOM 2 are Traffic type VDOMs.

E. OSPF routing can be configured between VDOM 1 and Root VDOM without any configuration changes to AccountVInk

Correct Answer: AD

A. You can apply OSPF routing on the VDOM link in either PPP or Ethernet mode. This is because VDOM links can be configured in either PPP or Ethernet mode, and OSPF routing can be configured on both types of links. D. Root VDOM is

an Admin type VDOM, while VDOM 1 and VDOM 2 are Traffic type VDOMs. This is because the Root VDOM is the default VDOM, and it is used for management and internet access. VDOM 1 and VDOM 2 are traffic type VDOMs, which are

used for segregating internal traffic.

The other options are not correct.

B. Traffic on AccountVInk and SalesVInk will not be accelerated. This is because VDOM links are not accelerated by default. However, you can configure acceleration on VDOM links if you want.

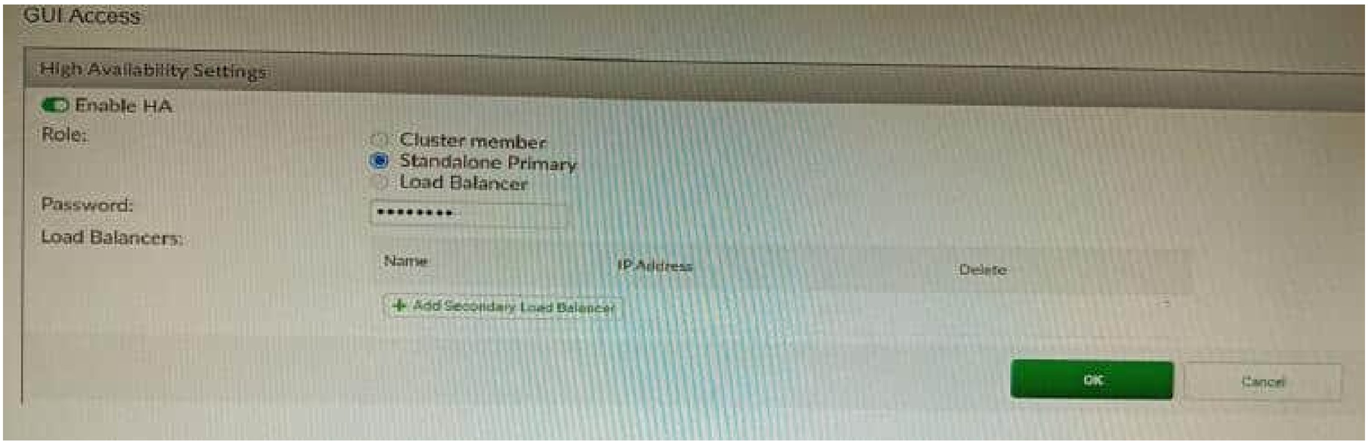
C. The VDOM links are in Ethernet mode because they have IP addressed assigned on both sides. This is not necessarily true. The VDOM links could be in PPP mode even if they have IP addresses assigned on both sides. E. OSPF routing

can be configured between VDOM 1 and Root VDOM without any configuration changes to AccountVInk. This is correct. OSPF routing can be configured between any two VDOMs, even if they are not directly connected. In this case, the

OSPF routing would be configured on the AccountVInk link.

QUESTION 4

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.

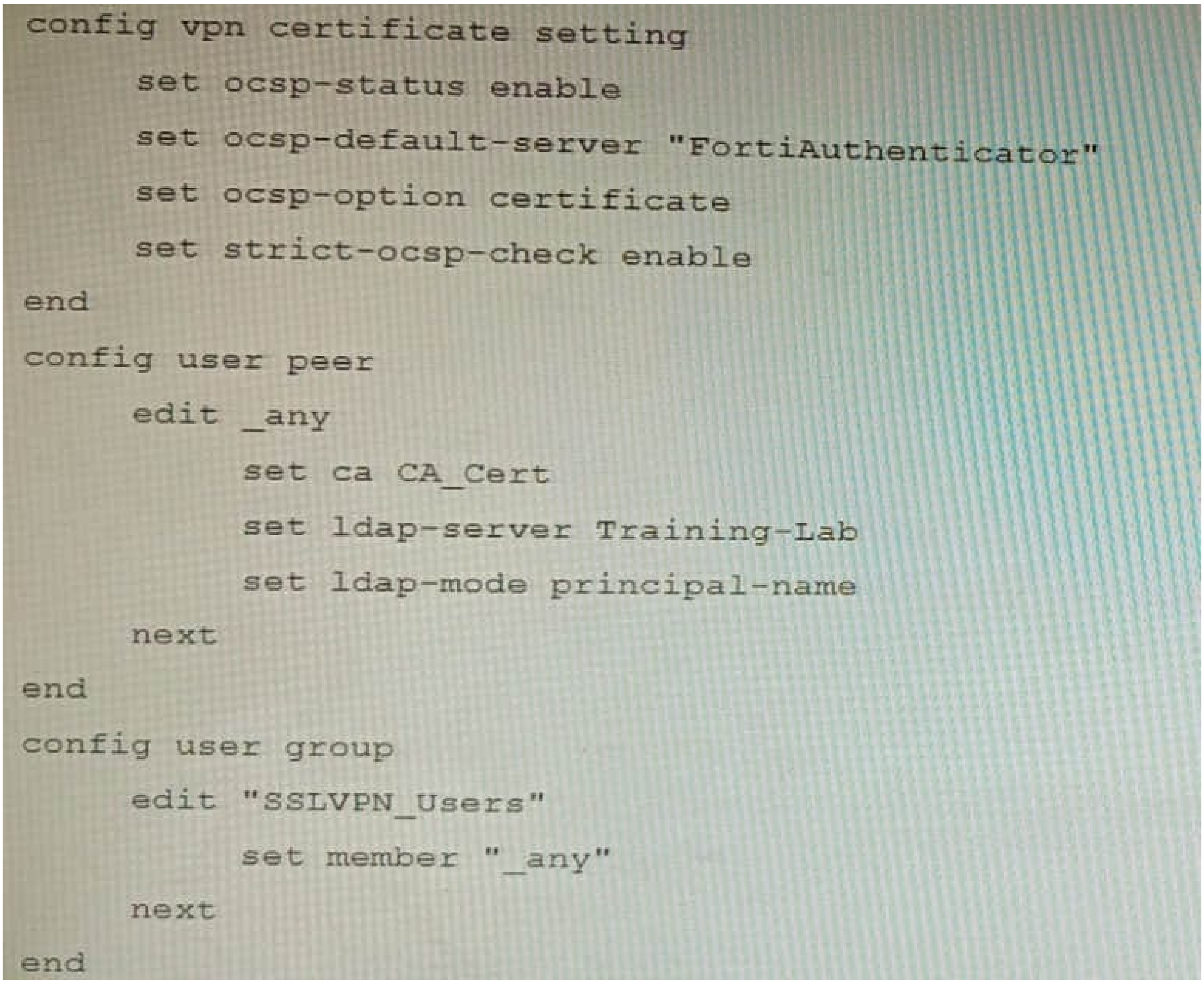
D. FSSO sessions from FAC1 will be synchronized to FAC2.

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 5

An administrator has configured a FortiGate device to authenticate SSL VPN users using digital certificates. A FortiAuthenticator is the certificate authority (CA) and the Online Certificate Status Protocol (OCSP) server. Part of the FortiGate configuration is shown below:



```
config vpn certificate setting
    set ocsp-status enable
    set ocsp-default-server "FortiAuthenticator"
    set ocsp-option certificate
    set strict-ocsp-check enable
end
config user peer
    edit _any
        set ca CA_Cert
        set ldap-server Training-Lab
        set ldap-mode principal-name
    next
end
config user group
    edit "SSLVPN_Users"
        set member "_any"
    next
end
```

Based on this configuration, which two statements are true? (Choose two.)

A. OCSP checks will always go to the configured FortiAuthenticator

B. The OCSP check of the certificate can be combined with a certificate revocation list.

C. OCSP certificate responses are never cached by the FortiGate.

D. If the OCSP server is unreachable, authentication will succeed if the certificate matches the CA.

Correct Answer: BD

B is correct because the OCSP check of the certificate can be combined with a certificate revocation list (CRL). This means that the FortiGate will check the OCSP server to see if the certificate has been revoked, and it will also check the CRL to see if the certificate has been revoked. D is correct because if the OCSP server is unreachable, authentication will succeed if the certificate matches the CA. This is because the FortiGate will fall back to using the CRL if the OCSP server is unreachable. The other options are incorrect. Option A is incorrect because OCSP checks can go to other OCSP servers, not just the FortiAuthenticator. Option C is incorrect because OCSP certificate responses can be cached by the FortiGate. References: Configuring SSL VPN authentication using digital certificates | FortiGate / FortiOS 7.2.0 - Fortinet Document Library Online Certificate Status Protocol (OCSP) | FortiGate / FortiOS 7.2.0 - Fortinet Document Library Certificate Revocation Lists (CRLs) | FortiGate / FortiOS 7.2.0 - Fortinet Document Library