NSE8_812 Q&As

Network Security Expert 8 Written Exam

Pass Fortinet NSE8_812 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/nse8_812.html

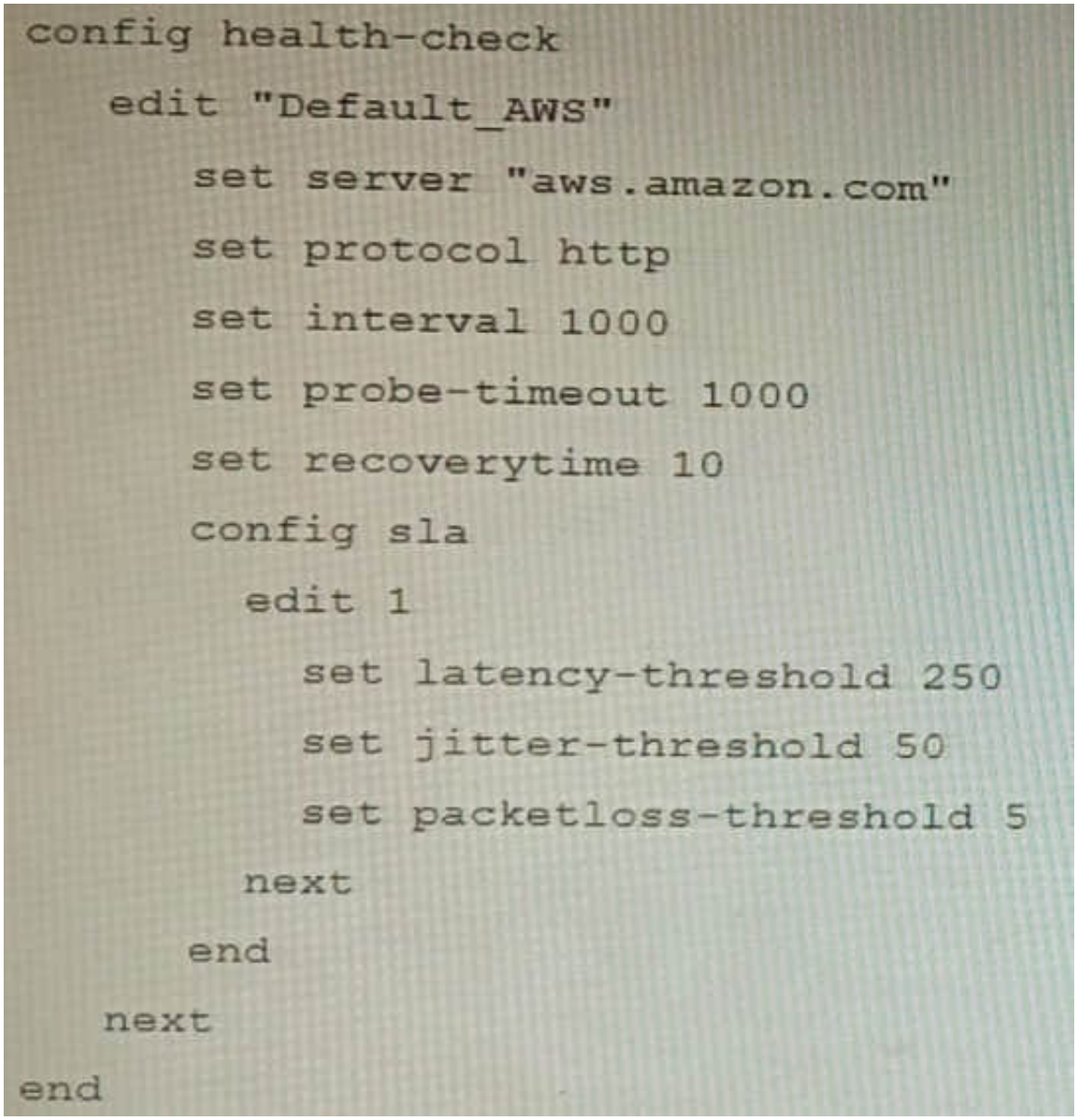
100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

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:



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

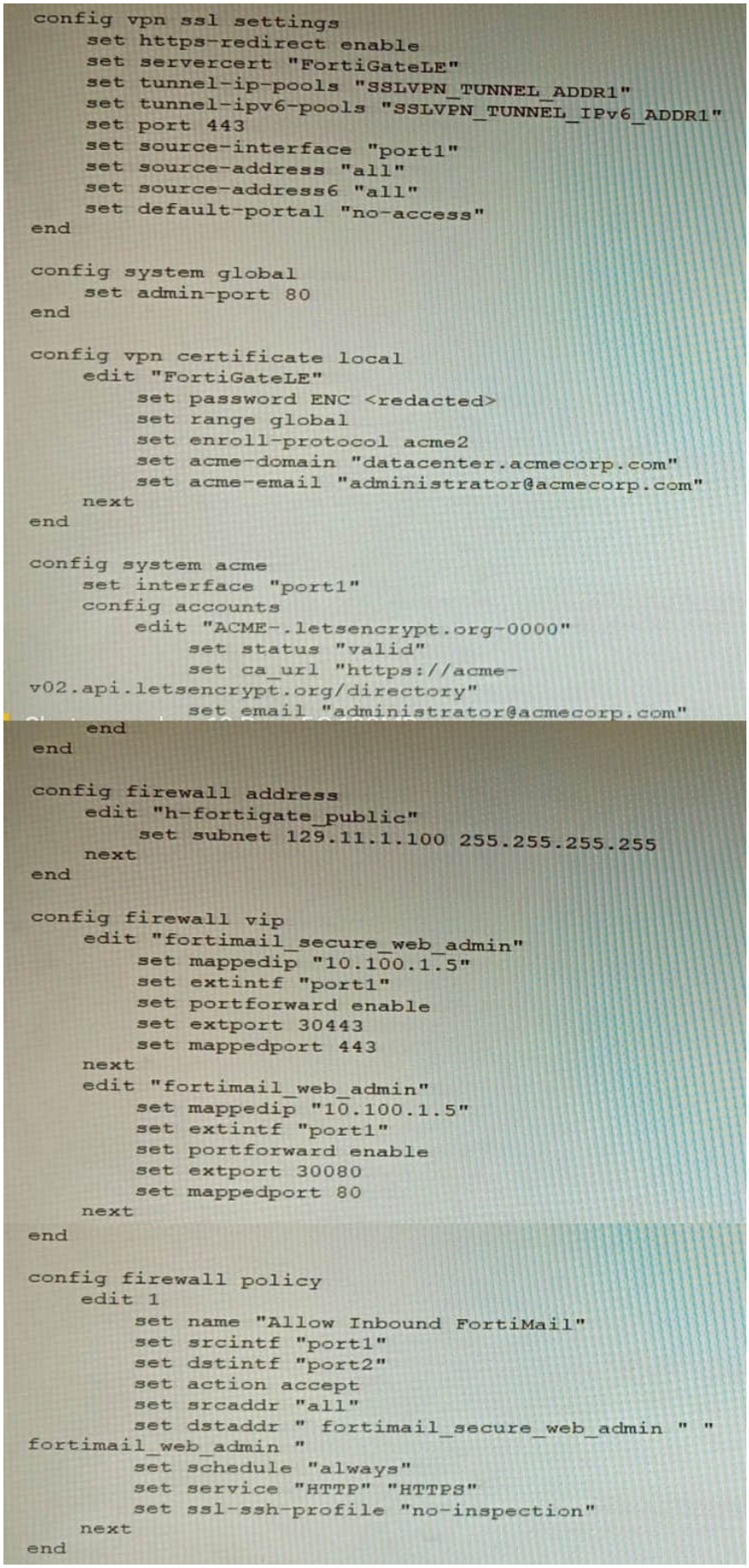
D. set members all

Correct Answer: A

Explanation: The set members any option will ensure that all of the SD-WAN interfaces are included in the Performance SLA. This is the best option if you want to be sure that the Performance SLA will be triggered even if more connections are added to the branch in the future. The set members 0 option will exclude all of the SD-WAN interfaces from the Performance SLA. This is not a good option because it will prevent the Performance SLA from being triggered even if there is a problem with the network. The current configuration already fulfills the requirement option is incorrect because it does not ensure that all of the SD-WAN interfaces will be included in the Performance SLA. The set members all option will include all of the SD-WAN interfaces in the Performance SLA, but it is not the best option because it is not scalable. If you have a large number of SD-WAN interfaces, this option will cause the Performance SLA to be triggered too often. References: Performance SLA | FortiGate / FortiOS 7.4.0 Configuring Performance SLA | FortiGate / FortiOS 7.4.0

QUESTION 2

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 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.

Correct Answer: AD

Explanation: A. The FortiMail access control rule to relay from Office 365 servers FQDN is missing.

If the access control rule to relay from Office 365 servers FQDN is missing, then FortiMail will not be able to send emails to Office 365. This is because the access control rule specifies which IP addresses or domains are allowed to relay

emails through FortiMail. D. A Mail Flow connector from the Exchange Admin Center has not been set properly to the FortiMail Cloud FQDN.

If the Mail Flow connector from the Exchange Admin Center is not set properly to the FortiMail Cloud FQDN, then Office 365 will not be able to send emails to FortiMail. This is because the Mail Flow connector specifies which SMTP server is

used to send emails to external recipients.

QUESTION 4

Refer to the exhibit.

You have deployed a security fabric with three FortiGate devices as shown in the exhibit. FGT_2 has the following configuration:

```
config system csf
set fabric-object-unification local
end
```

FGT_1 and FGT_3 are configured with the default setting. Which statement is true for the synchronization of fabric-objects?

A. Objects from the FortiGate FGT_2 will be synchronized to the upstream FortiGate.

B. Objects from the root FortiGate will only be synchronized to FGT__2.

C. Objects from the root FortiGate will not be synchronized to any downstream FortiGate.

D. Objects from the root FortiGate will only be synchronized to FGT_3.

Correct Answer: C

Explanation: The fabric-object-unification setting on FGT_2 is set to local, which means that objects will not be synchronized to any other FortiGate devices in the security fabric. The default setting for fabric-object-unification is default, which

means that objects will be synchronized from the root FortiGate to all downstream FortiGate devices. Since FGT_2 is not the root FortiGate and the fabric-object-unification setting is set to local, objects from the root FortiGate will not be

synchronized to FGT_2.

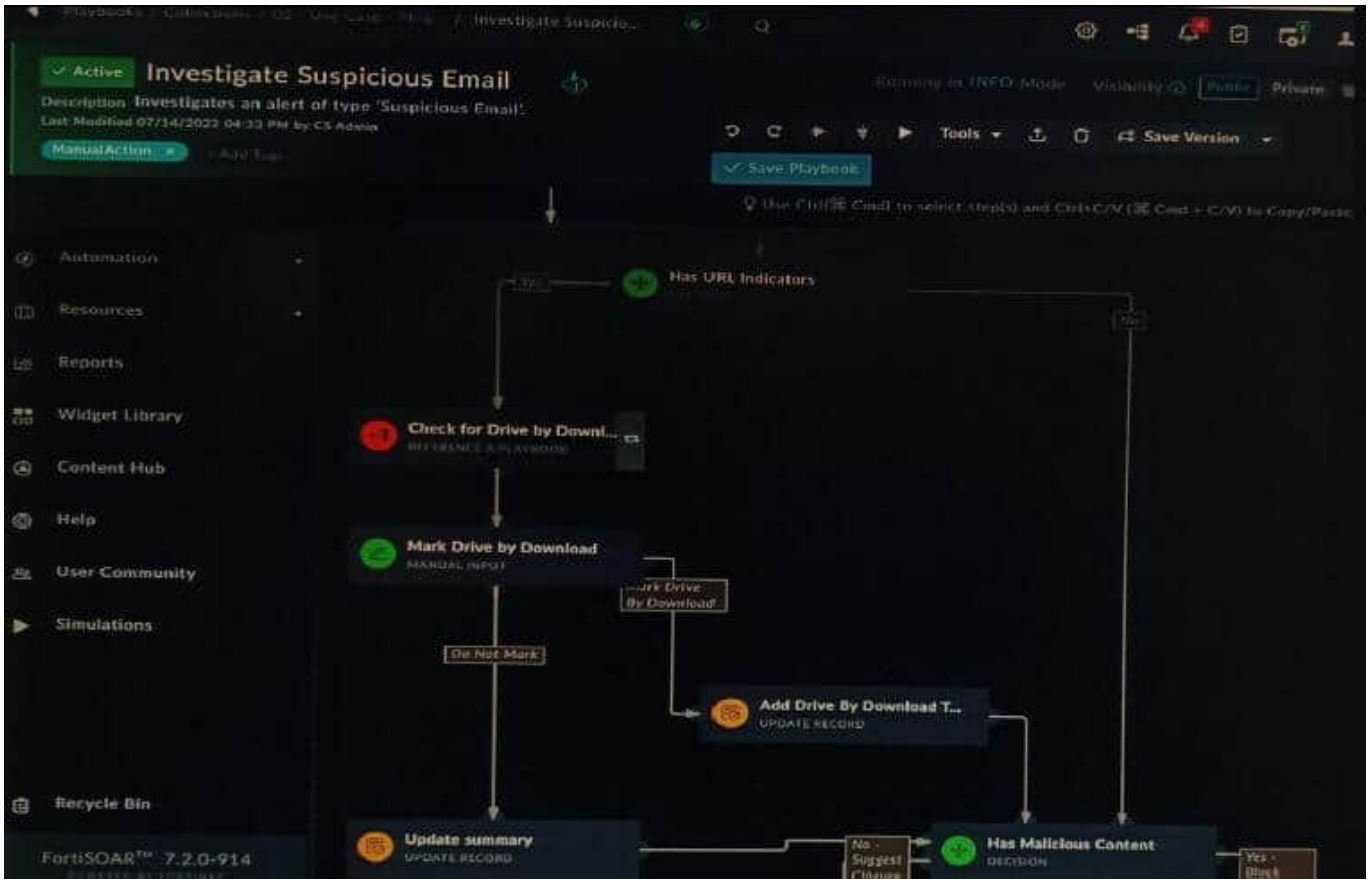
Reference:

Synchronizing objects across the Security Fabric:

https://docs.fortinet.com/document/fortigate/6.4.0/administration- guide/880913/synchronizing-objects-across-the-security-fabric

QUESTION 5

Refer to the exhibit showing a FortiSOAR playbook.



You are investigating a suspicious e-mail alert on FortiSOAR, and after reviewing the executed playbook, you can see that it requires intervention.

What should be your next step?

A. Go to the Incident Response tasks dashboard and run the pending actions

B. Click on the notification icon on FortiSOAR GUI and run the pending input action

C. Run the Mark Drive by Download playbook action

D. Reply to the e-mail with the requested Playbook action

Correct Answer: A

Explanation: The exhibited playbook requires intervention, which means that the playbook has reached a point where it needs a human operator to take action. The next step should be to go to the Incident Response tasks dashboard and run

the pending actions. This will allow you to see the pending actions that need to be taken and to take those actions. The other options are not correct. Option B will only show you the notification icon, but it will not allow you to run the pending

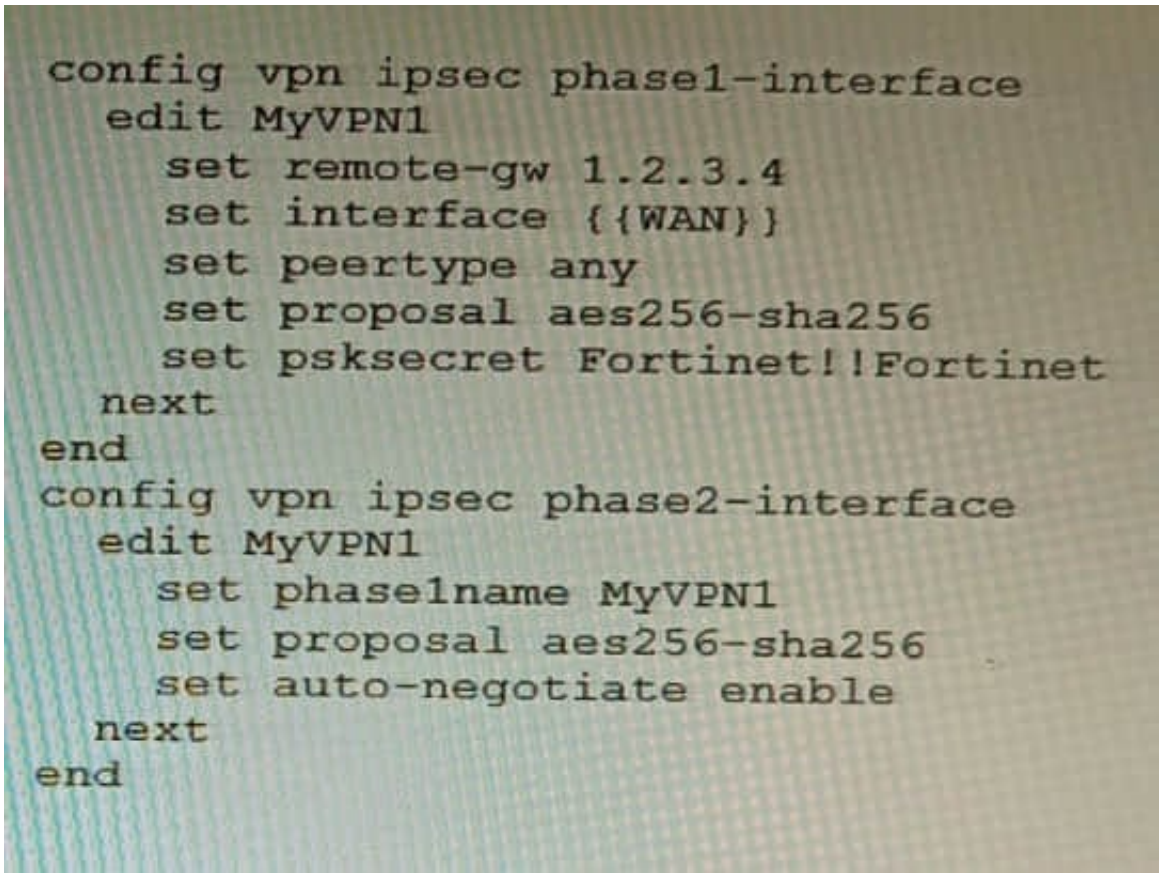
input action. Option C will run the Mark Drive by Download playbook action, but this is not the correct action to take in this case. Option D is not a valid option.

Here are some additional details about pending actions in FortiSOAR:

Pending actions are actions that need to be taken by a human operator. Pending actions are displayed in the Incident Response tasks dashboard. Pending actions can be run by clicking on the action in the dashboard.

QUESTION 6

Refer to the exhibit.



FortiManager is configured with the Jinja Script under CLI Templates shown in the exhibit.

Which two statements correctly describe the expected behavior when running this template? (Choose two.)

A. The Jinja template will automatically map the interface with "WAN" role on the managed FortiGate.

B. The template will work if you change the variable format to $(WAN).

C. The template will work if you change the variable format to {{ WAN }}.

D. The administrator must first manually map the interface for each device with a meta field.

E. The template will fail because this configuration can only be applied with a CLI or TCL script.

Correct Answer: DE

Explanation: D. The administrator must first manually map the interface for each device with a meta field.

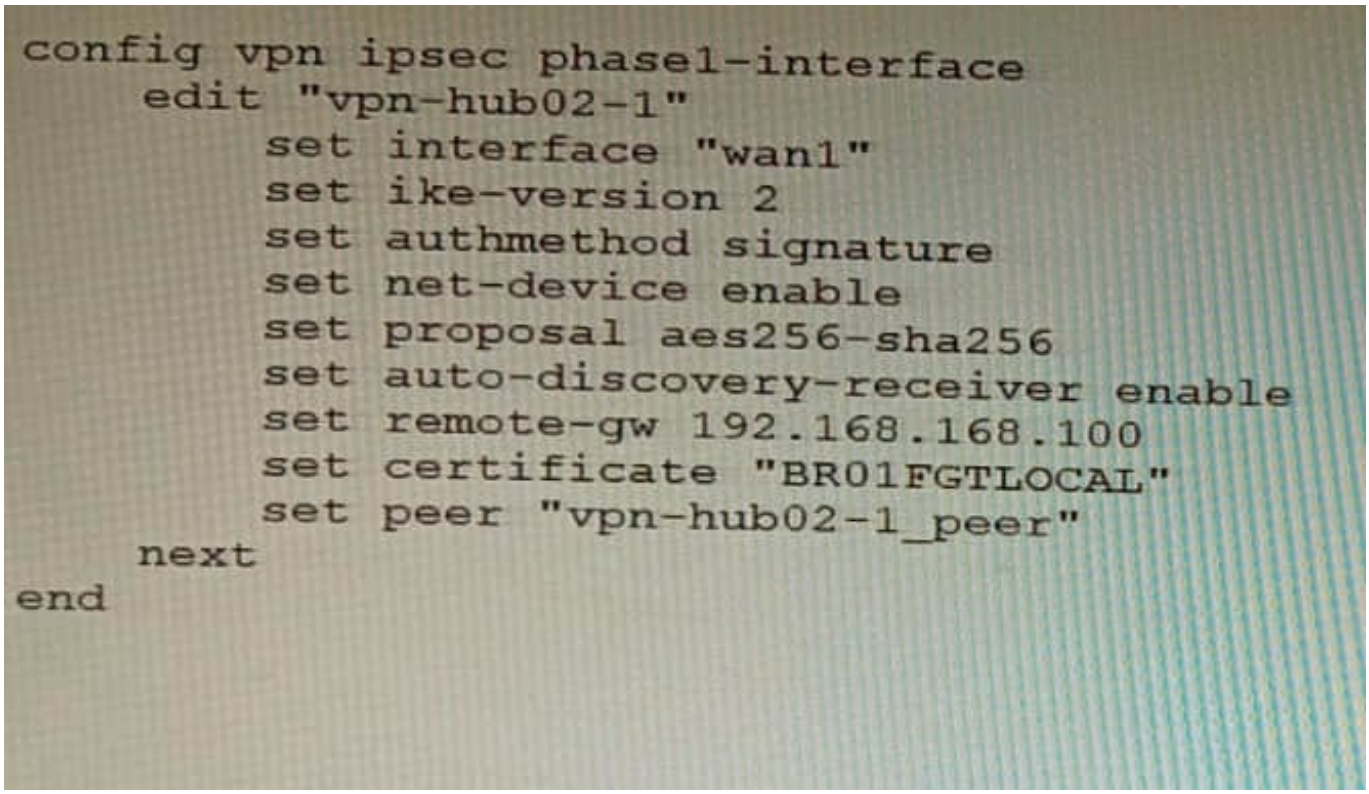
The Jinja template in the exhibit is expecting a meta field calledWANto be set on the managed FortiGate. This meta field will specify which interface on the FortiGate should be assigned the "WAN" role. If the meta field is not set, then the

template will fail. E. The template will fail because this configuration can only be applied with a CLI or TCL script.

The Jinja template in the exhibit is trying to configure the interface role on the managed FortiGate. This type of configuration can only be applied with a CLI or TCL script. The Jinja template will fail because it is not a valid CLI or TCL script.

QUESTION 7

Refer to the exhibit.



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.)

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

Correct Answer: BDE

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

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

E must 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 8

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 9

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

Correct Answer: BD

B is 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.

D is 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

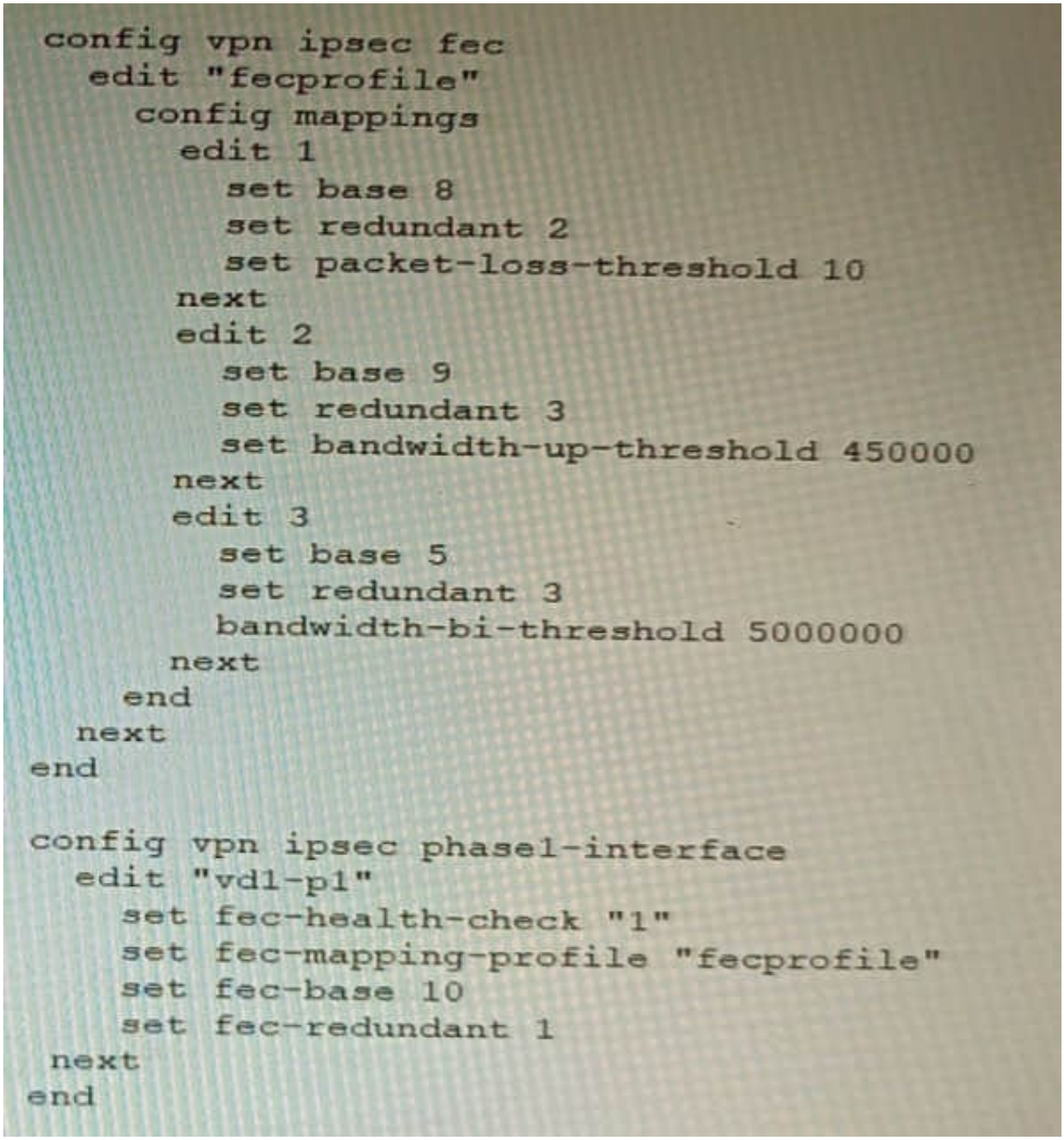
interfaces will not change the throughput capacity of the device.

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

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

Correct 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.

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