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

Network Security Expert 8 Written Exam

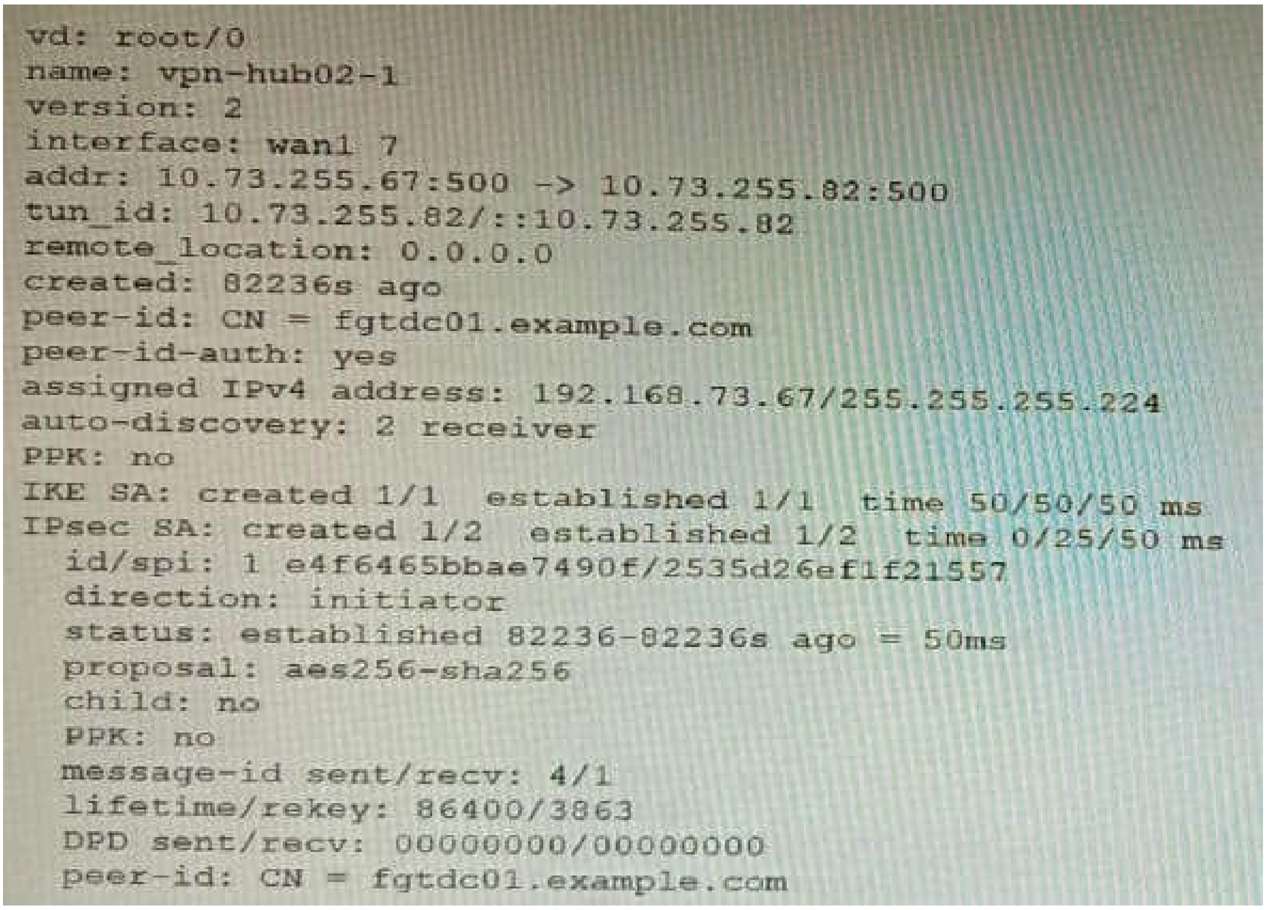
## Pass Fortinet NSE8_812 Exam with 100% Guarantee

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

**QUESTION 1**

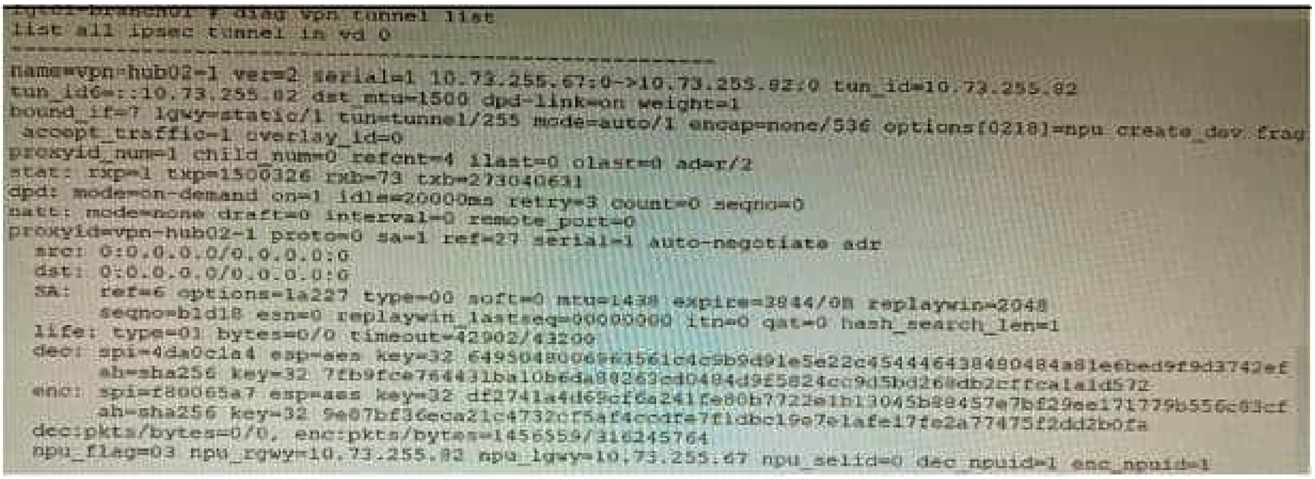
Refer to the exhibits.

Exhibit A



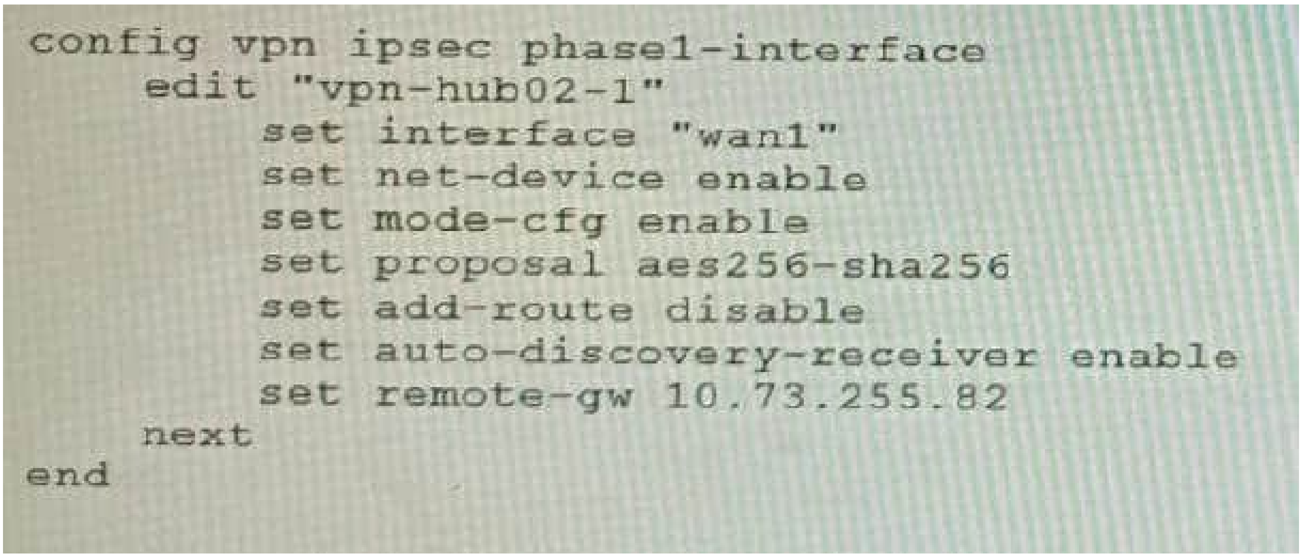
```
vd: root/0
name: vpn-hub02-1
version: 2
interface: wan1 7
addr: 10.73.255.67:500 -> 10.73.255.82:500
tun_id: 10.73.255.82/::10.73.255.82
remote_location: 0.0.0.0
created: 82236s ago
peer-id: CN = fgtdc01.example.com
peer-id-auth: yes
assigned IPv4 address: 192.168.73.67/255.255.255.224
auto-discovery: 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 64950480069e3561c4c9b9d91e5e22c454444643848 0484a81e6bed9f9d3742ef
       ah=sha256 key=32 7fb9fce764431ba10be4a80263cd0484d9f5824cc9d5bd268db2cffca1a1d572
  enc: spi=f80065a7 esp=aes key=32 df2741a4d69cf6a241fe80b7722e1b13045b88457e7bf29ee171779b556c03cf
       ah=sha256 key=32 9e07bf36eca21c4732cf5af4ccdfe7f1dbc19e7e1afe17fe2a77475f2dd2b0fa
  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
```

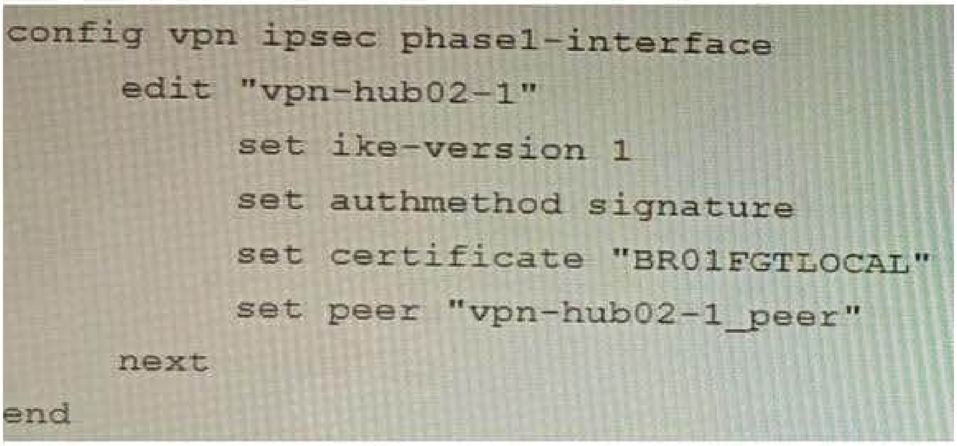
Exhibit C



```
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
```

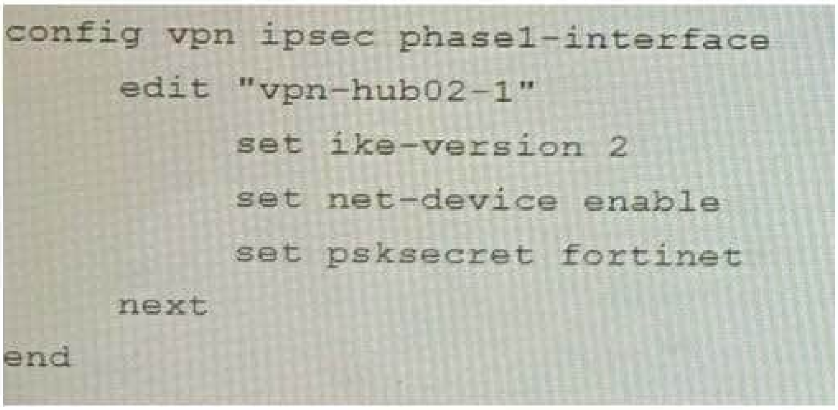
A customer is trying to set up a VPN with a FortiGate, but they do not have a backup of the configuration. Output during a troubleshooting session is shown in the exhibits A and B and a baseline VPN configuration is shown in Exhibit C Referring to the exhibits, which configuration will restore VPN connectivity?

○ A.



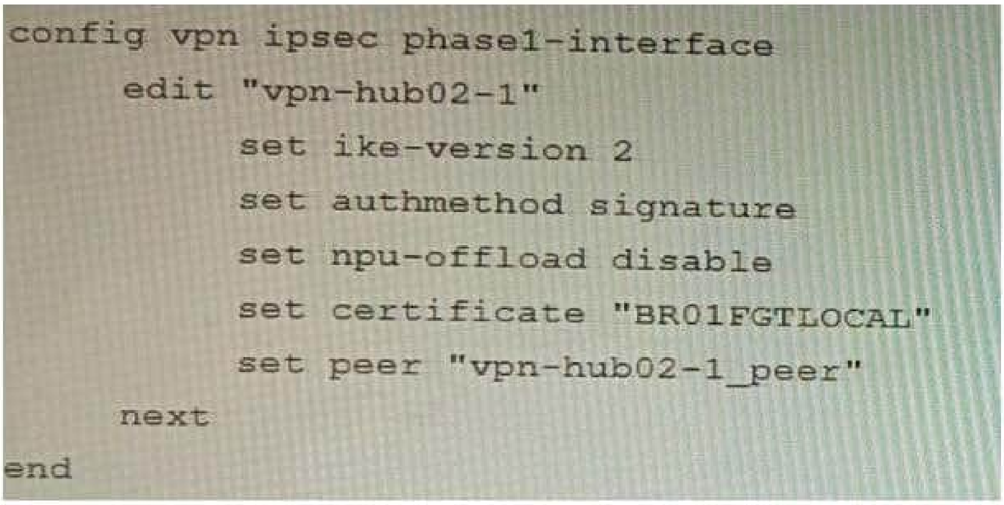
```
config vpn ipsec phase1-interface
    edit "vpn-hub02-1"
        set ike-version 1
        set authmethod signature
        set certificate "BR01FGTLOCAL"
        set peer "vpn-hub02-1_peer"
    next
end
```

○ B.



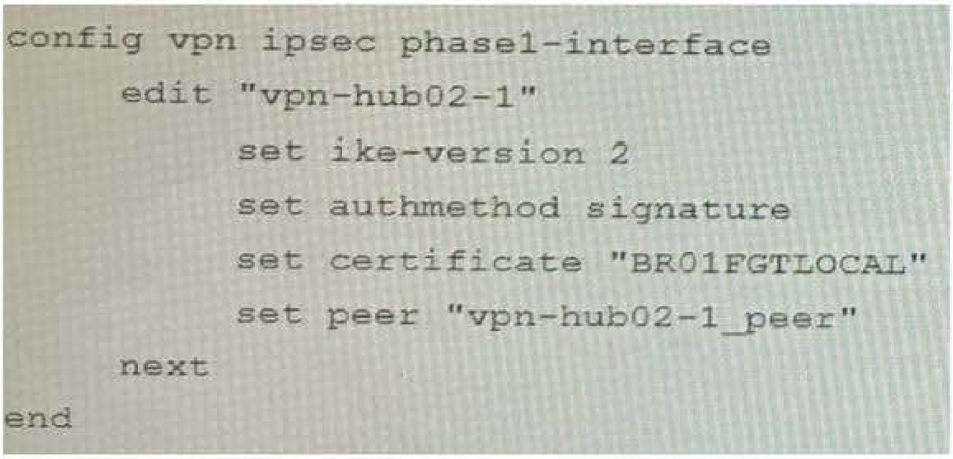
```
config vpn ipsec phase1-interface
    edit "vpn-hub02-1"
        set ike-version 2
        set net-device enable
        set psksecret fortinet
    next
end
```

○ 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

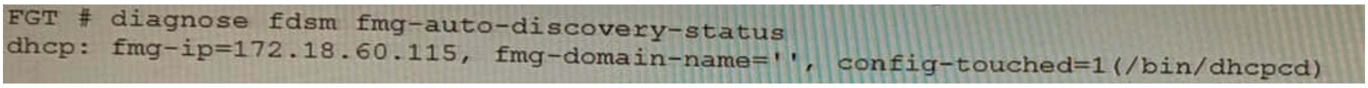
Correct Answer: C

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 2**

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:



```
FGT # diagnose fdsm fmg-auto-discovery-status
dhcp: fmg-ip=172.18.60.115, fmg-domain-name='', config-touched=1(/bin/dhcpcd)
```

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

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

Correct 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-availabilityhttps://docs.fortinet.com/document/fortimanager/7.4.0/administration- guide/568591/high-availability/568592/configuring-ha-options

**QUESTION 3**

Which two methods are supported for importing user defined Lookup Table Data into the FortiSIEM? (Choose two.)

A. Report

B. FTP

C. API D. SCP

Correct Answer: AC

Explanation: FortiSIEM supports two methods for importing user defined Lookup Table Data:

Report: You can import lookup table data from a report. This is the most common method for importing lookup table data.

API: You can also import lookup table data using the FortiSIEM API. This is a more advanced method that allows you to import lookup table data programmatically.

FTP, SCP, and other file transfer protocols are not supported for importing lookup table data into FortiSIEM.

Reference:https://help.fortinet.com/fsiem/6-7-4/Online- Help/HTML5_Help/importing_lookup_table_data.htm

**QUESTION 4**

What is the benefit of using FortiGate NAC LAN Segments?

A. It provides support for multiple DHCP servers within the same VLAN.

B. It provides physical isolation without changing the IP address of hosts.

C. It provides support for IGMP snooping between hosts within the same VLAN

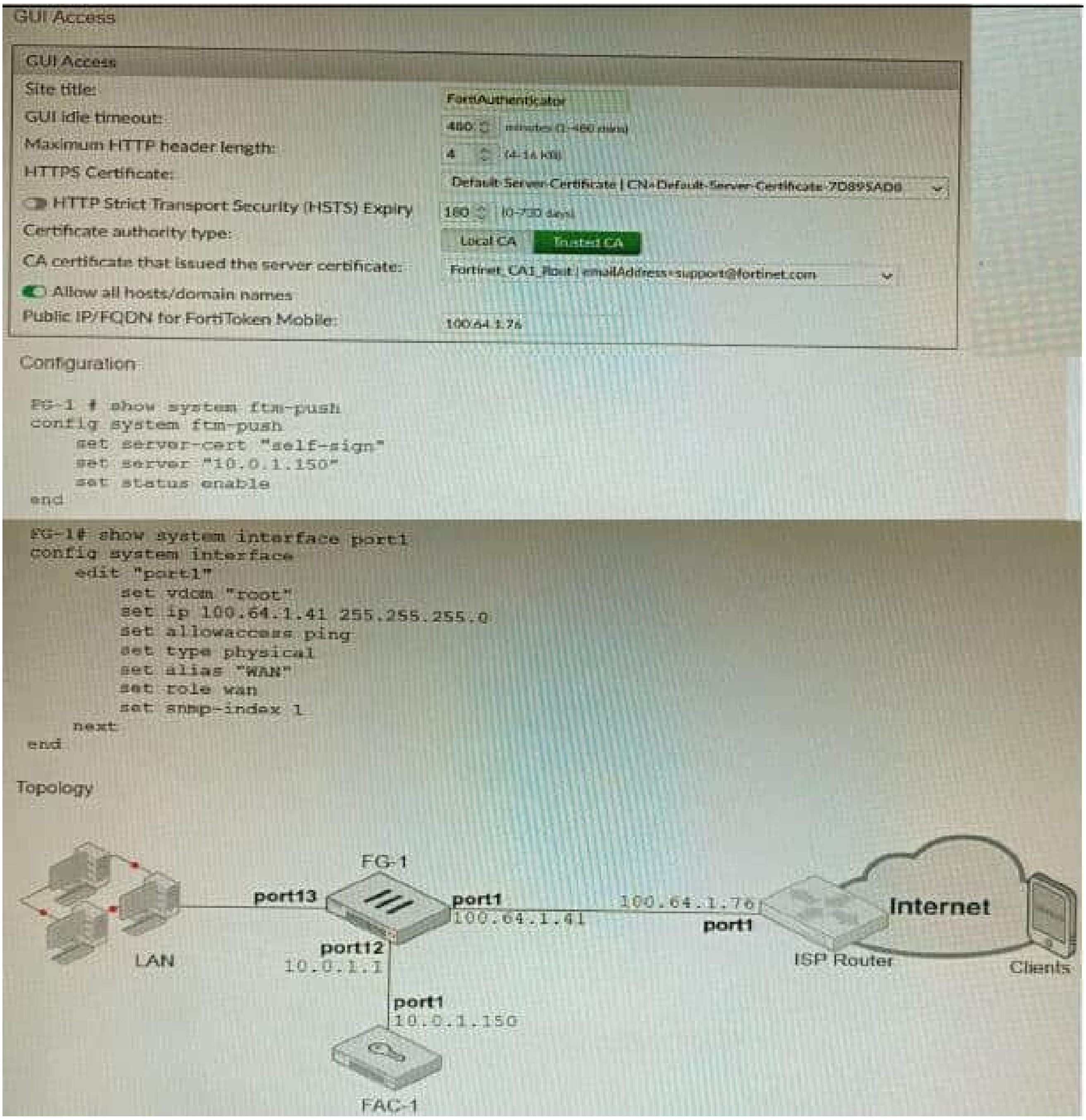
D. It allows for assignment of dynamic address objects matching NAC policy.

Correct Answer: D

Explanation: FortiGate NAC LAN Segments are a feature that allows users to assign different VLANs to different LAN segments without changing the IP address of hosts or bouncing the switch port. This provides physical isolation while maintaining firewall sessions and avoiding DHCP issues. One benefit of using FortiGate NAC LAN Segments is that it allows for assignment of dynamic address objects matching NAC policy. This means that users can create firewall policies based on dynamic address objects that match the NAC policy criteria, such as device type, OS type, MAC address, etc. This simplifies firewall policy management and enhances security byapplying different security profiles to different types of devices. References: https://docs.fortinet.com/document/fortigate/7.0.0/new-features/856212/nac-lan-segments- 7-0-1

**QUESTION 5**

Refer to the exhibits.



GUI Access

GUI Access

Site title: FortiAuthenticator

GUI idle timeout: 480 minutes (1-480 mins)

Maximum HTTP header length: 4 (4-16 KB)

HTTPS Certificate: Default-Server-Certificate | CN=Default-Server-Certificate-7D895AD8

HTTP Strict Transport Security (HSTS) Expiry 180 (0-730 days)

Certificate authority type: Local CA | Trusted CA

CA certificate that issued the server certificate: Fortinet_CA1_Root | emailAddress=support@fortinet.com

Allow all hosts/domain names

Public IP/FQDN for FortiToken Mobile: 100.64.1.76

Configuration

```
FG-1 # show system ftm-push
config system ftm-push
    set server-cert "self-sign"
    set server "10.0.1.150"
    set status enable
end
```

```
FG-1# show system interface port1
config system interface
    edit "port1"
        set vdom "root"
        set ip 100.64.1.41 255.255.255.0
        set allowaccess ping
        set type physical
        set alias "WAN"
        set role wan
        set snmp-index 1
    next
end
```

Topology

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

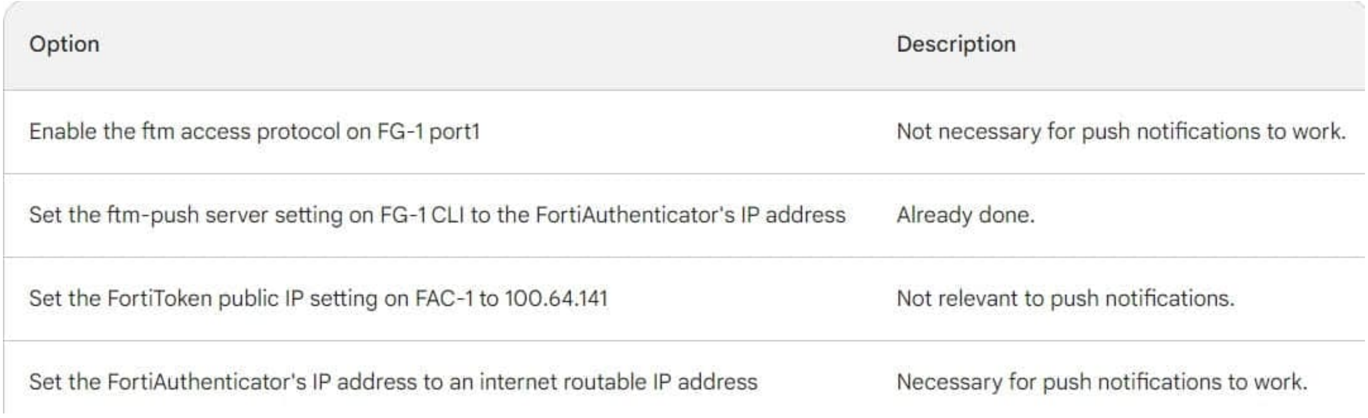
Correct Answer: B

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. |

NSE8_812 Study Guide NSE8_812 Exam Questions NSE8_812 Braindumps