Free Questions for NSE8_812 by certscare

Shared by Ruiz on 09-08-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Review the VPN configuration shown in the exhibit.

```
config vpn ipsec fec
  edit "fecprofile"
    config mappings
      edit 1
        set base 8
        set redundant 2
        set packet-loss-threshold 10
      next
      edit 2
        set base 9
        set redundant 3
        set bandwidth-up-threshold 450000
      next
      edit 3
        set base 5
        set redundant 3
        bandwidth-bi-threshold 5000000
      next
    end
  next
end

config vpn ipsec phase1-interface
  edit "vd1-p1"
    set fec-health-check "1"
    set fec-mapping-profile "fecprofile"
    set fec-base 10
    set fec-redundant 1
 next
end
```

What is the Forward Error Correction behavior if the SD-WAN network traffic download is 500 Mbps and has 8% of packet loss in the environment?

Options:

A- 1 redundant packet for every 10 base packets

B- 3 redundant packet for every 5 base packets

C- 2 redundant packet for every 8 base packets

D- 3 redundant packet for every 9 base packets

Answer:

C

Explanation:

The FEC configuration in the exhibit specifies that if the packet loss is greater than 10%, then the FEC mapping will be 8 base packets and 2 redundant packets. The download bandwidth of 500 Mbps is not greater than 950 Mbps, so the FEC mapping is not overridden by the bandwidth setting. Therefore, the FEC behavior will be 2 redundant packets for every 8 base packets.

Here is the explanation of the FEC mappings in the exhibit:

Packet loss greater than 10%:8 base packets and 2 redundant packets.

Upload bandwidth greater than 950 Mbps:9 base packets and 3 redundant packets.

The mappings are matched from top to bottom, so the first mapping that matches the conditions will be used. In this case, the first mapping matches because the packet loss is greater than 10%. Therefore, the FEC behavior will be 2 redundant packets for every 8 base packets.

Question 2

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

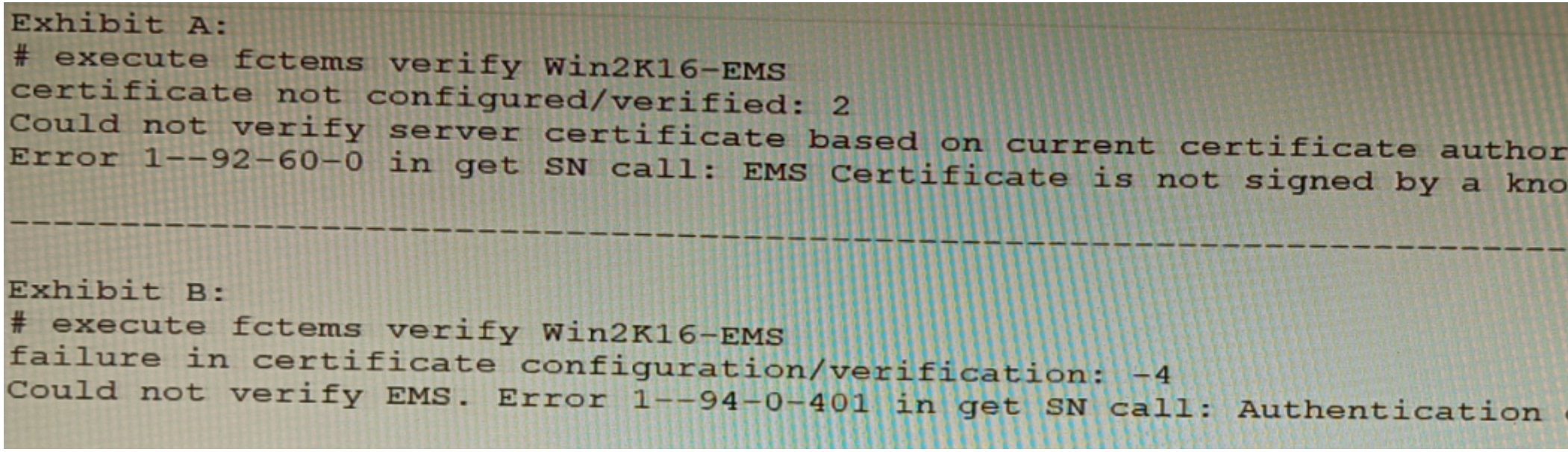
Explanation:

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 3

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:

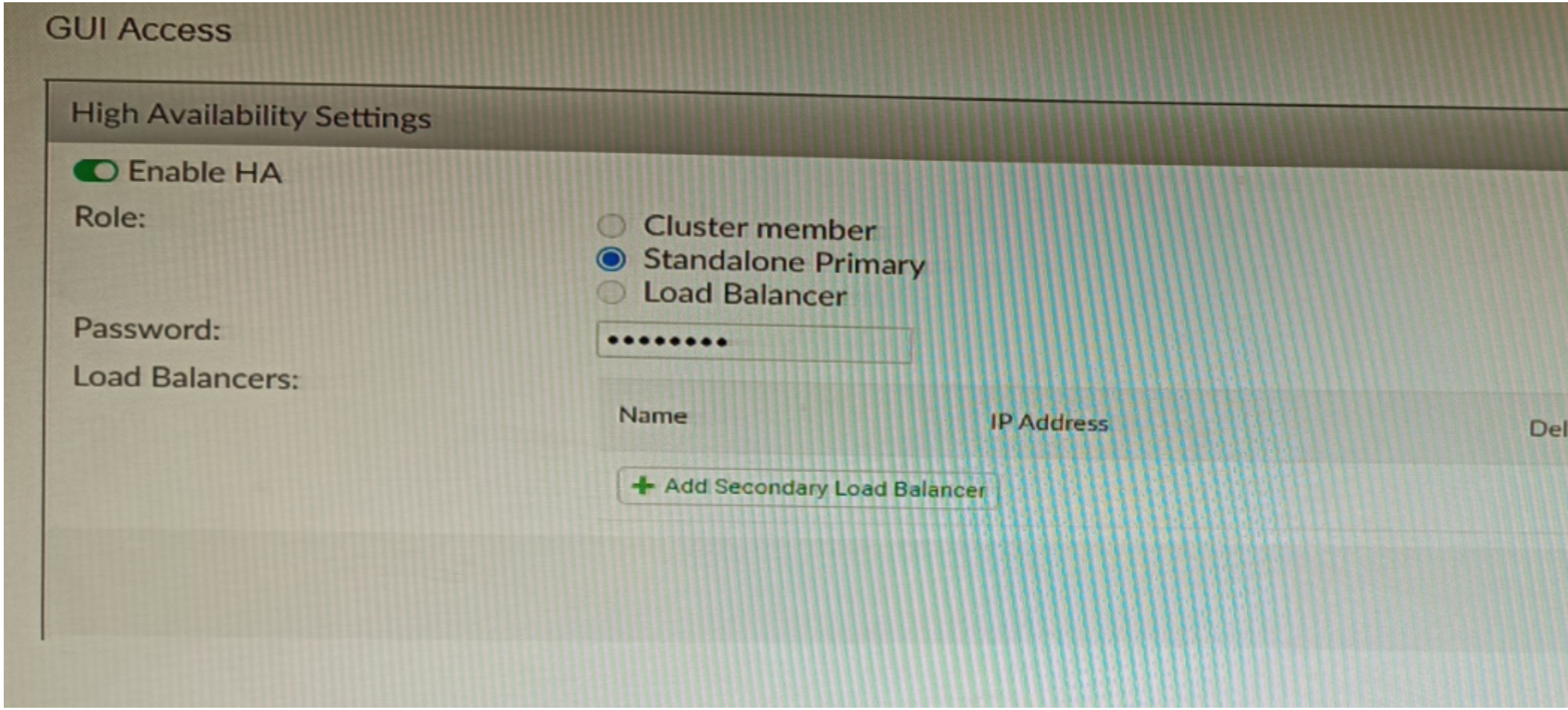
Troubleshooting FortiClient EMS connectivity | FortiClient / FortiOS 7.0.0 - Fortinet Document Library

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

Question 4

Question Type: MultipleChoice

Refer to the exhibit, which shows the high availability configuration for the FortiAuthenticator (FAC1).



Based on this information, which statement is true about the next FortiAuthenticator (FAC2) member that will join an HA cluster with this FortiAuthenticator (FAC1)?

Options:

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.

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

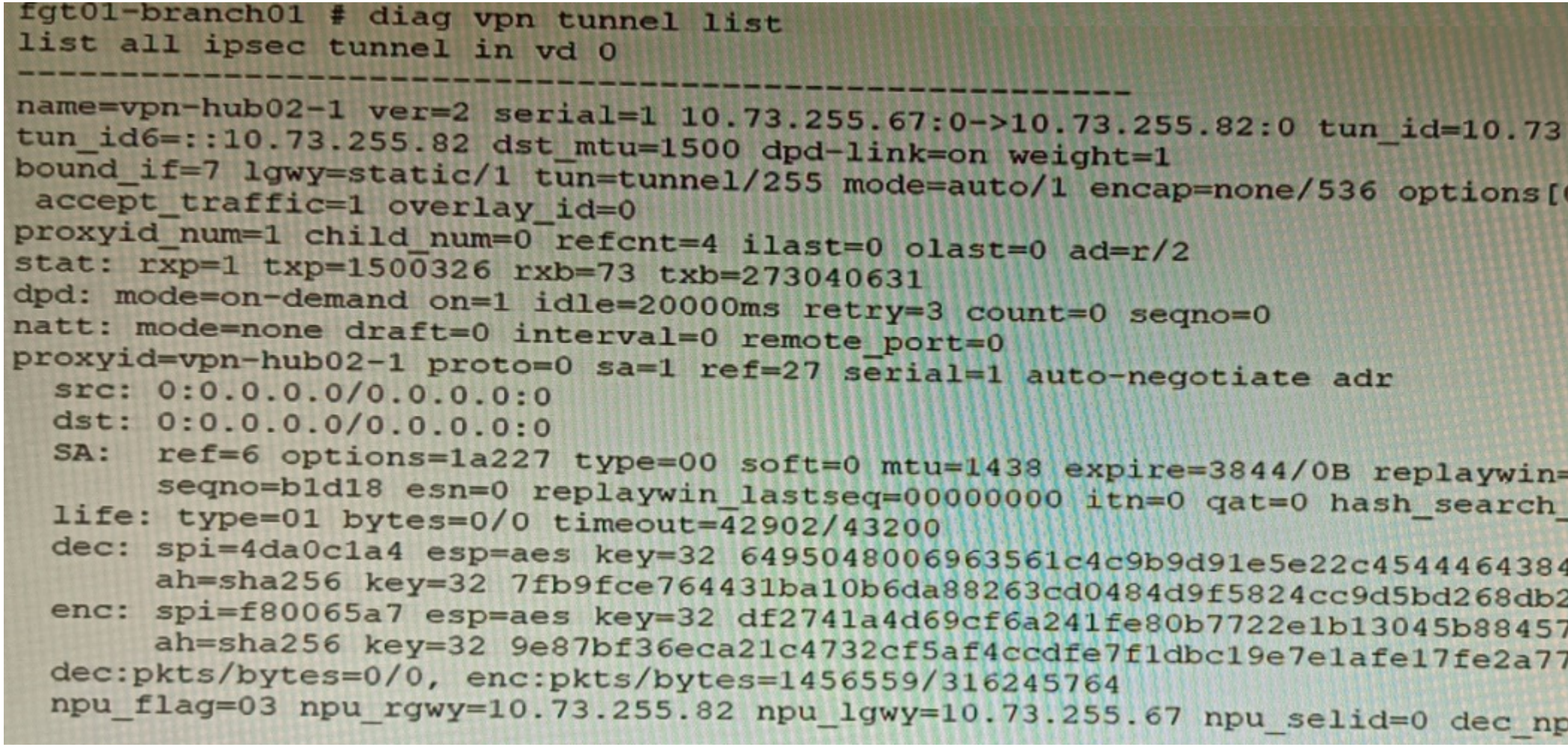
Question Type: MultipleChoice

Refer to the exhibits.

Exhibit A

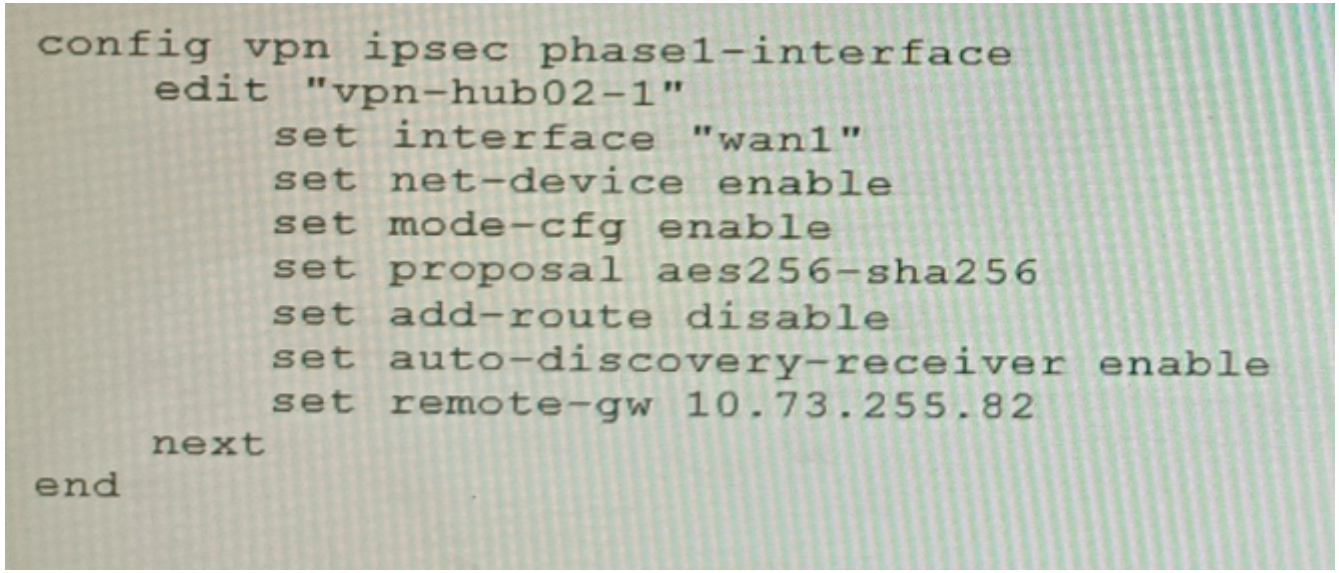
```
vd: root/0
name: vpn-hub02-1
version: 2
interface: wan1 7
addr: 10.73.255.67:500 -> 10.73.255.82:500
tun_id: 10.73.255.82/::10.73.255.82
remote_location: 0.0.0.0
created: 82236s ago
peer-id: CN = fgtdc01.example.com
peer-id-auth: yes
assigned IPv4 address: 192.168.73.67/255.255.255.224
auto-discovery: 2 receiver
PPK: no
IKE SA: created 1/1  established 1/1  time 50/50/50 ms
IPsec SA: created 1/2  established 1/2  time 0/25/50 ms
  id/spi: 1 e4f6465bbae7490f/2535d26ef1f21557
  direction: initiator
  status: established 82236-82236s ago = 50ms
  proposal: aes256-sha256
  child: no
  PPK: no
  message-id sent/recv: 4/1
  lifetime/rekey: 86400/3863
  DPD sent/recv: 00000000/00000000
  peer-id: CN = fgtdc01.example.com
```

Exhibit B



```
fgt01-branch01 # diag vpn tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=vpn-hub02-1 ver=2 serial=1 10.73.255.67:0->10.73.255.82:0 tun_id=10.73
tun_id6=::10.73.255.82 dst_mtu=1500 dpd-link=on weight=1
bound_if=7 lgwy=static/1 tun=tunnel/255 mode=auto/1 encap=none/536 options[
 accept_traffic=1 overlay_id=0
proxyid_num=1 child_num=0 refcnt=4 ilast=0 olast=0 ad=r/2
stat: rxp=1 txp=1500326 rxb=73 txb=273040631
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=vpn-hub02-1 proto=0 sa=1 ref=27 serial=1 auto-negotiate adr
  src: 0:0.0.0.0/0.0.0.0:0
  dst: 0:0.0.0.0/0.0.0.0:0
  SA:  ref=6 options=1a227 type=00 soft=0 mtu=1438 expire=3844/0B replaywin=
       seqno=b1d18 esn=0 replaywin_lastseq=00000000 itn=0 qat=0 hash_search_
  life: type=01 bytes=0/0 timeout=42902/43200
  dec: spi=4da0c1a4 esp=aes key=32 649504800696356lc4c9b9d91e5e22c4544464384
       ah=sha256 key=32 7fb9fce764431ba10b6da88263cd0484d9f5824cc9d5bd268db2
  enc: spi=f80065a7 esp=aes key=32 df2741a4d69cf6a241fe80b7722e1b13045b88457
       ah=sha256 key=32 9e87bf36eca21c4732cf5af4ccdfe7f1dbc19e7e1afe17fe2a77
  dec:pkts/bytes=0/0, enc:pkts/bytes=1456559/316245764
  npu_flag=03 npu_rgwy=10.73.255.82 npu_lgwy=10.73.255.67 npu_selid=0 dec_np
```

Exhibit C



```
config vpn ipsec phase1-interface
    edit "vpn-hub02-1"
        set interface "wan1"
        set net-device enable
        set mode-cfg enable
        set proposal aes256-sha256
        set add-route disable
        set auto-discovery-receiver enable
        set remote-gw 10.73.255.82
    next
end
```

A customer is trying to set up a VPN with a FortiGate, but they do not have a backup of the configuration. Output during a troubleshooting session is shown in the exhibits A and B and a baseline VPN configuration is shown in Exhibit C Referring to the exhibits, which configuration will restore VPN connectivity?

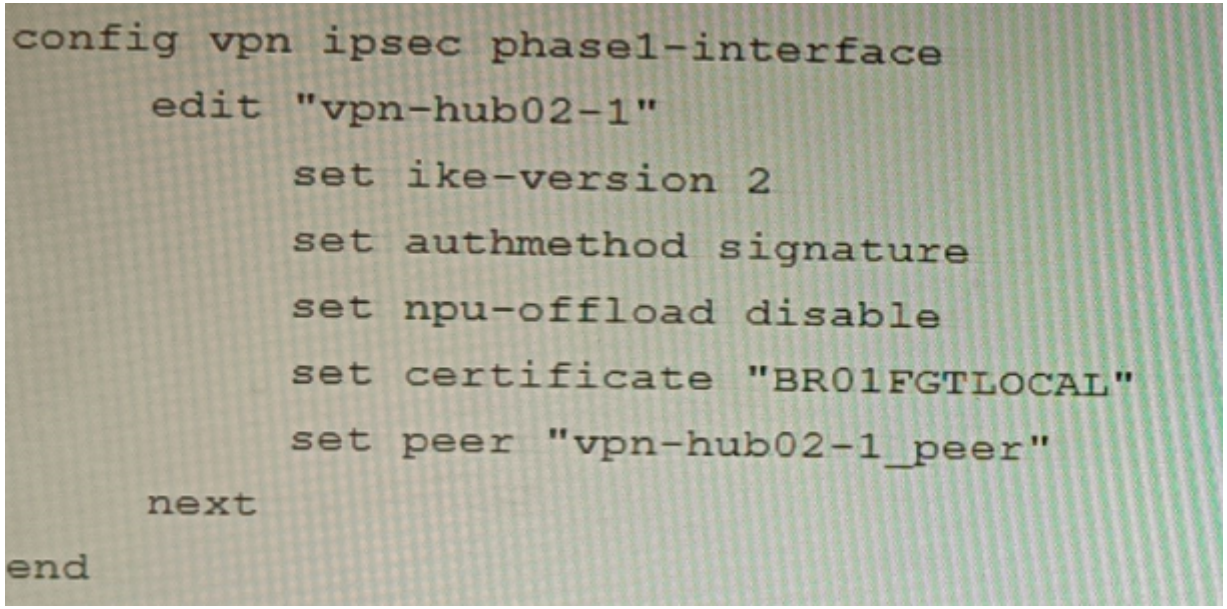
A)

```
config vpn ipsec phase1-interface
     edit "vpn-hub02-1"
          set ike-version 1
          set authmethod signature
          set certificate "BR01FGTLOCAL"
          set peer "vpn-hub02-1_peer"
     next
end
```

B)

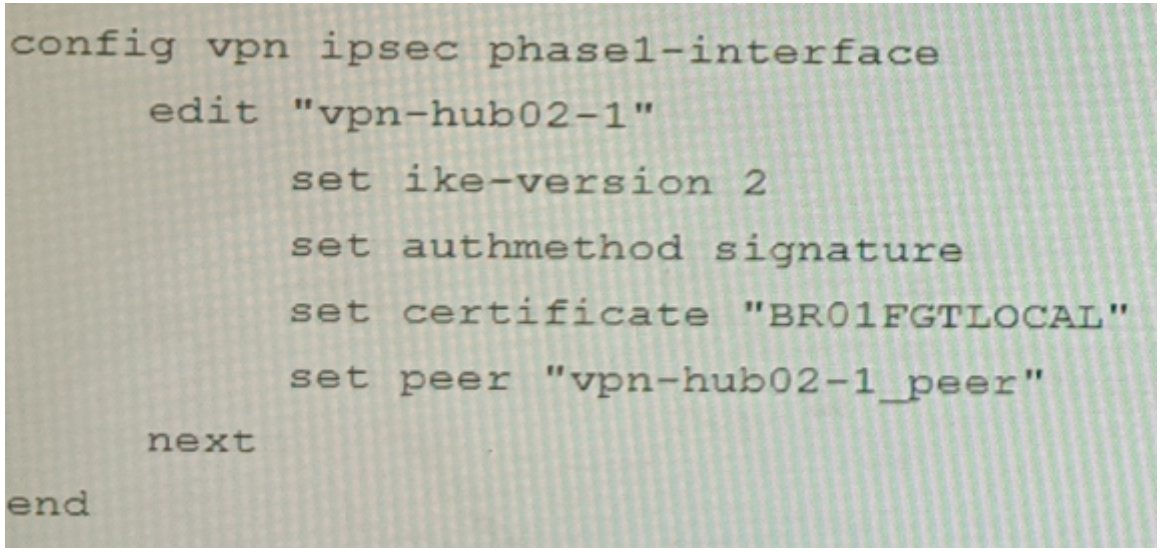
```
config vpn ipsec phase1-interface
     edit "vpn-hub02-1"
          set ike-version 2
          set net-device enable
          set psksecret fortinet
     next
end
```

C)



```
config vpn ipsec phase1-interface
     edit "vpn-hub02-1"
          set ike-version 2
          set authmethod signature
          set npu-offload disable
          set certificate "BR01FGTLOCAL"
          set peer "vpn-hub02-1_peer"
     next
end
```

D)



Options:

A- Option A

B- Option B

C- Option C

D- Option D

Answer:

C

Explanation:

The output in Exhibit A shows that the VPN tunnel is not established because the peer IP address is incorrect. The output in Exhibit B shows that the peer IP address is 192.168.1.100, but the baseline VPN configuration in Exhibit C shows that the peer IP address should be 192.168.1.101.

To restore VPN connectivity, you need to change the peer IP address in the VPN tunnel configuration to 192.168.1.101. The correct configuration is shown below:

config vpn ipsec phase1-interface

edit 'wan'

set peer-ip 192.168.1.101

set peer-id 192.168.1.101

set dhgrp 1

set auth-mode psk

set psk SECRET_PSK

next

end

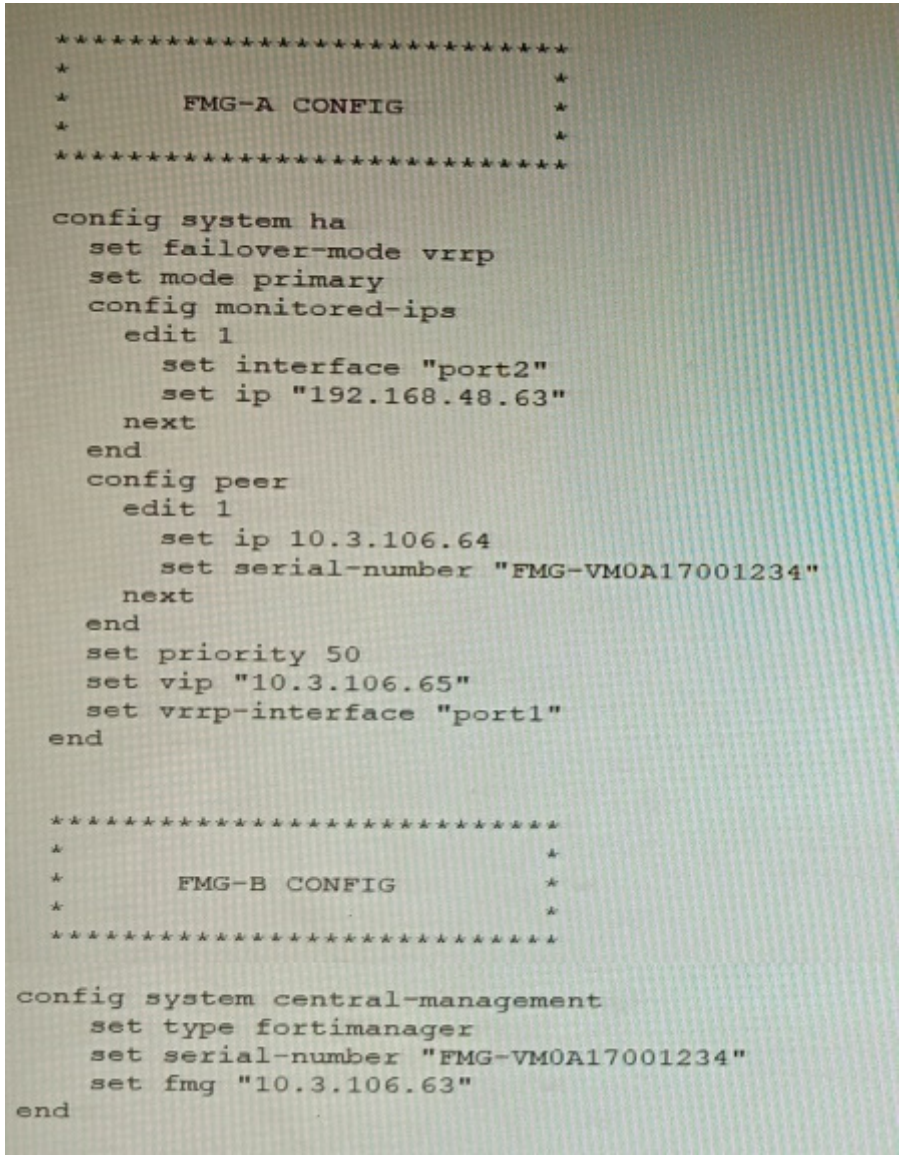
Option A is incorrect because it does not change the peer IP address. Option B is incorrect because it changes the peer IP address to 192.168.1.100, which is the incorrect IP address. Option D is incorrect because it does not include the necessary configuration for the

VPN tunnel.

Question 6

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 7

Question Type: MultipleChoice

Refer to the exhibits.

Configuration

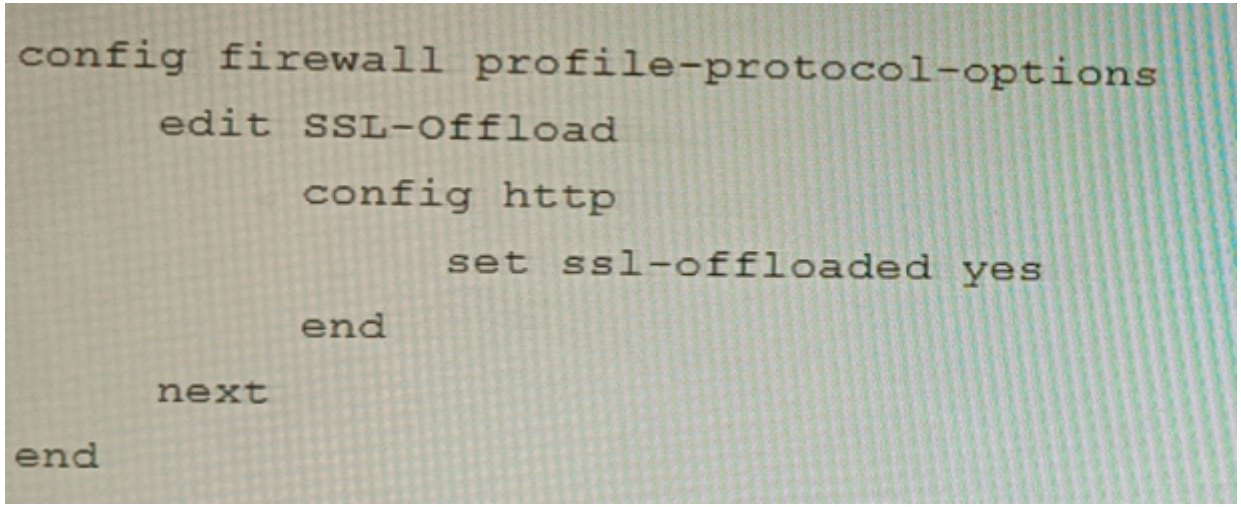
```
config firewall profile-protocol-options
    edit "SSL-Offload"
        set comment "For FAD decrypted traffic"
        config http
            set ports 80
            unset options
            unset post-lang
        end
        config ftp
            set ports 21
            set options splice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



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 8

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