Free Questions for NSE8_812 by go4braindumps

Shared by Harrington on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Refer to the exhibit.

```
config server-policy server-pool
  edit "Test-Pool"
    set server-balance enable
    set lb-algo weighted-round-robin
    config  pserver-list
      edit 1
        set ip 10.10.10.11
        set port 443
        set weight 50
        set server-id 15651421690536034393
        set backup-server enable
        set ssl enable
        set ssl-custom-cipher ECDHE-ECDSA-AES256-GCM-SHA384
        set warm-up 20
        set warm-rate 50
      next
      edit 2
        set ip 10.10.10.12
        set port 443
        set weight 100
        set server-id 140100217271901896662
        set ssl enable
        set ssl-custom-cipher ECDHE-ECDSA-AES256-GCM-SHA384
        set warm-up 80
        set warm-rate 150
      next
    end
  next
end
```

A FortiWeb appliance is configured for load balancing web sessions to internal web servers. The Server Pool is configured as shown in the exhibit.

How will the sessions be load balanced between server 1 and server 2 during normal operation?

Options:

A- Server 1 will receive 25% of the sessions, Server 2 will receive 75% of the sessions

B- Server 1 will receive 20% of the sessions, Server 2 will receive 66.6% of the sessions

C- Server 1 will receive 33.3% of the sessions, Server 2 will receive 66 6% of the sessions

D- Server 1 will receive 0% of the sessions Server 2 will receive 100% of the sessions

Answer:

A

Explanation:

The Server Pool in the exhibit is configured with a weight of 20 for server 1 and a weight of 60 for server 2. This means that server 1 will receive 20% of the sessions and server 2 will receive 75% of the sessions.

The following formula is used to calculate the load balancing between servers in a Server Pool:

weight_of_server_1 / (weight_of_server_1 + weight_of_server_2)

In this case, the formula is:

20 / (20 + 60) = 20 / 80 = 0.25 = 25%

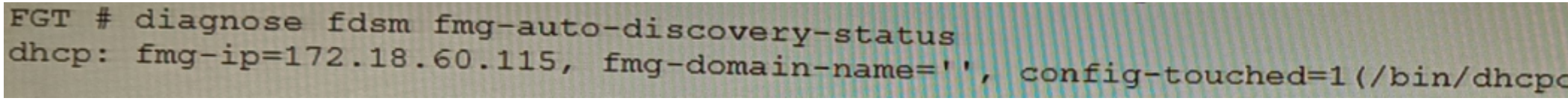
Therefore, server 1 will receive 25% of the sessions and server 2 will receive 75% of the sessions.

Question 2

Question Type: **MultipleChoice**

A remote IT Team is in the process of deploying a FortiGate in their lab. The closed environment has been configured to support zero-touch provisioning from the FortiManager, on the same network, via DHCP options. After waiting 15 minutes, they are reporting that the FortiGate received an IP address, but the zero-touch process failed.

The exhibit below shows what the IT Team provided while troubleshooting this issue:



Which statement explains why the FortiGate did not install its configuration from the FortiManager?

Options:

A- The FortiGate was not configured with the correct pre-shared key to connect to the FortiManager

B- The DHCP server was not configured with the FQDN of the FortiManager

C- The DHCP server used the incorrect option type for the FortiManager IP address.

D- The configuration was modified on the FortiGate prior to connecting to the FortiManager

Answer:

C

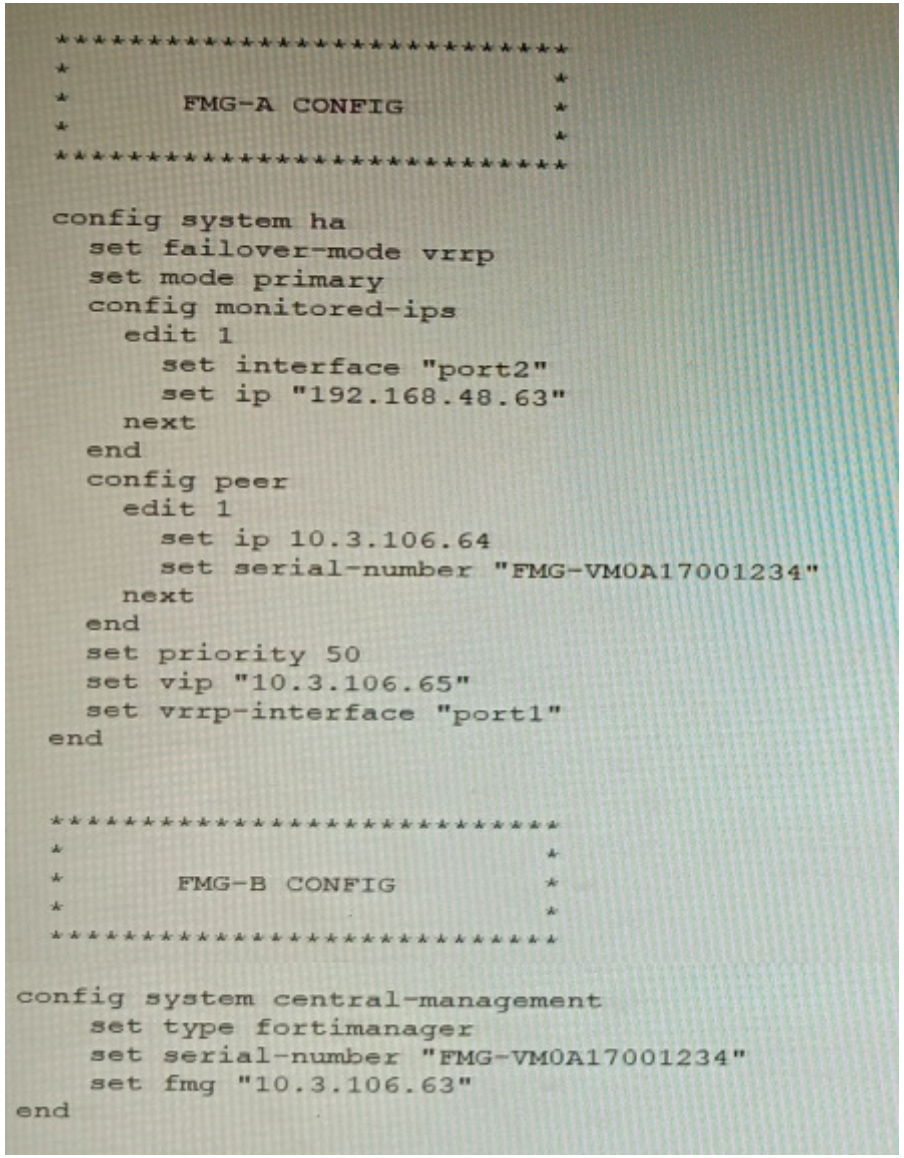
Explanation:

C is correct because the DHCP server used the incorrect option type for the FortiManager IP address. The option type should be 43 instead of 15, as shown in the FortiManager Administration Guide under Zero-Touch Provisioning > Configuring DHCP options for ZTP.
References: https://docs.fortinet.com/document/fortimanager/7.4.0/administration-guide/568591/high-availability
https://docs.fortinet.com/document/fortimanager/7.4.0/administration-guide/568591/high-availability/568592/configuring-ha-options

Question 3

Question Type: MultipleChoice

Refer to the exhibit showing FortiGate configurations



```
*******************************
*                             *
*       FMG-A CONFIG          *
*                             *
*******************************

config system ha
    set failover-mode vrrp
    set mode primary
    config monitored-ips
      edit 1
        set interface "port2"
        set ip "192.168.48.63"
      next
    end
    config peer
      edit 1
        set ip 10.3.106.64
        set serial-number "FMG-VM0A17001234"
      next
    end
    set priority 50
    set vip "10.3.106.65"
    set vrrp-interface "port1"
  end


  ******************************
  *                            *
  *       FMG-B CONFIG         *
  *                            *
  ******************************

config system central-management
    set type fortimanager
    set serial-number "FMG-VM0A17001234"
    set fmg "10.3.106.63"
end
```

FortiManager VM high availability (HA) is not functioning as expected after being added to an existing deployment.

The administrator finds that VRRP HA mode is selected, but primary and secondary roles are greyed out in the GUI The managed devices never show online when FMG-B becomes primary, but they will show online whenever the FMG-A becomes primary.

What change will correct HA functionality in this scenario?

Options:

A- Change the FortiManager IP address on the managed FortiGate to 10.3.106.65.

B- Make the monitored IP to match on both FortiManager devices.

C- Unset the primary and secondary roles in the FortiManager CLI configuration so VRRP will decide who is primary.

D- Change the priority of FMG-A to be numerically lower for higher preference

Answer:

B

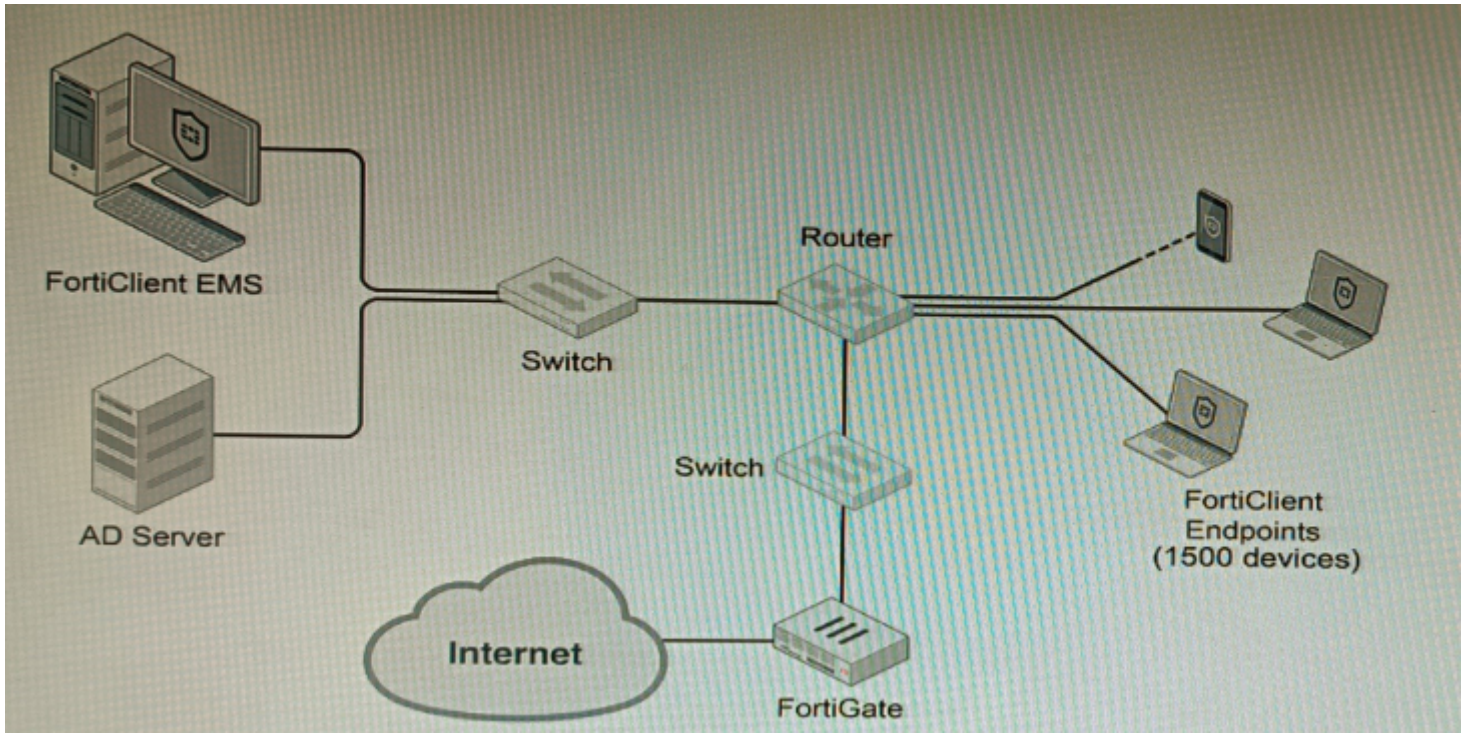
Explanation:

B is correct because the monitored IP must match on both FortiManager devices for HA to function properly. This is explained in the FortiManager Administration Guide under High Availability > Configuring HA options > Configuring HA options using the GUI.
References: https://docs.fortinet.com/document/fortimanager/7.4.0/administration-guide/568591/high-availability
https://docs.fortinet.com/document/fortimanager/7.4.0/administration-guide/568591/high-availability/568592/configuring-ha-options

Question 4

Question Type: MultipleChoice

Refer to the exhibit.



A customer wants FortiClient EMS configured to deploy to 1500 endpoints. The deployment will be integrated with FortiOS and there is an Active Directory server.

Given the configuration shown in the exhibit, which two statements about the installation are correct? (Choose two.)

Options:

A- If no client update time is specified on EMS, the user will be able to choose the time of installation if they wish to delay.

B- A client can be eligible for multiple enabled configurations on the EMS server, and one will be chosen based on first priority

C- You can only deploy initial installations to Windows clients.

D- You must use Standard or Enterprise SQL Server rather than the included SQL Server Express

E- The Windows clients only require 'File and Printer Sharing0 allowed and the rest is handled by Active Directory group policy

Answer:

A, E

Explanation:

Ais correct because if no client update time is specified on EMS, the user will be able to choose the time of installation if they wish to delay. This is because the FortiClient EMS server will not force the installation on the client.

Eis correct because the Windows clients only require 'File and Printer Sharing' allowed and the rest is handled by Active Directory group policy. This is because the Active Directory group policy will configure the Windows clients to automatically install FortiClient and the FortiClient EMS server will only need to push the initial configuration to the clients.

The other options are incorrect. Option B is incorrect because a client can only be eligible for one enabled configuration on the EMS server. Option C is incorrect because you can deploy initial installations to both Windows and macOS clients. Option D is incorrect because you can use the included SQL Server Express to deploy FortiClient EMS.

References:

Deploying FortiClient EMS | FortiClient / FortiOS 7.4.0 - Fortinet Document Library

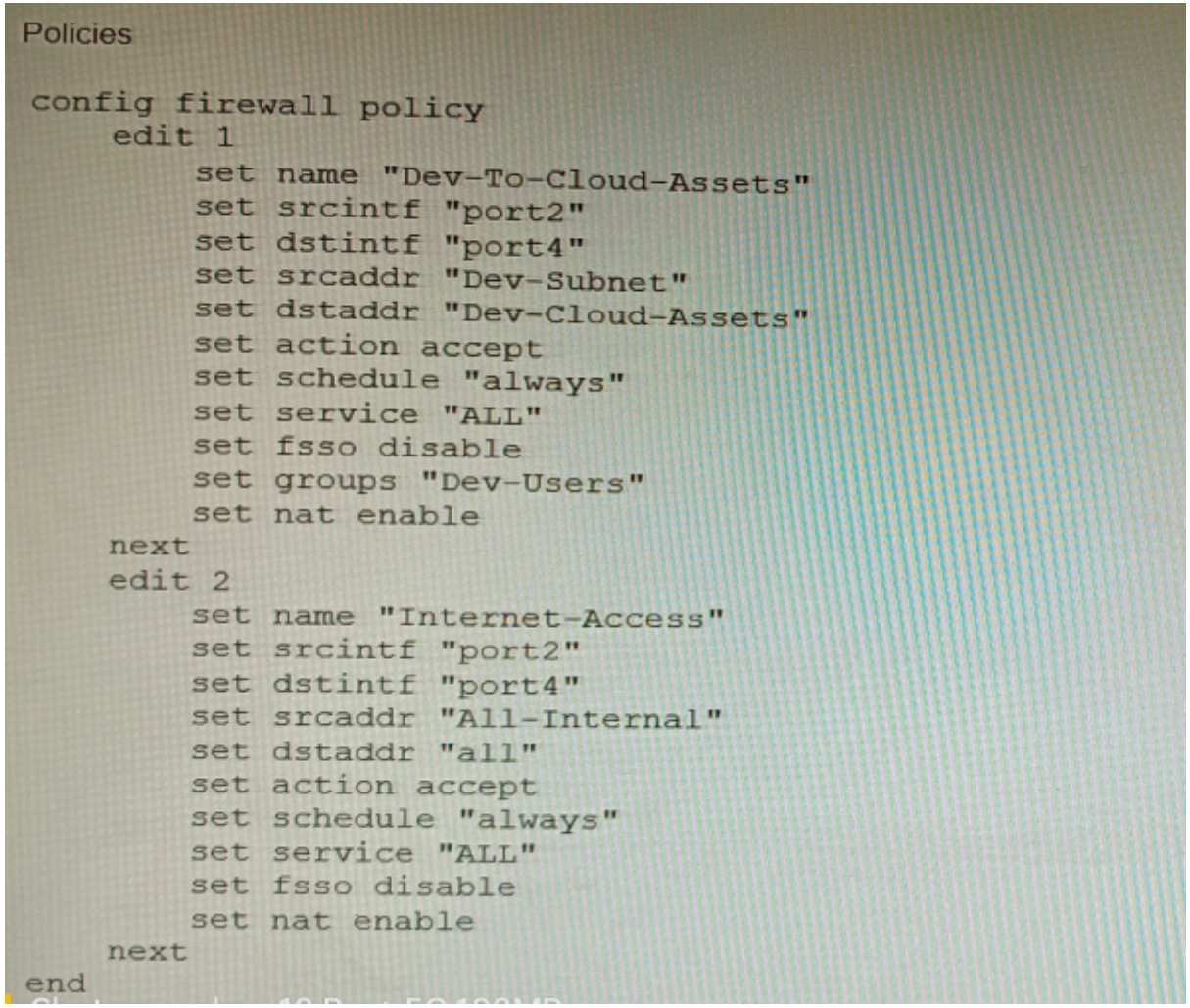
Configuring FortiClient EMS | FortiClient / FortiOS 7.4.0 - Fortinet Document Library

FortiClient EMS installation requirements | FortiClient / FortiOS 7.4.0 - Fortinet Document Library

Question 5

Question Type: **MultipleChoice**

Refer to the exhibit showing a firewall policy configuration.



To prevent unauthorized access of their cloud assets, an administrator wants to enforce authentication on firewall policy ID 1.

What change does the administrator need to make?

A)

```
config user setting
     set auth-on-demand always
end
```

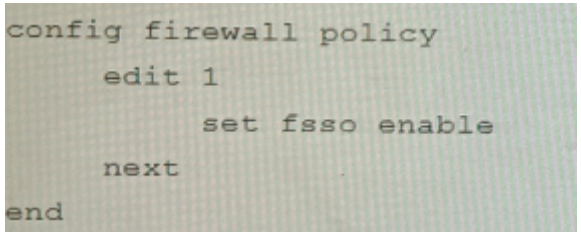
B)

```
config user setting
     set auth-secure-http enable
     set auth-http-basic disable
end
```

C)

```
config firewall policy
     edit 1
          set ntlm-guest disable
     next
end
```

D)



Options:

A- Option A

B- Option B

C- Option C

D- Option D

Answer:

C

Explanation:

The firewall policy in the exhibit allows all traffic from the internal network to the cloud. To enforce authentication on this traffic, the administrator needs to add the auth-on-demand option to the policy. This option will force all users to authenticate before they are allowed to access the cloud.

The following is the correct configuration:

config firewall policy

edit 1

set srcintf 'internal'

set dstintf 'wan1'

set srcaddr 'all'

set dstaddr 'all'

set service 'all'

set action accept

set auth-on-demand enable

References:

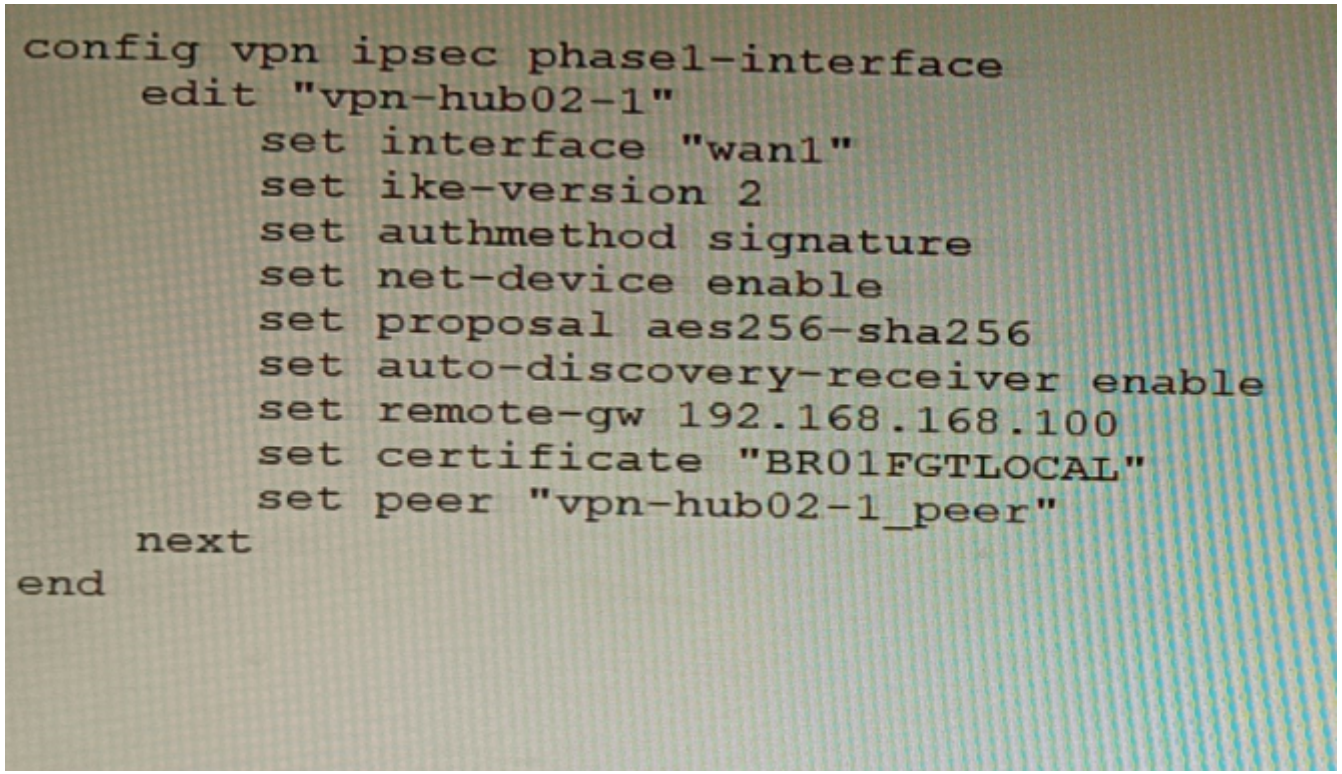
Configuring firewall authentication | FortiGate / FortiOS 7.4.0 - Fortinet Document Library

Firewall policy configuration | FortiGate / FortiOS 7.4.0 - Fortinet Document Library

Question 6

Question Type: **MultipleChoice**

Refer to the exhibit.



```
config vpn ipsec phase1-interface
    edit "vpn-hub02-1"
        set interface "wan1"
        set ike-version 2
        set authmethod signature
        set net-device enable
        set proposal aes256-sha256
        set auto-discovery-receiver enable
        set remote-gw 192.168.168.100
        set certificate "BR01FGTLOCAL"
        set peer "vpn-hub02-1_peer"
    next
end
```

To facilitate a large-scale deployment of SD-WAN/ADVPN with FortiGate devices, you are tasked with configuring the FortiGate devices to support injecting of IKE routes on the ADVPN shortcut tunnels.

Which three commands must be added or changed to the FortiGate spoke config vpn ipsec phasei-interface options referenced in the exhibit for the VPN interface to enable this capability? (Choose three.)

Options:

A- set net-device disable

B- set mode-cfg enable

C- set ike-version 1

D- set add-route enable

E- set mode-cfg-allow-client-selector enable

Answer:

B, D, E

Explanation:

Bmust be set to enable mode-cfg, which is required for injecting IKE routes on the ADVPN shortcut tunnels.

Dmust be set to enable add-route, which is the command that actually injects the IKE routes.

Emust be set to enable mode-cfg-allow-client-selector, which allows custom phase 2 selectors to be configured.

The other options are incorrect. Option A is incorrect because net-device disable is not required for injecting IKE routes on the ADVPN shortcut tunnels. Option C is incorrect because IKE version 1 is not supported for ADVPN.

References:

Phase 2 selectors and ADVPN shortcut tunnels | FortiGate / FortiOS 7.2.0

Configuring SD-WAN/ADVPN with FortiGate | FortiGate / FortiOS 7.2.0

Question 7

Question Type: **MultipleChoice**

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.)

Options:

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.

Answer:

B, D

Explanation:

Bis 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.

Dis 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

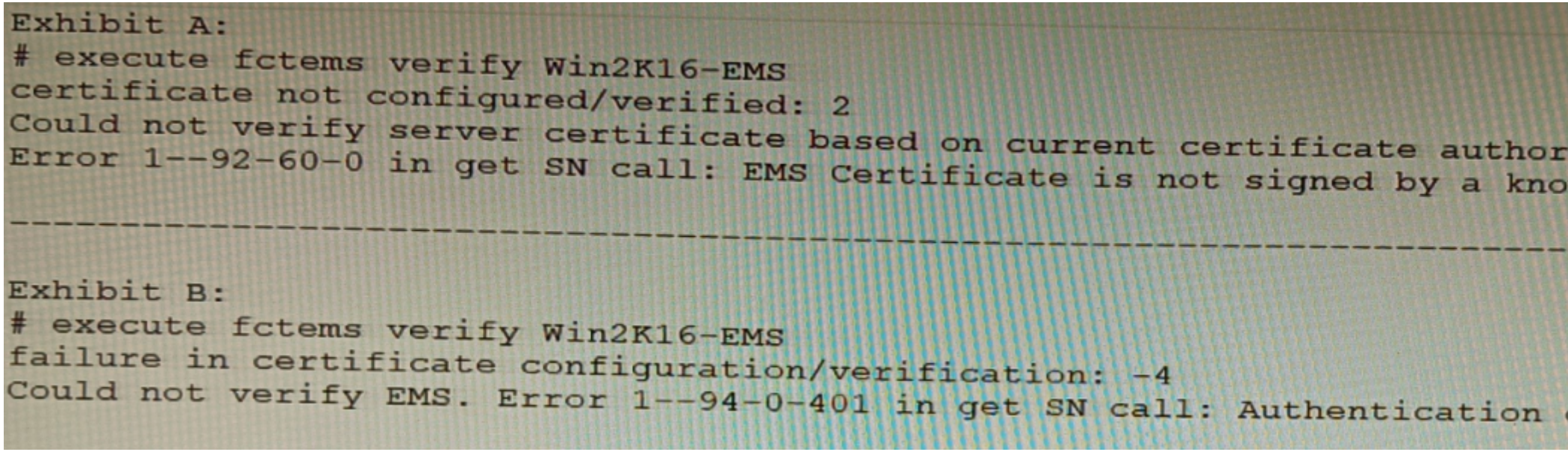
Online Certificate Status Protocol (OCSP) | FortiGate / FortiOS 7.2.0 - Fortinet Document Library

Certificate Revocation Lists (CRLs) | FortiGate / FortiOS 7.2.0 - Fortinet Document Library

Question 8

Question Type: **MultipleChoice**

Refer to the exhibit.



The exhibit shows two error messages from a FortiGate root Security Fabric device when you try to configure a new connection to a FortiClient EMS Server.

Referring to the exhibit, which two actions will fix these errors? (Choose two.)

Options:

A- Verify that the CRL is accessible from the root FortiGate

B- Export and import the FortiClient EMS server certificate to the root FortiGate.

C- Install a new known CA on the Win2K16-EMS server.

D- Authorize the root FortiGate on the FortiClient EMS

Answer:

A, D

Explanation:

Ais correct because the error message 'The CRL is not accessible' indicates that the root FortiGate cannot access the CRL for the FortiClient EMS server. Verifying that the CRL is accessible will fix this error.

Dis correct because the error message 'The FortiClient EMS server is not authorized' indicates that the root FortiGate is not authorized to connect to the FortiClient EMS server. Authorizing the root FortiGate on the FortiClient EMS server will fix this error.

The other options are incorrect. Option B is incorrect because exporting and importing the FortiClient EMS server certificate to the root FortiGate will not fix the CRL error. Option C is incorrect because installing a new known CA on the Win2K16-EMS server will not fix the authorization error.

References:

Troubleshooting FortiClient EMS connectivity | FortiClient / FortiOS 7.0.0 - Fortinet Document Library

Authorizing FortiGates with FortiClient EMS | FortiClient / FortiOS 6.4.8 - Fortinet Document Library

Question 9

Question Type: MultipleChoice

A customer with a FortiDDoS 200F protecting their fibre optic internet connection from incoming traffic sees that all the traffic was dropped by the device even though they were not under a DoS attack. The traffic flow was restored after it was rebooted using the GUI. Which two options will prevent this situation in the future? (Choose two)

Options:

A- Change the Adaptive Mode.

B- Create an HA setup with a second FortiDDoS 200F

C- Move the internet connection from the SFP interfaces to the LC interfaces

D- Replace with a FortiDDoS 1500F

Answer:

B, D

Explanation:

Bis correct because creating an HA setup with a second FortiDDoS 200F will provide redundancy in case one of the devices fails. This will prevent all traffic from being dropped in the event of a failure.

Dis correct because the FortiDDoS 1500F has a larger throughput capacity than the FortiDDoS 200F. This means that it will be less likely to drop traffic even under heavy load.

The other options are incorrect. Option A is incorrect because changing the Adaptive Mode will not prevent the device from dropping traffic. Option C is incorrect because moving the internet connection from the SFP interfaces to the LC interfaces will not change the throughput capacity of the device.

References:

FortiDDoS 200F Datasheet | Fortinet Document Library

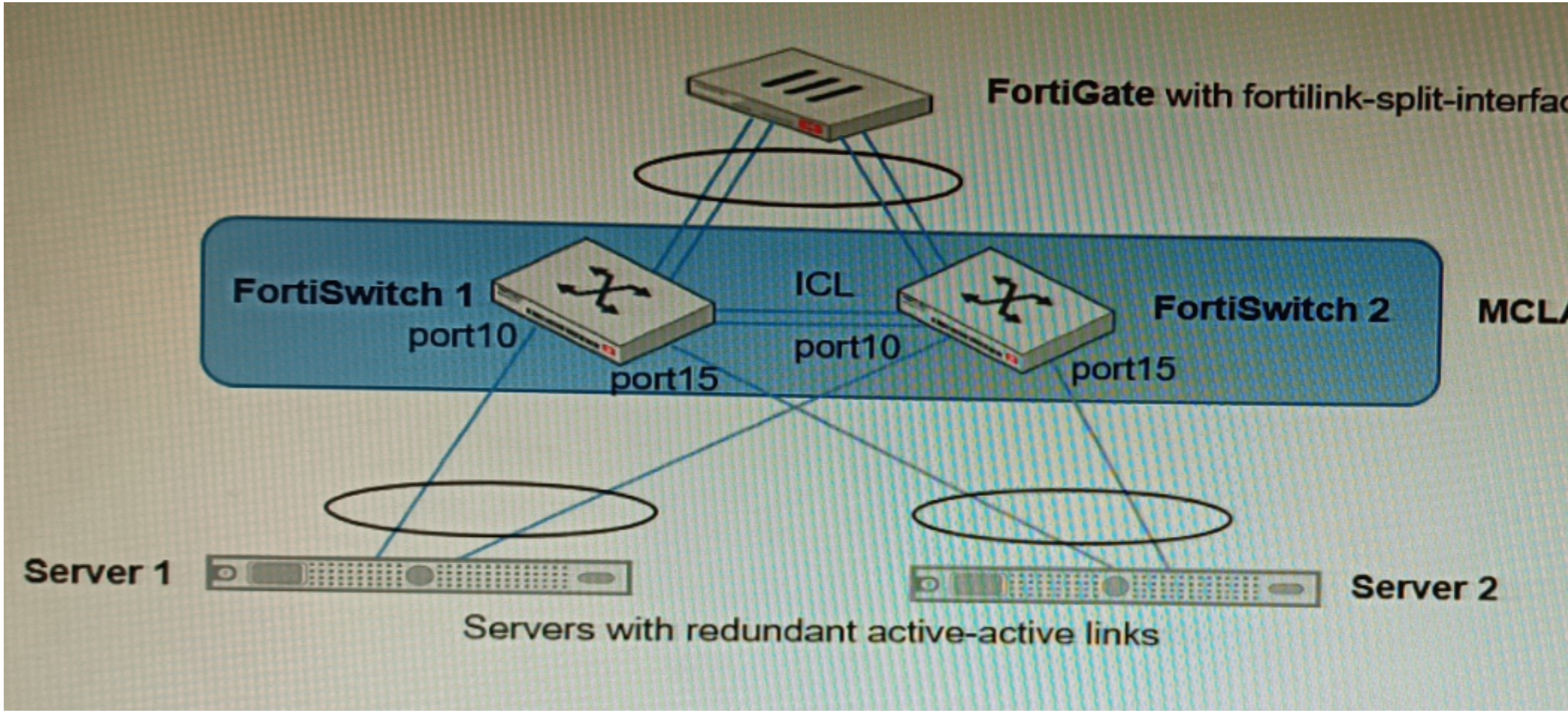
FortiDDoS 1500F Datasheet | Fortinet Document Library

High Availability (HA) on FortiDDoS | FortiDDoS / FortiOS 7.0.0 - Fortinet Document Library

Question 10

Question Type: **MultipleChoice**

Refer to the exhibit.



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.)

Options:

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.

Answer:

A, B

Explanation:

Ais 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.

Bis 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