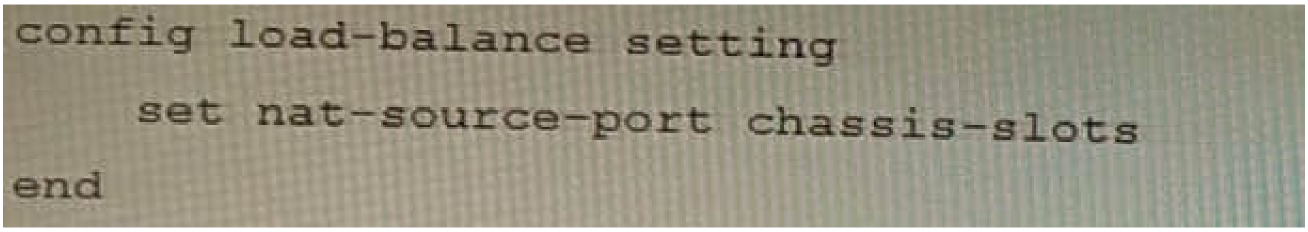
NSE8_812$^{Q\&As}$

Network Security Expert 8 Written Exam

Pass Fortinet NSE8_812 Exam with 100% Guarantee

QUESTION 1

Review the following FortiGate-6000 configuration excerpt:



```
config load-balance setting
    set nat-source-port chassis-slots
end
```

Based on the configuration, which statement is correct regarding SNAT source port partitioning behavior?

A. It dynamically distributes SNAT source ports to operating FPCs or FPMs.

B. It is the default SNAT configuration and preserves active sessions when an FPC or FPM goes down.

C. It statically distributes SNAT source ports to operating FPCs or FPMs

D. It equally distributes SNAT source ports across chassis slots.

Correct Answer: A

Explanation: The configuration excerpt shows that the SNAT source port partitioning behavior is set to dynamic. This means that the FortiGate will dynamically distribute SNAT source ports to operating FPCs or FPMs. This ensures that active

sessions are not interrupted if an FPC or FPM goes down.

The other options are incorrect. Option B is incorrect because the default SNAT configuration is static. Option C is incorrect because the configuration excerpt does not specify that SNAT source ports are statically distributed. Option D is

incorrect because the SNAT source ports are not evenly distributed across chassis slots. Here are some additional details about SNAT source port partitioning behavior:

SNAT source port partitioning behavior can be set to dynamic or static.

The default SNAT configuration is static.

Dynamic SNAT source port partitioning ensures that active sessions are not interrupted if an FPC or FPM goes down.

Static SNAT source port partitioning can improve performance by reducing the number of SNAT lookups.

QUESTION 2

Refer to the exhibit.

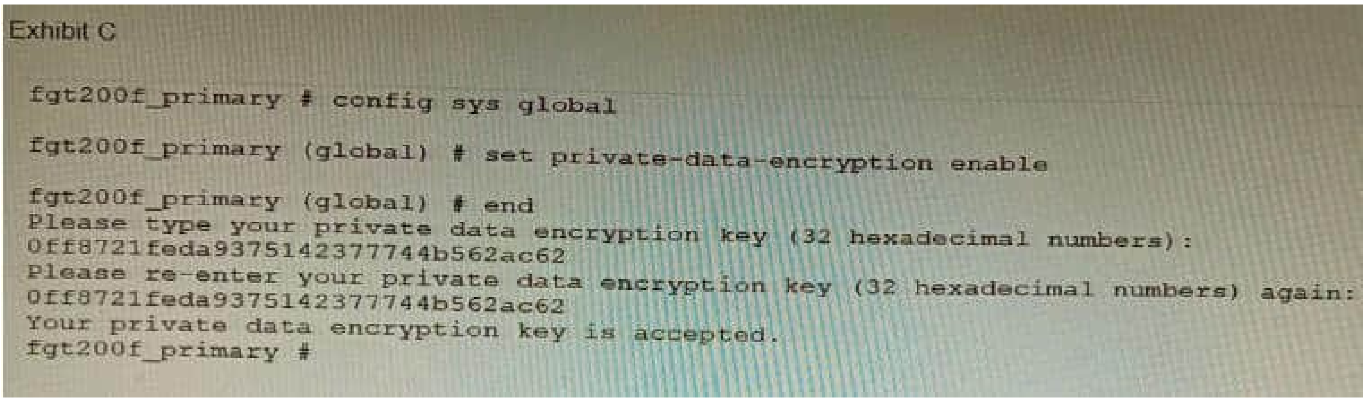


Exhibit C

```
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):
0ff8721feda9375142377744b562ac62
Please re-enter your private data encryption key (32 hexadecimal numbers) again:
0ff8721feda9375142377744b562ac62
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.

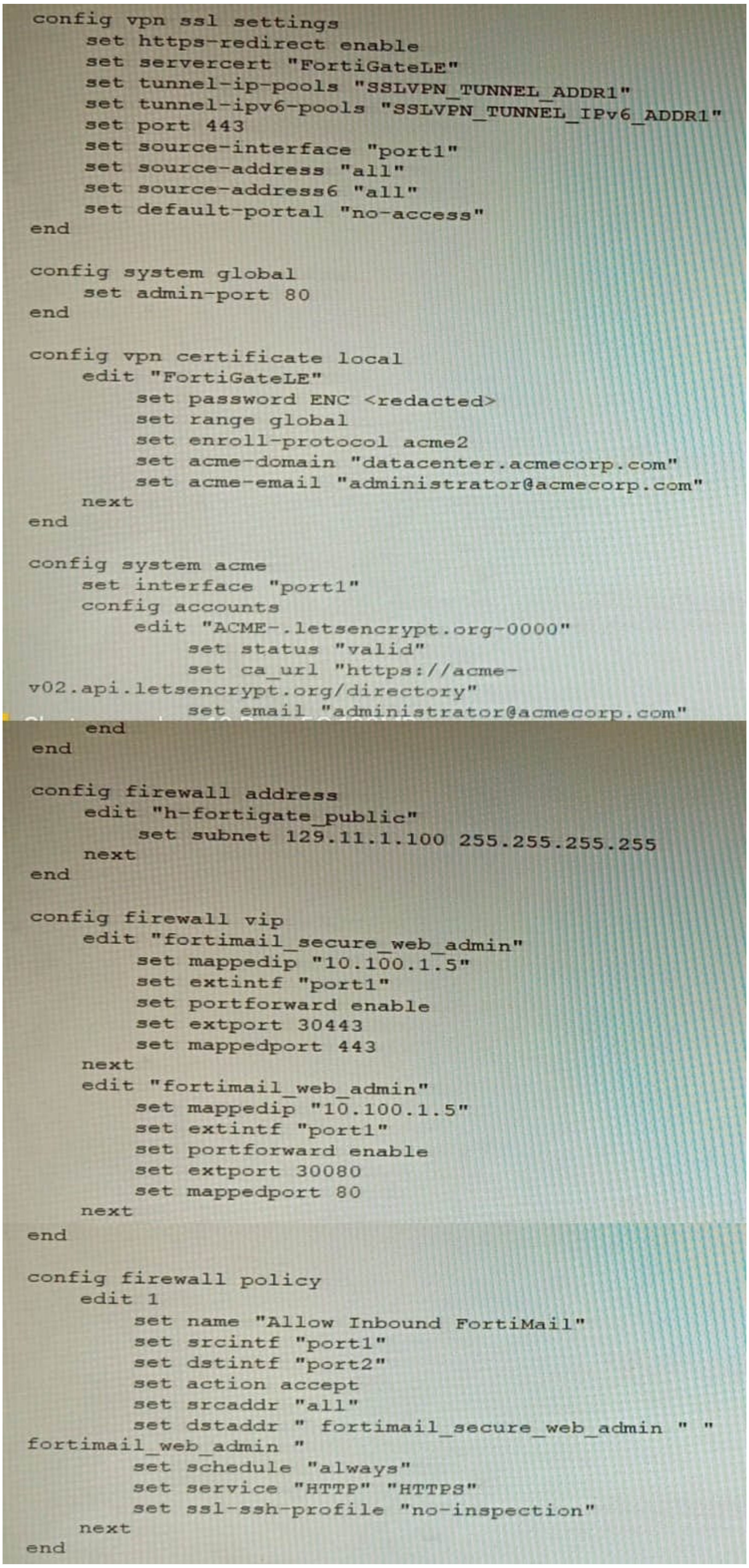
D. TPM functionality is not yet compatible with FortiGate HA D The administrator needs to manually enter the hex private data encryption key in FortiManager

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

QUESTION 3

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

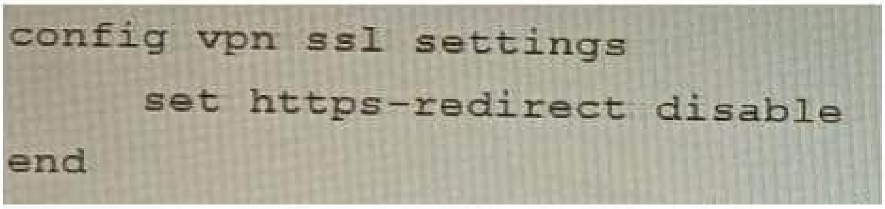


```
config vpn ssl settings
    set https-redirect enable
    set servercert "FortiGateLE"
    set tunnel-ip-pools "SSLVPN_TUNNEL_ADDR1"
    set tunnel-ipv6-pools "SSLVPN_TUNNEL_IPv6_ADDR1"
    set port 443
    set source-interface "port1"
    set source-address "all"
    set source-address6 "all"
 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

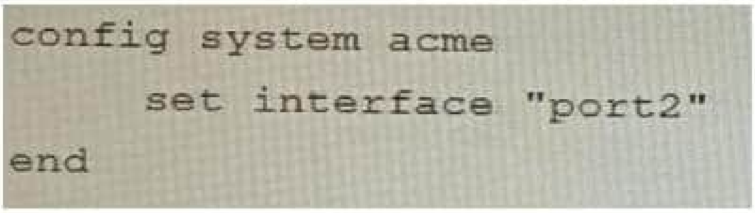
Reviewing the requirement and the exhibit, which configuration change below will resolve this issue?

○ A.



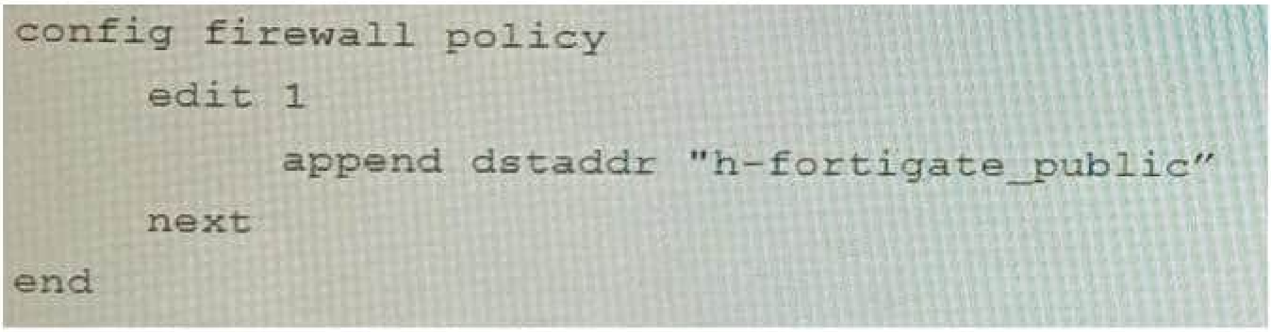
```
config vpn ssl settings
      set https-redirect disable
end
```

○ B.



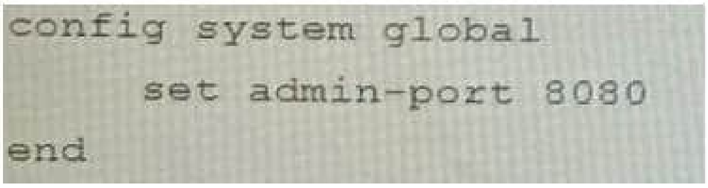
```
config system acme
      set interface "port2"
end
```

○ 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:

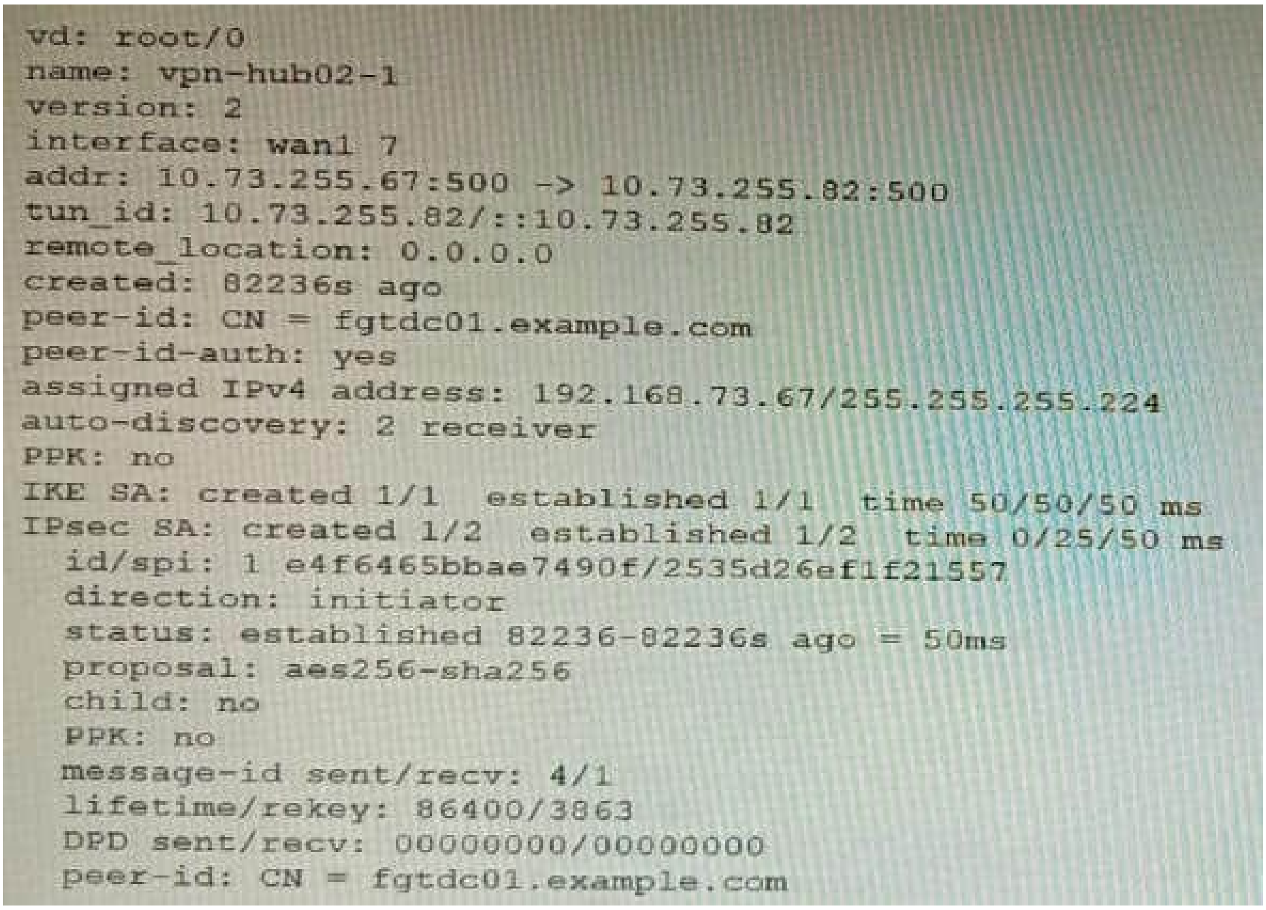
https://docs.fortinet.com/document/fortigate/7.0.0/administration- guide/822087/acme-certificate-support

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

QUESTION 4

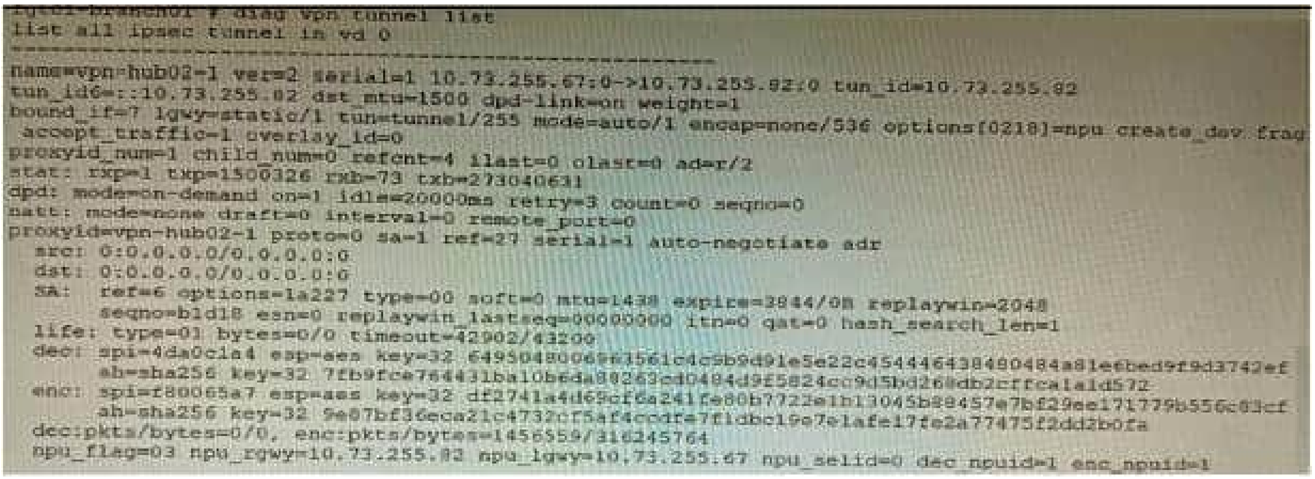
Refer to the exhibits.

Exhibit A



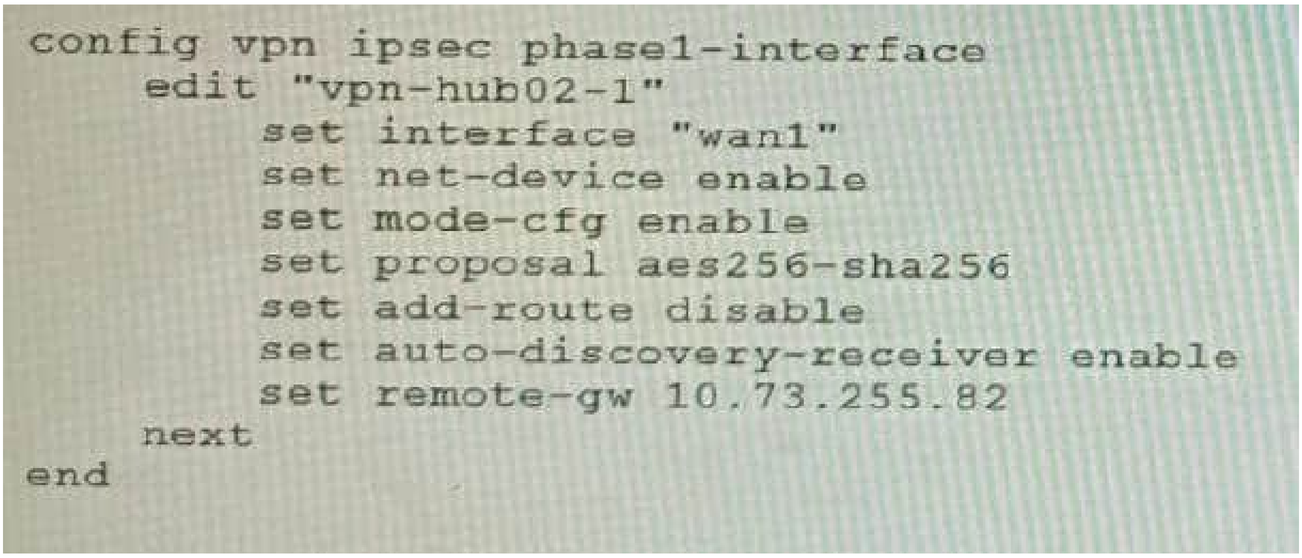
```
vd: root/0
name: vpn-hub02-1
version: 2
interface: wan1 7
addr: 10.73.255.67:500 -> 10.73.255.82:500
tun_id: 10.73.255.82/::10.73.255.82
remote_location: 0.0.0.0
created: 82236s ago
peer-id: CN = fgtdc01.example.com
peer-id-auth: yes
assigned IPv4 address: 192.168.73.67/255.255.255.224
auto-discovery: 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=10.73.255.82
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[0218]=npu create_dev frag
 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=2048
       seqno=b1d18 esn=0 replaywin_lastseq=00000000 itn=0 qat=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=42902/43200
  dec: spi=4da0c1a4 esp=aes key=32 6495048006963561c4c9b9d91e5e22c454446438480484a81e6bed9f9d3742ef
       ah=sha256 key=32 7fb9fce764431ba10b6da80263cd0484d9f5824cc9d5bd268db2cffca1a1d572
  enc: spi=f80065a7 esp=aes key=32 df2741a4d69cf6a241fe80b7722e1b13045b88457e7bf29ee171779b556c83cf
       ah=sha256 key=32 9e87bf36eca21c4732cf5af4ccdfe7f1dbc19e7e1afe17fe2a77475f2dd2b0fa
  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_npuid=1 enc_npuid=1
```

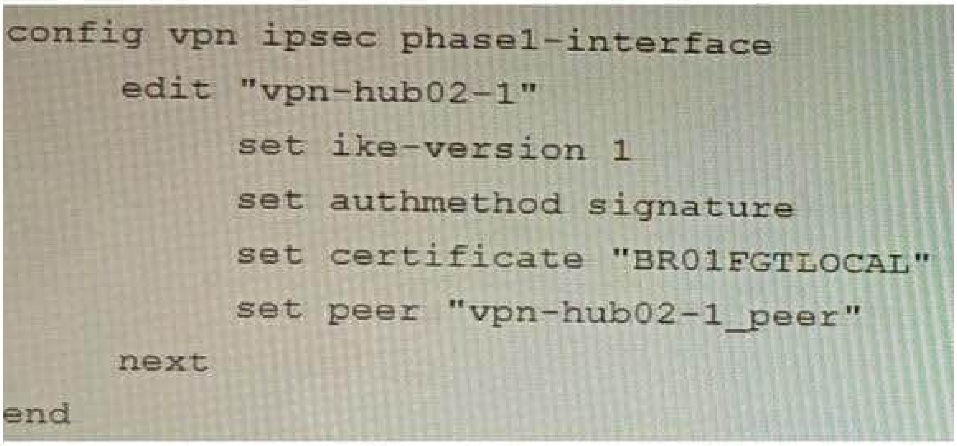
Exhibit C



```
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
```

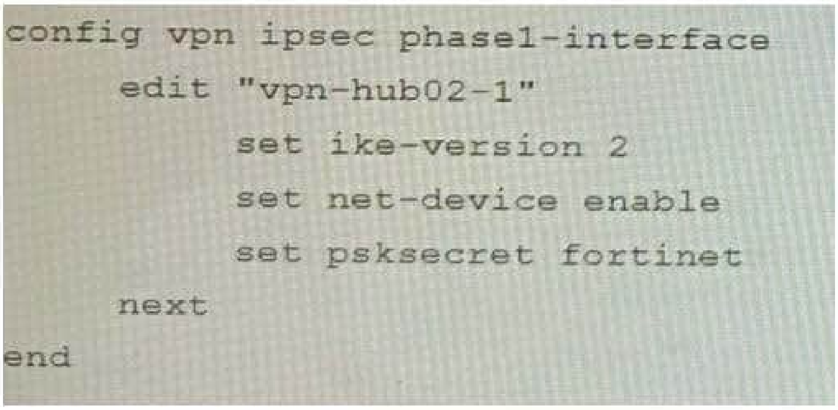
A customer is trying to set up a VPN with a FortiGate, but they do not have a backup of the configuration. Output during a troubleshooting session is shown in the exhibits A and B and a baseline VPN configuration is shown in Exhibit C Referring to the exhibits, which configuration will restore VPN connectivity?

○ A.



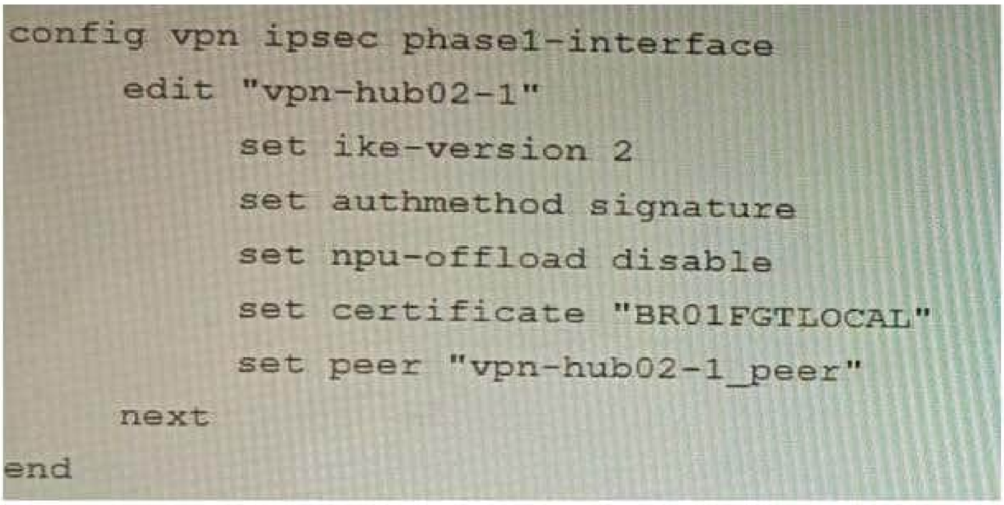
```
config vpn ipsec phase1-interface
     edit "vpn-hub02-1"
          set ike-version 1
          set authmethod signature
          set certificate "BR01FGTLOCAL"
          set peer "vpn-hub02-1_peer"
     next
end
```

○ B.



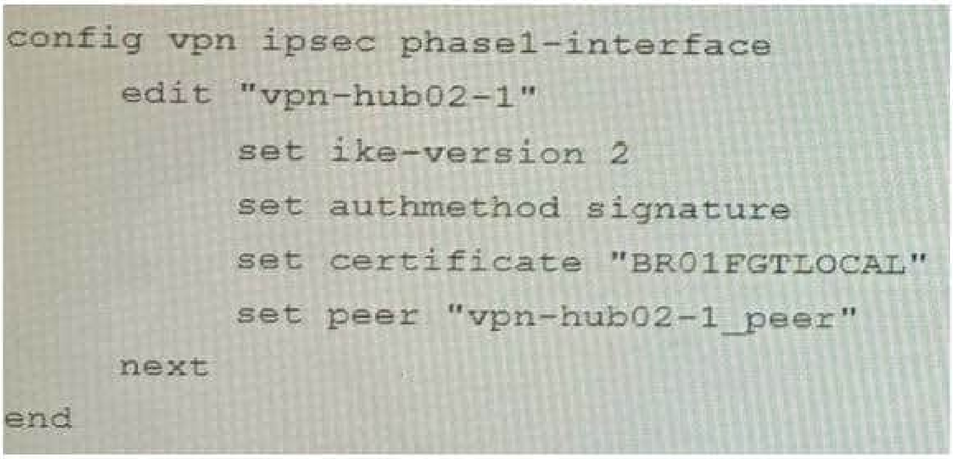
```
config vpn ipsec phase1-interface
     edit "vpn-hub02-1"
          set ike-version 2
          set net-device enable
          set psksecret fortinet
     next
end
```

○ 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.



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

A. Option A

B. Option B

C. Option C

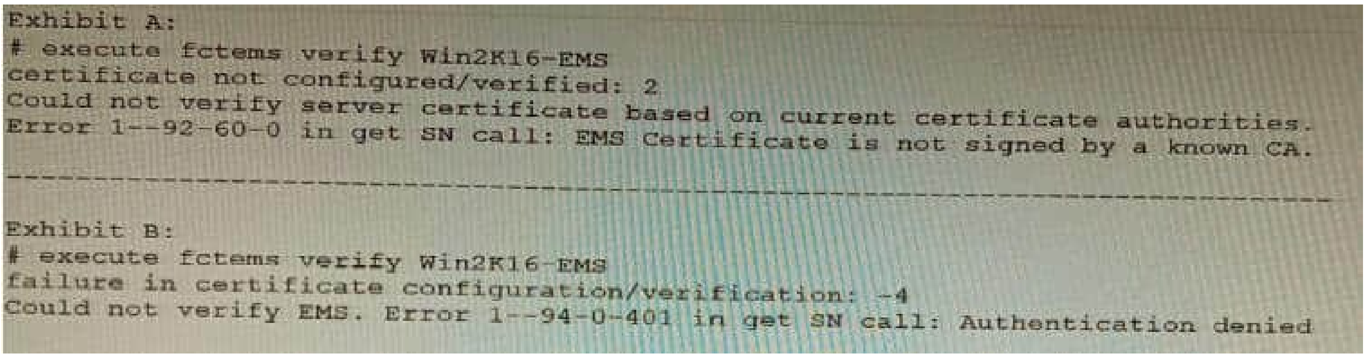
D. Option D

Correct 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 5

Refer to the exhibit.



```
Exhibit A:
# execute fctems verify Win2K16-EMS
certificate not configured/verified: 2
Could not verify server certificate based on current certificate authorities.
Error 1--92-60-0 in get SN call: EMS Certificate is not signed by a known CA.
------------------------------------------------------------------------------

Exhibit B:
# execute fctems verify Win2K16-EMS
failure in certificate configuration/verification: -4
Could not verify EMS. Error 1--94-0-401 in get SN call: Authentication denied
```

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.)

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

Correct Answer: AD

A is 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.

D is 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