NSE8_812 Q&As

Network Security Expert 8 Written Exam

Pass Fortinet NSE8_812 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/nse8_812.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

On a FortiGate Configured in Transparent mode, which configuration option allows you to control Multicast traffic passing through the?

A.
```
config system settings
    set multicast-skip-policy disable
end
```

B.
```
config system settings
    set multicast-forward enable
end
```

C.
```
config system settings
    set multicast-forward disable
end
```

D.
```
config system settings
    set multicast-skip-policy enable
end
```

A. Option A

B. Option B

C. Option C

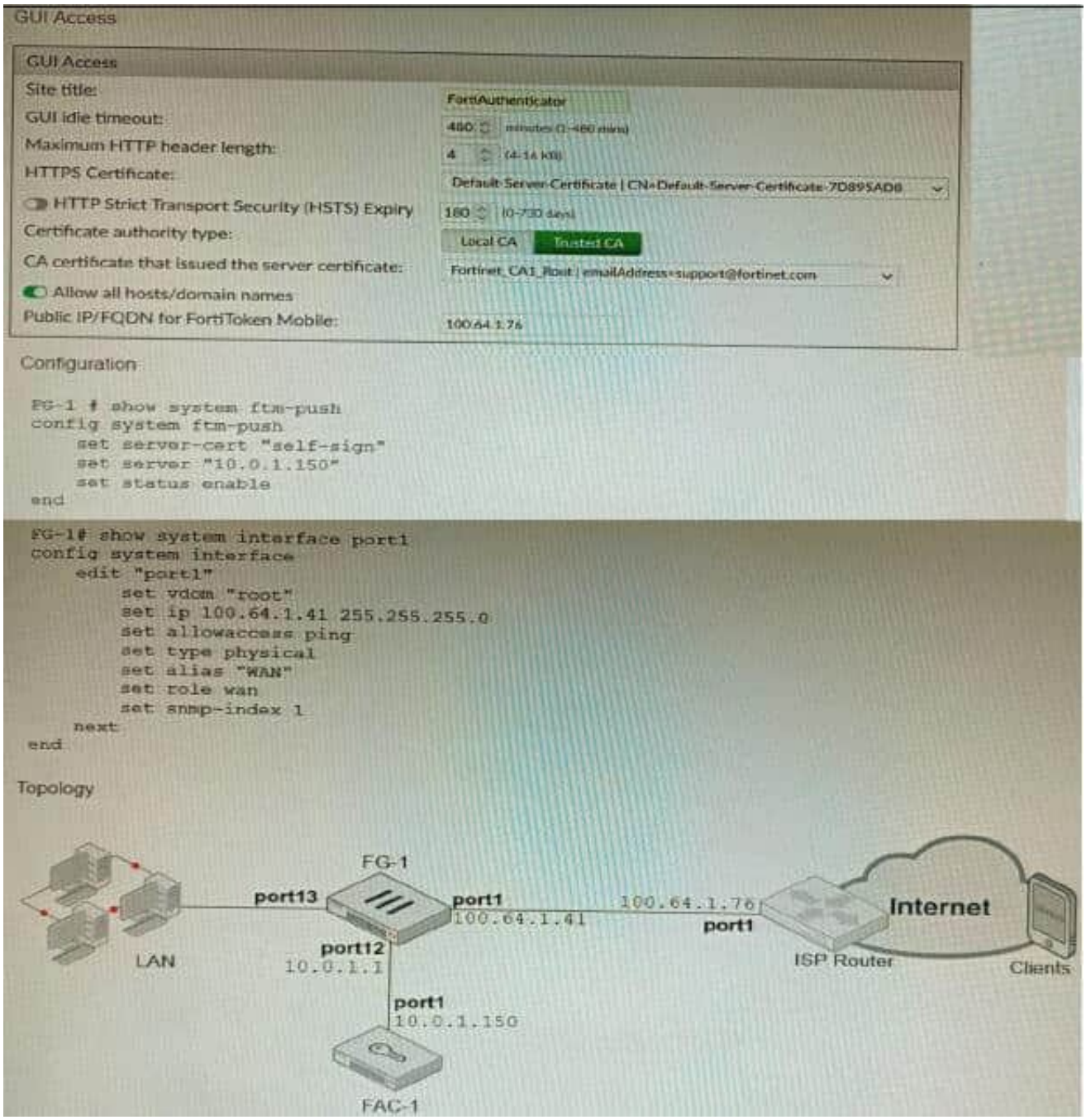
D. Option D

Correct Answer: C

Explanation: To control multicast traffic passing through a FortiGate configured in transparent mode, you can use multicast policies. Multicast policies allow you to filter multicast traffic based on source and destination addresses, protocols, and interfaces. You can also apply securityprofiles to scan multicast traffic for threats and violations. References:https://docs.fortinet.com/document/fortigate/6.2.14/cookbook/968606/configurin g-multicast-forwarding

QUESTION 2

Refer to the exhibits.



An administrator has configured a FortiGate and Forti Authenticator for two-factor authentication with FortiToken push notifications for their SSL VPN login. Upon initial review of the setup, the administrator has discovered that the customers can manually type in their two-factor code and authenticate but push notifications do not work

Based on the information given in the exhibits, what must be done to fix this?

A. On FG-1 port1, the ftm access protocol must be enabled.

B. FAC-1 must have an internet routable IP address for push notifications.

C. On FG-1 CLI, the ftm-push server setting must point to 100.64.141.

D. On FAC-1, the FortiToken public IP setting must point to 100.64.1 41

Correct Answer: B

Explanation: FortiToken push notifications require that the FortiAuthenticator has an internet routable IP address. This is because the FortiAuthenticator uses this IP address to send push notifications to the FortiGate.

The other options are not correct. Enabling the ftm access protocol on FG-1 port1 is not necessary for push notifications to work. The ftm-push server setting on FG-1 CLI should already point to the FortiAuthenticator\\'s IP address. The

FortiToken public IP setting on FAC-1 is not relevant to push notifications.

Here is a table that summarizes the different options:

Option	Description
Enable the ftm access protocol on FG-1 port1	Not necessary for push notifications to work.
Set the ftm-push server setting on FG-1 CLI to the FortiAuthenticator's IP address	Already done.
Set the FortiToken public IP setting on FAC-1 to 100.64.141	Not relevant to push notifications.
Set the FortiAuthenticator's IP address to an internet routable IP address	Necessary for push notifications to work.

QUESTION 3

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 4

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

QUESTION 5

Refer to the exhibit.

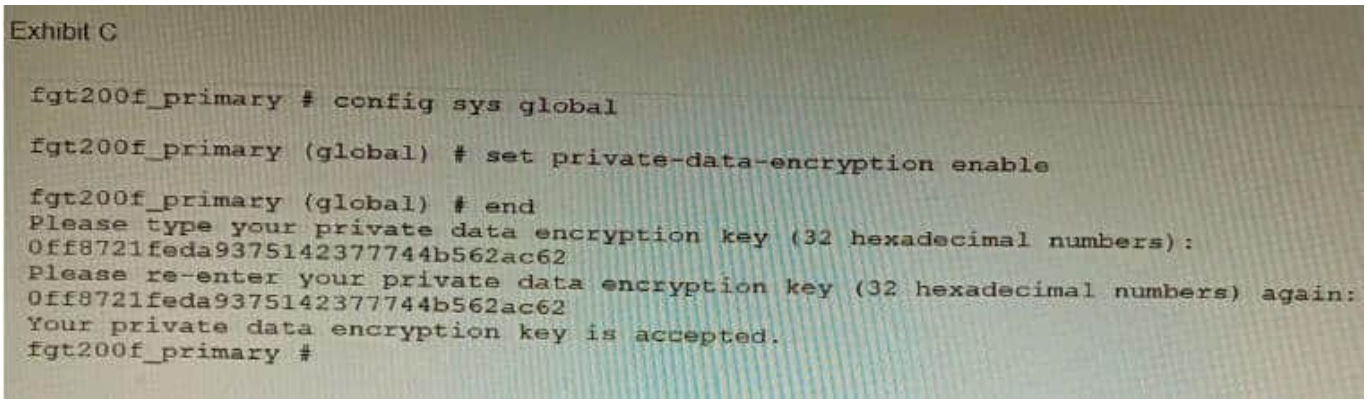


Exhibit C

```
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