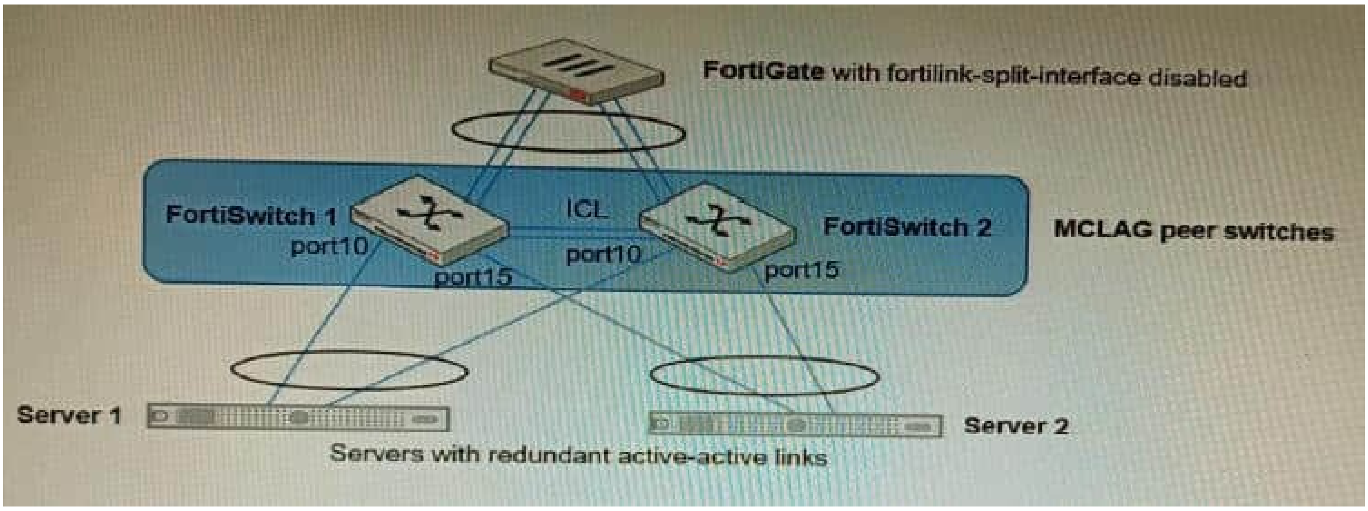
NSE8_812$^{\text{Q\&As}}$

Network Security Expert 8 Written Exam

Pass Fortinet NSE8_812 Exam with 100% Guarantee

QUESTION 1

Refer to the exhibit.


FortiGate with fortilink-split-interface disabled
FortiSwitch 1
port10
port15
ICL
port10
FortiSwitch 2
port15
MCLAG peer switches
Server 1
Server 2
Servers with redundant active-active links

You have been tasked with replacing the managed switch Forti Switch 2 shown in the topology. Which two actions are correct regarding the replacement process? (Choose two.)

A. After replacing the FortiSwitch unit, the automatically created trunk name does not change

B. CLAG-ICL needs to be manually reconfigured once the new switch is connected to the FortiGate

C. After replacing the FortiSwitch unit, the automatically created trunk name changes.

D. MCLAG-ICL will be automatically reconfigured once the new switch is connected to the FortiGate.

Correct Answer: AB

A is correct because the automatically created trunk name is based on the MAC address of the FortiSwitch unit. When the FortiSwitch unit is replaced, the MAC address will change, but the trunk name will not change. B is correct because CLAG-ICL is a manually configured link aggregation group. When the FortiSwitch unit is replaced, the CLAG-ICL configuration will need to be manually reconfigured on the new FortiSwitch unit. The other options are incorrect. Option C is incorrect because the automatically created trunk name does not change when the FortiSwitch unit is replaced. Option D is incorrect because MCLAG-ICL is a manually configured link aggregation group and will not be automatically reconfigured when the FortiSwitch unit is replaced. References: Configuring link aggregation on FortiSwitches | FortiSwitch / FortiOS 7.0.4 - Fortinet Document Library Managing FortiLink | FortiGate / FortiOS 7.0.4 - Fortinet Document Library

QUESTION 2

You are troubleshooting a FortiMail Cloud service integrated with Office 365 where outgoing emails are not reaching the recipients\\' mail What are two possible reasons for this problem? (Choose two.)

A. The FortiMail access control rule to relay from Office 365 servers FQDN is missing.

B. The FortiMail DKIM key was not set using the Auto Generation option.

C. The FortiMail access control rules to relay from Office 365 servers public IPs are missing.

D. A Mail Flow connector from the Exchange Admin Center has not been set properly to the FortiMail Cloud FQDN.

Correct Answer: AD

Explanation: A. The FortiMail access control rule to relay from Office 365 servers FQDN is missing.

If the access control rule to relay from Office 365 servers FQDN is missing, then FortiMail will not be able to send emails to Office 365. This is because the access control rule specifies which IP addresses or domains are allowed to relay

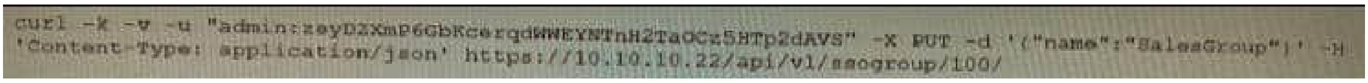
emails through FortiMail. D. A Mail Flow connector from the Exchange Admin Center has not been set properly to the FortiMail Cloud FQDN.

If the Mail Flow connector from the Exchange Admin Center is not set properly to the FortiMail Cloud FQDN, then Office 365 will not be able to send emails to FortiMail. This is because the Mail Flow connector specifies which SMTP server is

used to send emails to external recipients.

QUESTION 3

A customer wants to use the FortiAuthenticator REST API to retrieve an SSO group called SalesGroup. The following API call is being made with the \\'curl\\' utility:



```
curl -k -v -u "admin:zeyD2XmP6GbKcerqdWWEYNTnH2TaOCz5HTp2dAVS" -X PUT -d '{"name":"SalesGroup"}' -H
'Content-Type: application/json' https://10.10.10.22/api/v1/ssogroup/100/
```

Which two statements correctly describe the expected behavior of the FortiAuthenticator REST API? (Choose two.)

A. Only users with the "Full permission" role can access the REST API

B. This API call will fail because it requires that API version 2

C. If the REST API web service access key is lost, it cannot be retrieved and must be changed.

D. The syntax is incorrect because the API calls needs the get method.

Correct Answer: BD

Explanation: To retrieve an SSO group called SalesGroup using the FortiAuthenticator REST API, the following issues need to be fixed in the API call:

The API version should be v2, not v1, as SSO groups are only supported in version 2 of the REST API.

The HTTP method should be GET, not POST, as GET is used to retrieve information from the server, while POST is used to create or update information on the server. Therefore, a correct API call would look like this: curl -X GET -H

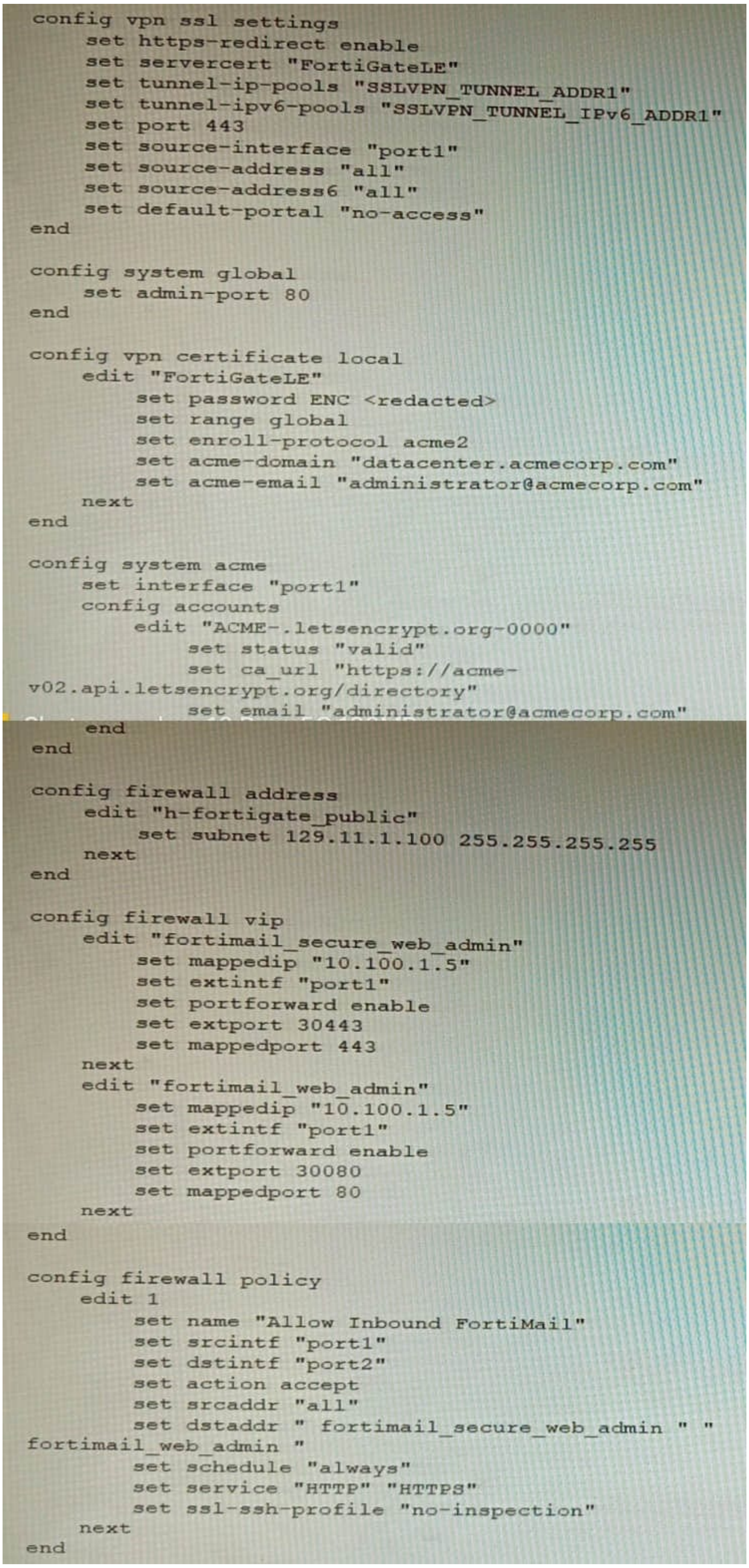
"Authorization: Bearer "

https://fac.example.com/api/v2/sso/groups/SalesGroup
References:https://docs.fortinet.com/document/fortiauthenticator/6.4.1/rest-api- solution-guide/927310/introduction

https://docs.fortinet.com/document/fortiauthenticator/6.4.1/rest-api-solution- guide/927311/sso-groups

QUESTION 4

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

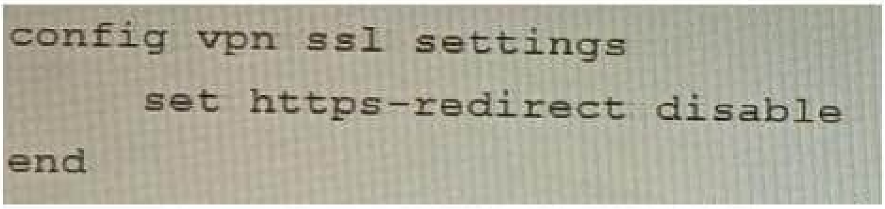


```
config vpn ssl settings
    set https-redirect enable
    set servercert "FortiGateLE"
    set tunnel-ip-pools "SSLVPN_TUNNEL_ADDR1"
    set tunnel-ipv6-pools "SSLVPN_TUNNEL_IPv6_ADDR1"
    set port 443
    set source-interface "port1"
    set source-address "all"
    set source-address6 "all"
    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.

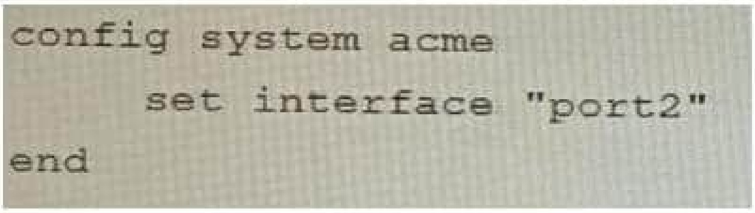
Reviewing the requirement and the exhibit, which configuration change below will resolve this issue?

○ A.



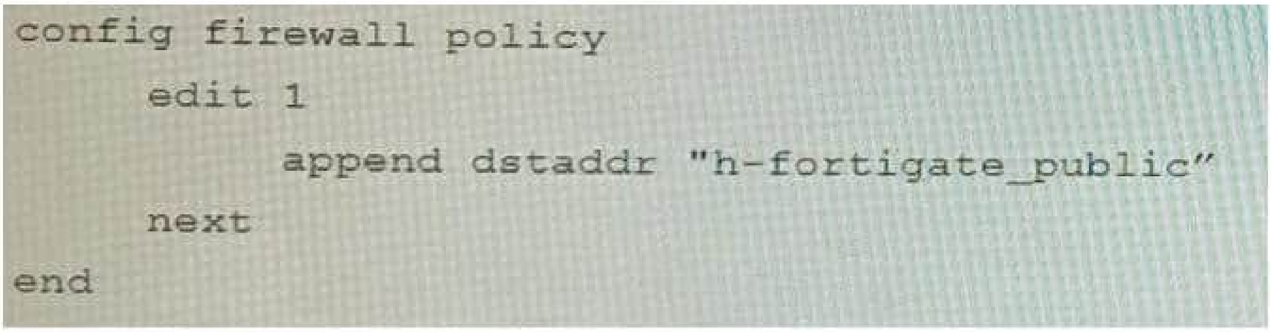
```
config vpn ssl settings
    set https-redirect disable
end
```

○ B.



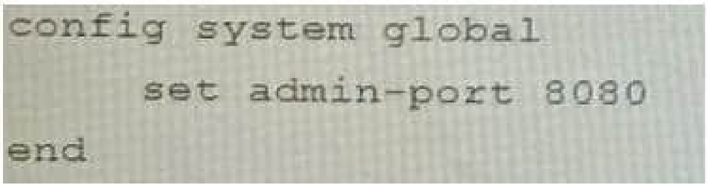
```
config system acme
    set interface "port2"
end
```

○ 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 5

Refer to the exhibit.

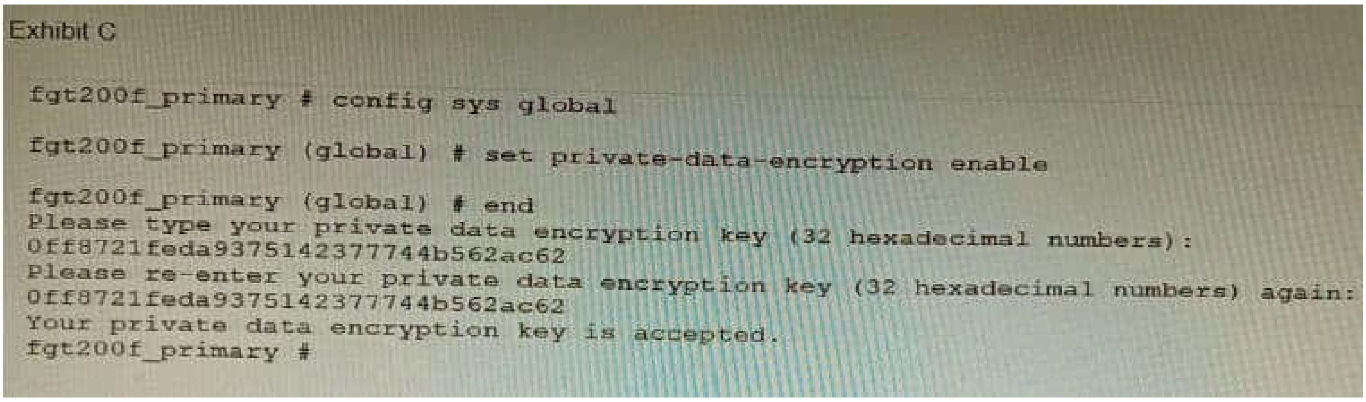


Exhibit C

```
fgt200f_primary # config sys global

fgt200f_primary (global) # set private-data-encryption enable

fgt200f_primary (global) # end
Please type your private data encryption key (32 hexadecimal numbers):
0ff8721feda93751423777744b562ac62
Please re-enter your private data encryption key (32 hexadecimal numbers) again:
0ff8721feda93751423777744b562ac62
Your private data encryption key is accepted.
fgt200f_primary #
```

A customer has deployed a FortiGate 200F high-availability (HA) cluster that contains and TPM chip. The exhibit shows output from the FortiGate CLI session where the administrator enabled TPM.

Following these actions, the administrator immediately notices that both FortiGate high availability (HA) status and FortiManager status for the FortiGate are negatively impacted.

What are the two reasons for this behavior? (Choose two.)

A. The private-data-encryption key entered on the primary did not match the value that the TPM expected.

B. Configuration for TPM is not synchronized between FortiGate HA cluster members.

C. The FortiGate has not finished the auto-update process to synchronize the new configuration to FortiManager yet.

D. TPM functionality is not yet compatible with FortiGate HA D The administrator needs to manually enter the hex private data encryption key in FortiManager

Correct Answer: AB

Explanation: The two reasons for the negative impact on the FortiGate HA status and FortiManager status after enabling TPM are: The private-data-encryption key entered on the primary unit did not match the value that the TPM expected. This could happen if the TPM was previously enabled and then disabled, and the key was changed in between. The

TPM will reject the new key and cause an error in the configuration synchronization. Configuration for TPM is not synchronized between FortiGate HA cluster members. Each cluster member must have the same private-data-encryption key to form a valid HA cluster and synchronize their configurations. However, enabling TPM on one unit does not automatically enable it on the other units, and the key must be manually entered on each unit. To resolve these issues, the administrator should disable TPM on all units, clear the TPM data, and then enable TPM again with the same private-data-encryption key on each unit. References:
https://docs.fortinet.com/document/fortigate/6.4.0/cookbook/103437/inbound-ssl- inspection
https://docs.fortinet.com/document/fortigate/6.4.0/cookbook/103438/application- detection-on-ssl-offloaded-traffic