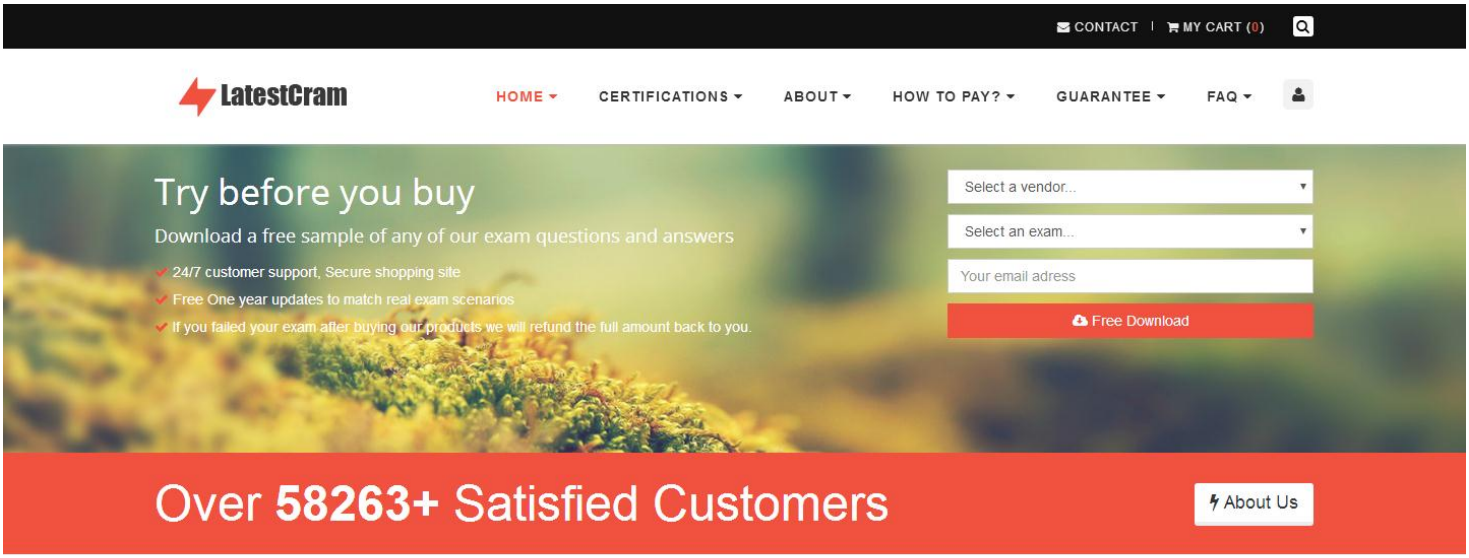
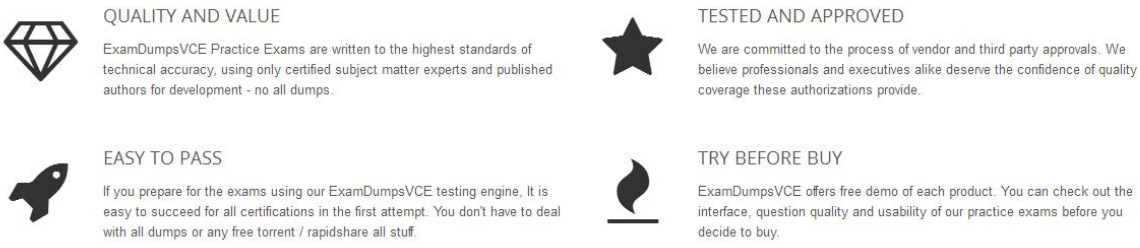
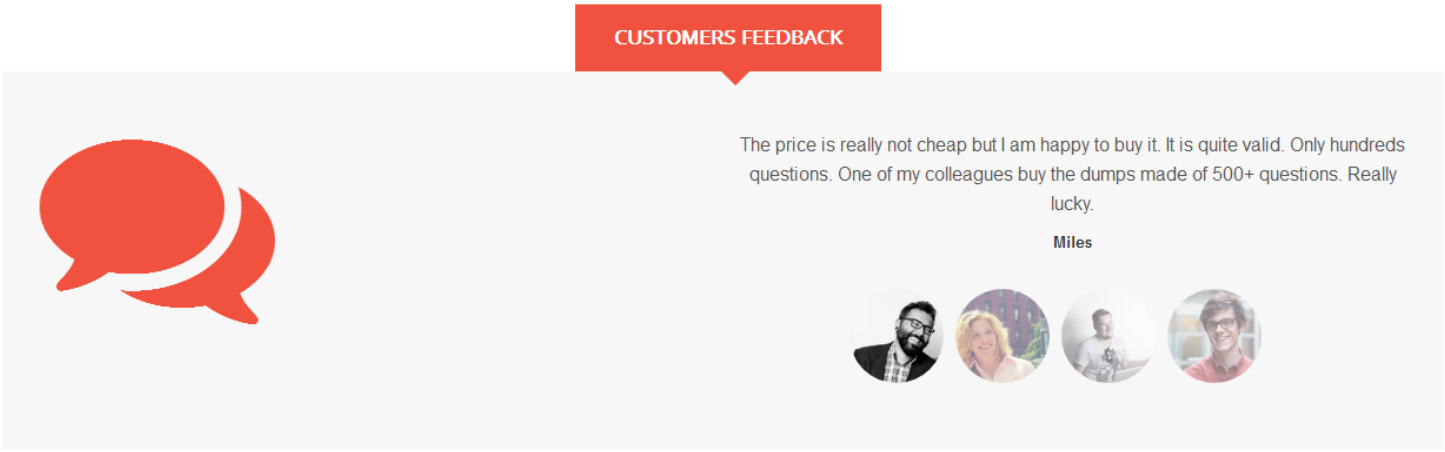
LatestCram

LatestCram







http://www.latestcram.com

Reliable Exam Braindumps & Valid Latest Questions & Right Exam Cram

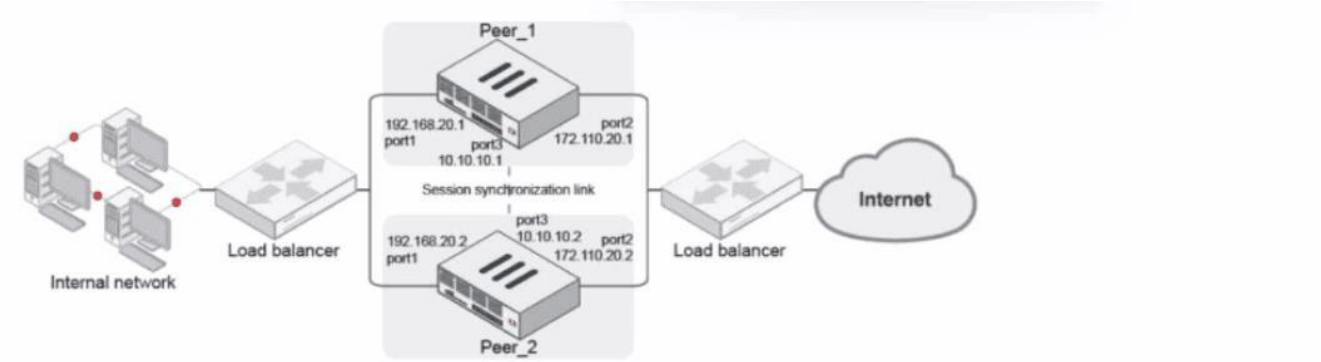
Exam : **NSE8_812**

Title : Fortinet NSE 8 - Written Exam (NSE8_812)

Vendor : Fortinet

Version : DEMO

NO.1 Refer to the exhibit.



Given the exhibit, which two statements about FortiGate FGSP HA cluster behavior are correct? (Choose two.)

A. You can run FortiGate Virtual Router Redundancy Protocol (VRRP) high availability in addition to FGSP simultaneously.

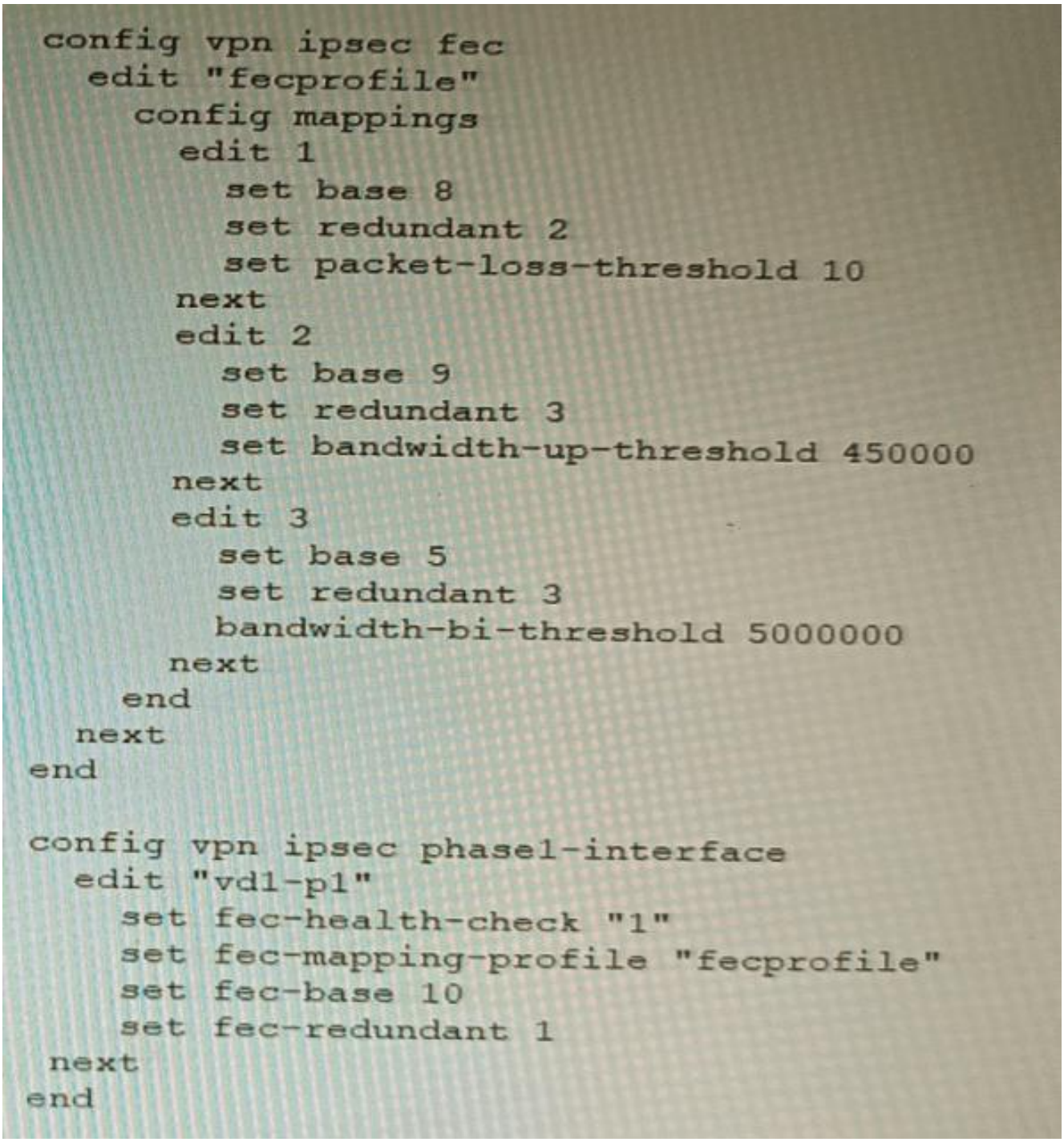
B. Session synchronization occurs over Layer 3 by default, and if unavailable it will then try Layer 2.

C. You can selectively synchronize only specific sessions between FGSP cluster members.

D. Cluster members will upgrade one at a time and failover during firmware upgrades.

Answer: A B

NO.2 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?

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: A

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.
Reference: https://docs.fortinet.com/document/fortigate/7.0.0/new-features/169010/adaptive-forward-error- correction-7-0-2

NO.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.
Answer: C D
Explanation:
https://docs.fortinet.com/document/fortimail/7.2.0/cookbook/963264/configuring-outbound-settings-in-office-
365

NO.4 You are designing a setup where the FortiGate device is connected to two upstream ISPs using BGP. Part of the requirement is that you must be able to refresh the route advertisements manually without disconnecting the BGP neighborships.
Which feature must you enable on the BGP neighbors to accomplish this goal?
A. Synchronization
B. Deterministic-med
C. Graceful-restart
D. Soft-reconfiguration
Answer: D
Explanation:
The soft reconfigure is correct by elimination (FGTs all support BGP Refresh, so question is not worded correctly - to refresh routes in advertisements, there is no need to do manually anything, after the change is committed to config FGT will send BGP Refresh message to the peers to notify them of it. The same is true for Cisco and Juniper routers. The question should ask "when routing policy was changed" - then yes, reconfiguraiton is the way to notify BGP peers that BGP policy was changed.

NO.5 Refer to the exhibits, which show a topology and diagnostic commands.

Exhibit A

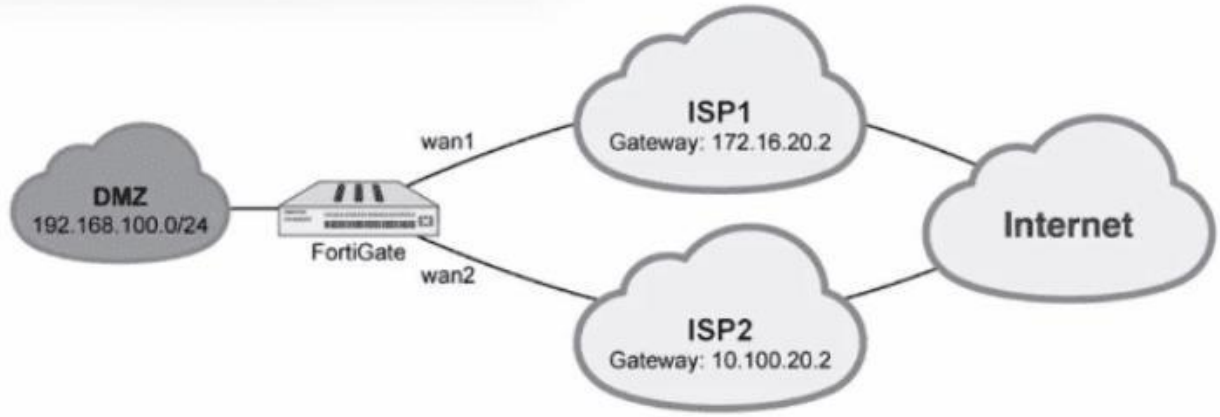


Exhibit B

```
FGT # diagnose sys sdwan service
Service(1): Address Mode(IPV4) flags=0x200
  Gen(6), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(priority), link-cost-factor(latency),
link-cost-threshold(20), heath-check(Default_Gmail)
  Members(2):
    1: Seq_num(1 wan1), alive, latency: 200.177, selected
    2: Seq_num(2 wan2), alive, latency: 167.417, selected
  Src address(1):
        192.168.100.0-192.168.100.255

  Dst address(1):
        0.0.0.0-255.255.255.255

FGT # diagnose sys sdwan health-check
Health Check(Default_Gmail):
Seq(1 wan1): state(alive), packet-loss(2.000%) latency(200.564), jitter(1.277) sla_map=0x1
Seq(2 wan2): state(alive), packet-loss(0.000%) latency(167.877), jitter(1.060) sla_map=0x1

FGT # diagnose sys sdwan member
Member(1): interface: wan1, priority: 0, weight: 0
Member(2): interface: wan2, priority: 0, weight: 0
```

Which two statements about the path resolution are true? (Choose two.)

A. Latency is the quality criteria.

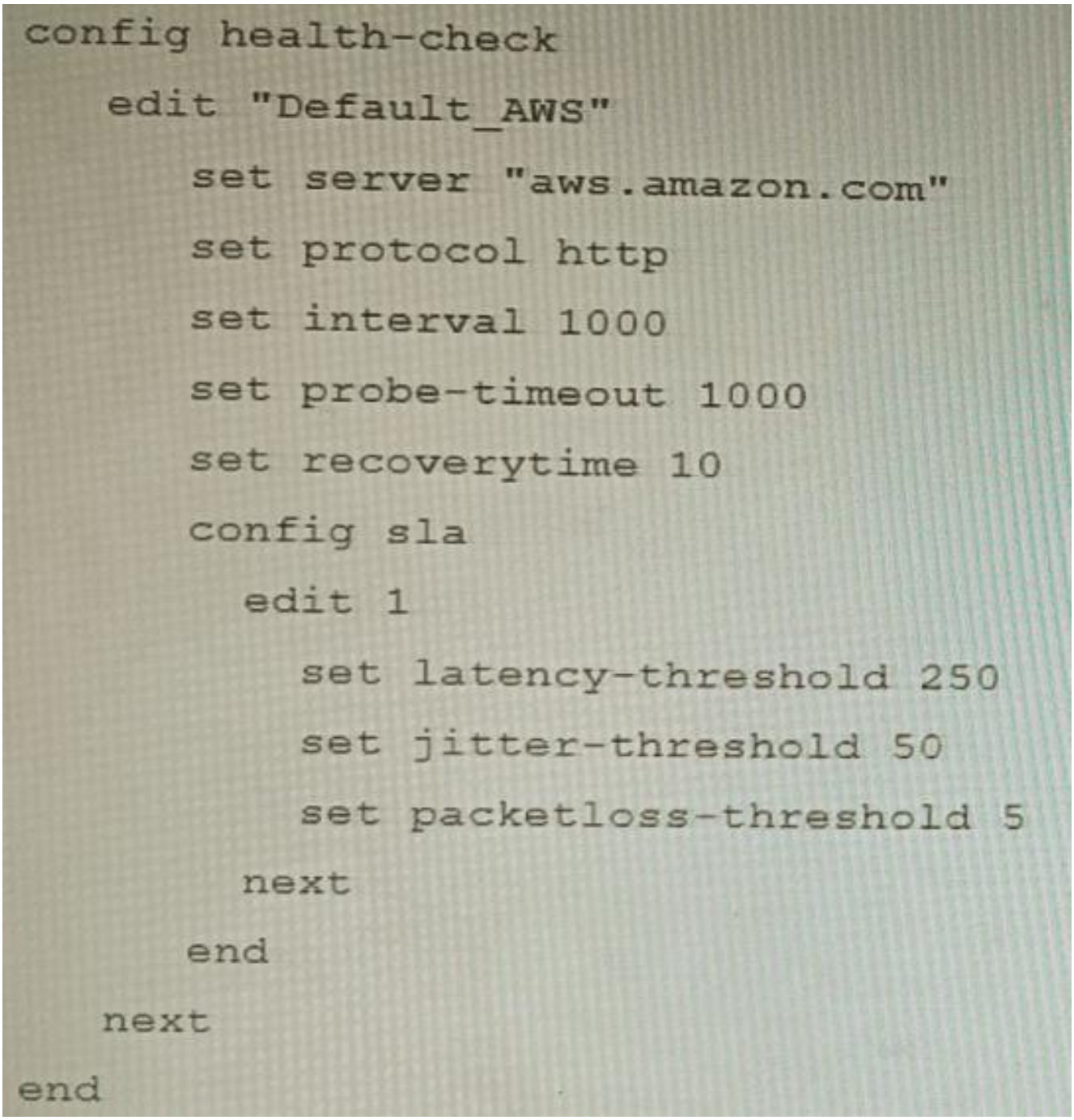
B. wan1 is currently used as an outgoing interface.

C. wan2 is currently used as an outgoing interface.

D. Packet-loss is the quality criteria.

Answer: A

NO.6 You are creating the CLI script to be used on a new SD-WAN deployment You will have branches with a different number of internet connections and want to be sure there is no need to change the Performance SLA configuration in case more connections are added to the branch. The current configuration is:



```
config health-check
    edit "Default_AWS"
        set server "aws.amazon.com"
        set protocol http
        set interval 1000
        set probe-timeout 1000
        set recoverytime 10
        config sla
            edit 1
                set latency-threshold 250
                set jitter-threshold 50
                set packetloss-threshold 5
            next
        end
    next
end
```

Which configuration do you use for the Performance SLA members?

A. set members any

B. set members 0

C. current configuration already fulfills the requirement

D. set members all

Answer: B

References:

Performance SLA | FortiGate / FortiOS 7.4.0

Configuring Performance SLA | FortiGate / FortiOS 7.4.0

NO.7 A remote worker requests access to an SSH server inside the network. You deployed a ZTNA Rule to their FortiClient. You need to follow the security requirements to inspect this traffic.

Which two statements are true regarding the requirements? (Choose two.)

A. FortiGate can perform SSH access proxy host-key validation.

B. You need to configure a FortiClient SSL-VPN tunnel to inspect the SSH traffic.

C. SSH traffic is tunneled between the client and the access proxy over HTTPS

D. Traffic is discarded as ZTNA does not support SSH connection rules

Answer: A C

Explanation:

ZTNA supports SSH connection rules that allow remote workers to access SSH servers inside the network through an HTTPS tunnel between the client and the access proxy (FortiGate). The access proxy acts as an SSH client to connect to the real SSH server on behalf of the user, and performs host-key validation to verify the identity of the server. The user can use any SSH client that supports HTTPS proxy settings, such as PuTTY or OpenSSH. References:

https://docs.fortinet.com/document/fortigate/7.0.0/ztna-deployment/899992/configuring-ztna-rules-to-control-access

https://docs.fortinet.com/document/fortigate/7.4.1/administration-guide/29927/ztna-ssh-access-proxy-example

NO.8 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)

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 C

NO.9 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 & 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.
E. The administrator needs to manually enter the hex private data encryption key in FortiManager.
Answer: B E
Explanation:
https://docs.fortinet.com/document/fortimanager/7.4.2/administration-guide/30332/verifying-devices-with- private-data-encryption-enabled

NO.10 Which two statements are correct on a FortiGate using the FortiGuard Outbreak Protection Service (VOS)?
(Choose two.)
A. The FortiGuard VOS can be used only with proxy-base policy inspections.
B. If third-party AV database returns a match the scanned file is deemed to be malicious.
C. The antivirus database queries FortiGuard with the hash of a scanned file
D. The AV engine scan must be enabled to use the FortiGuard VOS feature
E. The hash signatures are obtained from the FortiGuard Global Threat Intelligence database.
Answer: C E
Explanation:
* C. The antivirus database queries FortiGuard with the hash of a scanned file. This is how the FortiGuard VOS service works. The FortiGate queries FortiGuard with the hash of a scanned file, and FortiGuard returns a list of known malware signatures that match the hash.
* E. The hash signatures are obtained from the FortiGuard Global Threat Intelligence database. This is where the FortiGuard VOS service gets its hash signatures from. The FortiGuard Global Threat Intelligence database is updated regularly with new malware signatures.
https://docs.fortinet.com/document/fortigate/7.4.1/administration-guide/889364/fortiguard-outbreak- prevention

NO.11 Which two statements about bounce address tagging and verification (BATV) on FortiMail are true? (Choose two.)
A. You must publish the BATV public key as a DNS TXT record.
B. Emails with an empty sender address will be subjected to bounce verification.
C. FortiMail will insert the BATV tag to the sender address in the envelope.
D. BATV will use symmetric keys to verify the bounce address tag.
Answer: B C