NSE8_810$^{Q\&As}$

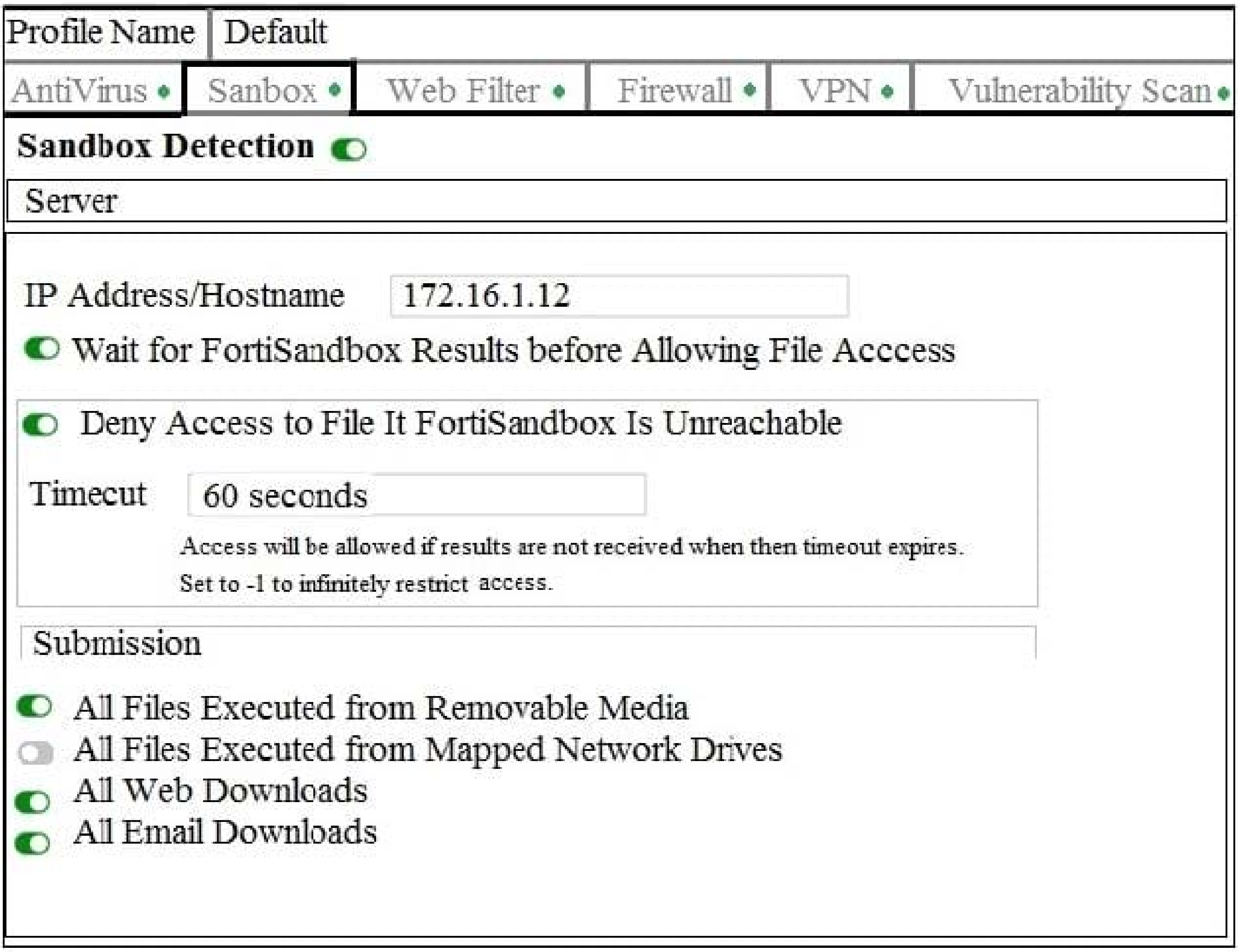
Fortinet Network Security Expert 8 Written Exam (810)

Pass Fortinet NSE8_810 Exam with 100% Guarantee

QUESTION 1

Exhibit

Click the Exhibit button. Referring to the exhibit, which two behaviors will the FortiClient endpoint have after receiving the profile update from the FortiClient EMS? (Choose two.)



Profile Name | Default

AntiVirus • | Sanbox • | Web Filter • | Firewall • | VPN • | Vulnerability Scan •

Sandbox Detection ●

Server

IP Address/Hostname: 172.16.1.12

● Wait for FortiSandbox Results before Allowing File Acccess

● Deny Access to File It FortiSandbox Is Unreachable

Timecut: 60 seconds

Access will be allowed if results are not received when then timeout expires. Set to -1 to infinitely restrict access.

Submission

● All Files Executed from Removable Media

○ All Files Executed from Mapped Network Drives

● All Web Downloads

● All Email Downloads

A. Files executed from a mapped network drive will not be inspected by the FortiCltent endpoint Antivirus engine.

B. The user will not be able to access a Web downloaded file for at least 60 seconds when the FortiSandbox is reachable.

C. The user will not be able to access a Web downloaded file for a maximum of 60 seconds if it is not a virus and the FortiSandbox s reachable.

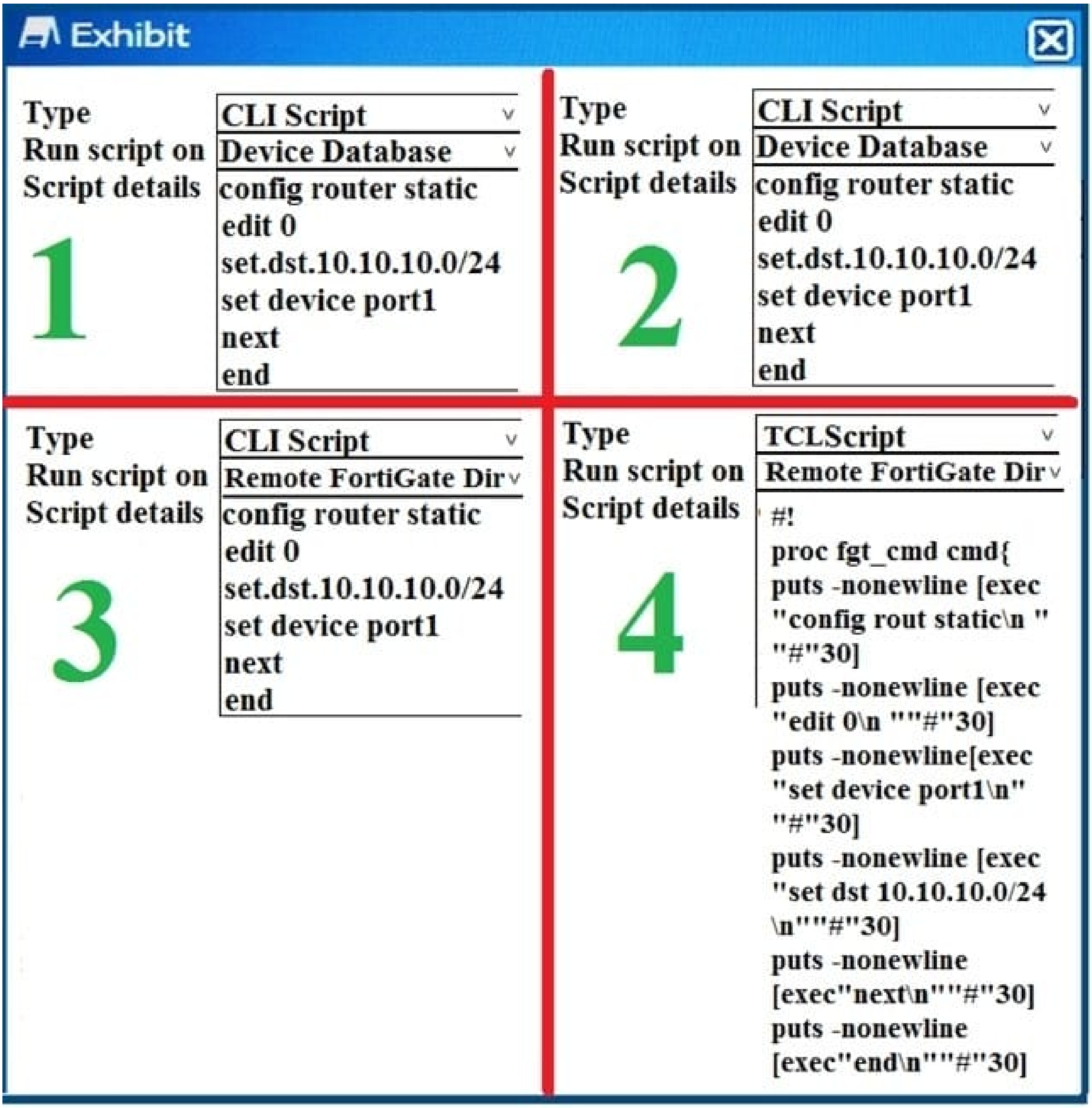
D. The user will not be able to access a Web downloaded file when the FortiSandbox is unreachable.

Correct Answer: AC

QUESTION 2

Refer to the Exhibit button.

You need to run a script in FortiManager against managed FortiGate devices in your organization to install a configuration for a new static route. Which two scripts will successfully configure the static route on the managed device? (Choose two.)



Exhibit

1

Type: CLI Script

Run script on: Device Database

Script details:

```
config router static
edit 0
set.dst.10.10.10.0/24
set device port1
next
end
```

2

Type: CLI Script

Run script on: Device Database

Script details:

```
config router static
edit 0
set.dst.10.10.10.0/24
set device port1
next
end
```

3

Type: CLI Script

Run script on: Remote FortiGate Dir

Script details:

```
config router static
edit 0
set.dst.10.10.10.0/24
set device port1
next
end
```

4

Type: TCLScript

Run script on: Remote FortiGate Dir

Script details:

```
#!
proc fgt_cmd cmd{
puts -nonewline [exec
"config rout static\n "
"#"30]
puts -nonewline [exec
"edit 0\n ""#"30]
puts -nonewline[exec
"set device port1\n"
"#"30]
puts -nonewline [exec
"set dst 10.10.10.0/24
\n""#"30]
puts -nonewline
[exec"next\n""#"30]
puts -nonewline
[exec"end\n""#"30]
```

A. Script 1

B. Script 2

C. Script 3

D. Script 4

Correct Answer: BC

QUESTION 3

You are asked to add a FortiDDoS to the network to combat detected slow connection attacks such as Slowloris.

Which prevention mode on FortiDDoS will protect you against this specific type of attack?

A. aggressive aging mode

B. rate limiting mode

C. blocking mode

D. asymmetric mode

Correct Answer: A

QUESTION 4

Click the Exhibit button.

```
config system ha

set mode a-a

set group-id 1

set group-name main

set hb_dev port2 100

set session-pickup enable

end
```

You have configured an HA cluster with two FortiGates. You want to make sure that you are able to

manage the individual cluster members directly using port3.

Referring to the exhibit, what are two ways to accomplish this task? (Choose two.)

A. Disable the sync feature on porl3: then configure specific IPs for ports on both cluster members.

B. Configure port3 to be a dedicated HA management interface, then configure specific IPs for port3 on both cluster members.

C. Create a management VDOM and Disable the HA synchronization for this VDOM, assign ports to this VDOM, then configure specific IPs for ports on both cluster member.

D. Allow administrative access in the HA heartbeat interfaces.

Correct Answer: BC

QUESTION 5

FortiMail configured with the protected domain "internal lab".

Which two envelopes addresses will need an access control rule to relay e-mail sent for unauthenticated users? (Choose two.)

A. MAIL FROM: traming@fortinet com: RCPT TO: student@fortmet com

B. MAIL FROM student@fortinet com: RCPT TO student@internal.lab

C. MAIL FROM: trainmg@internallab; RCPT TO student@mternallab

D. MAIL FROM student@internal lab: RCPT TO student@fortmet.com

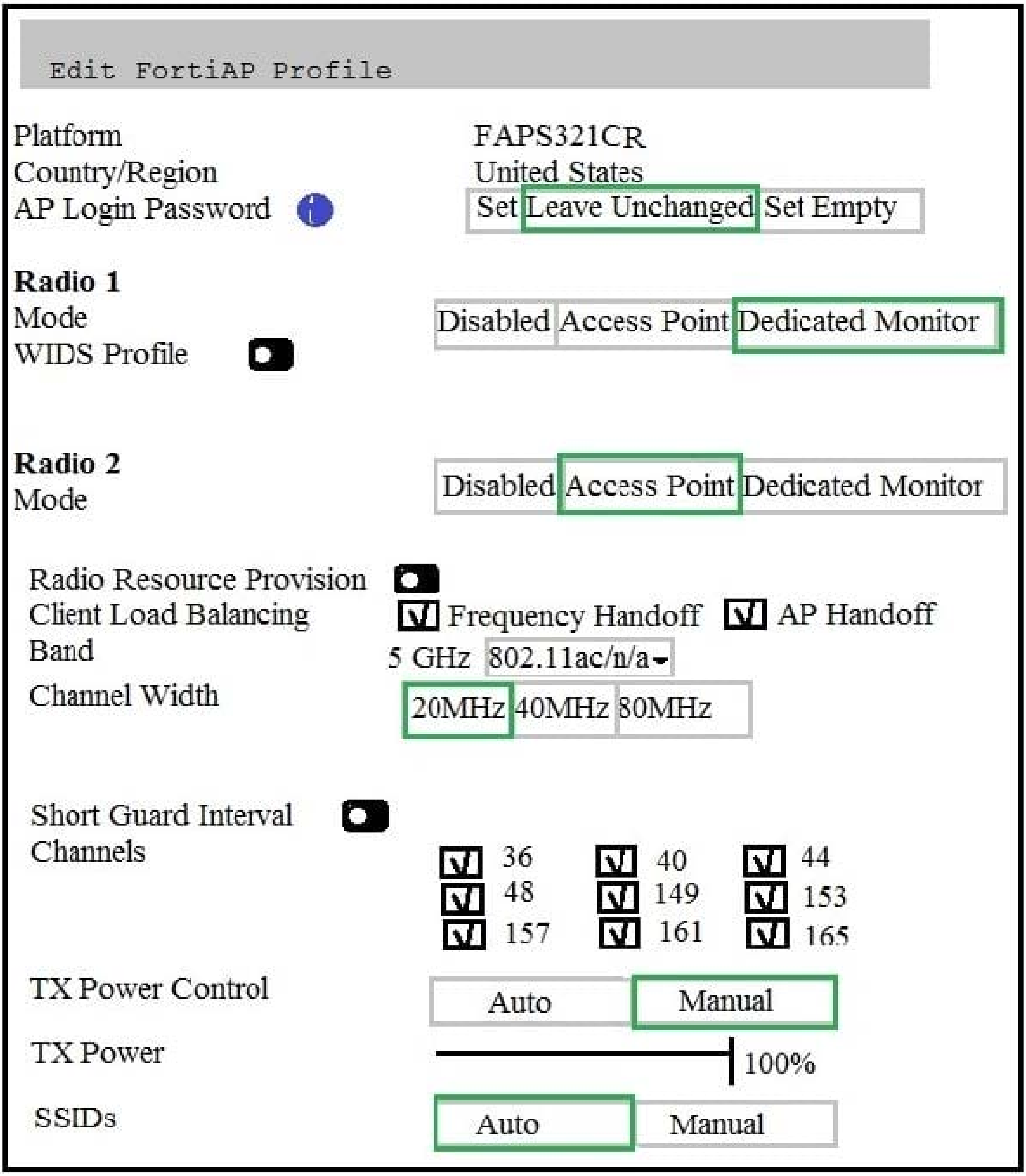
Correct Answer: BC

QUESTION 6

Click the Exhibit button.

The FortiAP profile used by the FortiGate managed AP is shown in the exhibit.

Which two statements are correct in this scenario? (Choose two.)



Edit FortiAP Profile

Platform FAPS321CR

Country/Region United States

AP Login Password ⓘ Set [✓ Leave Unchanged] Set Empty

Radio 1

Mode Disabled Access Point [✓ Dedicated Monitor]

WIDS Profile ●

Radio 2

Mode Disabled [✓ Access Point] Dedicated Monitor

Radio Resource Provision ●

Client Load Balancing ☑ Frequency Handoff ☑ AP Handoff

Band 5 GHz 802.11ac/n/a▾

Channel Width [✓ 20MHz] 40MHz 80MHz

Short Guard Interval ●

Channels

☑ 36	☑ 40	☑ 44
☑ 48	☑ 149	☑ 153
☑ 157	☑ 161	☑ 165

TX Power Control Auto [✓ Manual]

TX Power 100%

SSIDs [✓ Auto] Manual

A. All FortiAPs using thre profile will nave Radio 1 scan rogue access points.

B. Map this profile to SSIDs that you want to be available on the FortiAPs using this profile.

C. All FortiAPs using this profile will have Radio 1 monitor wireless clients.

D. Interference will be prevented between FortiAPs using this profile.

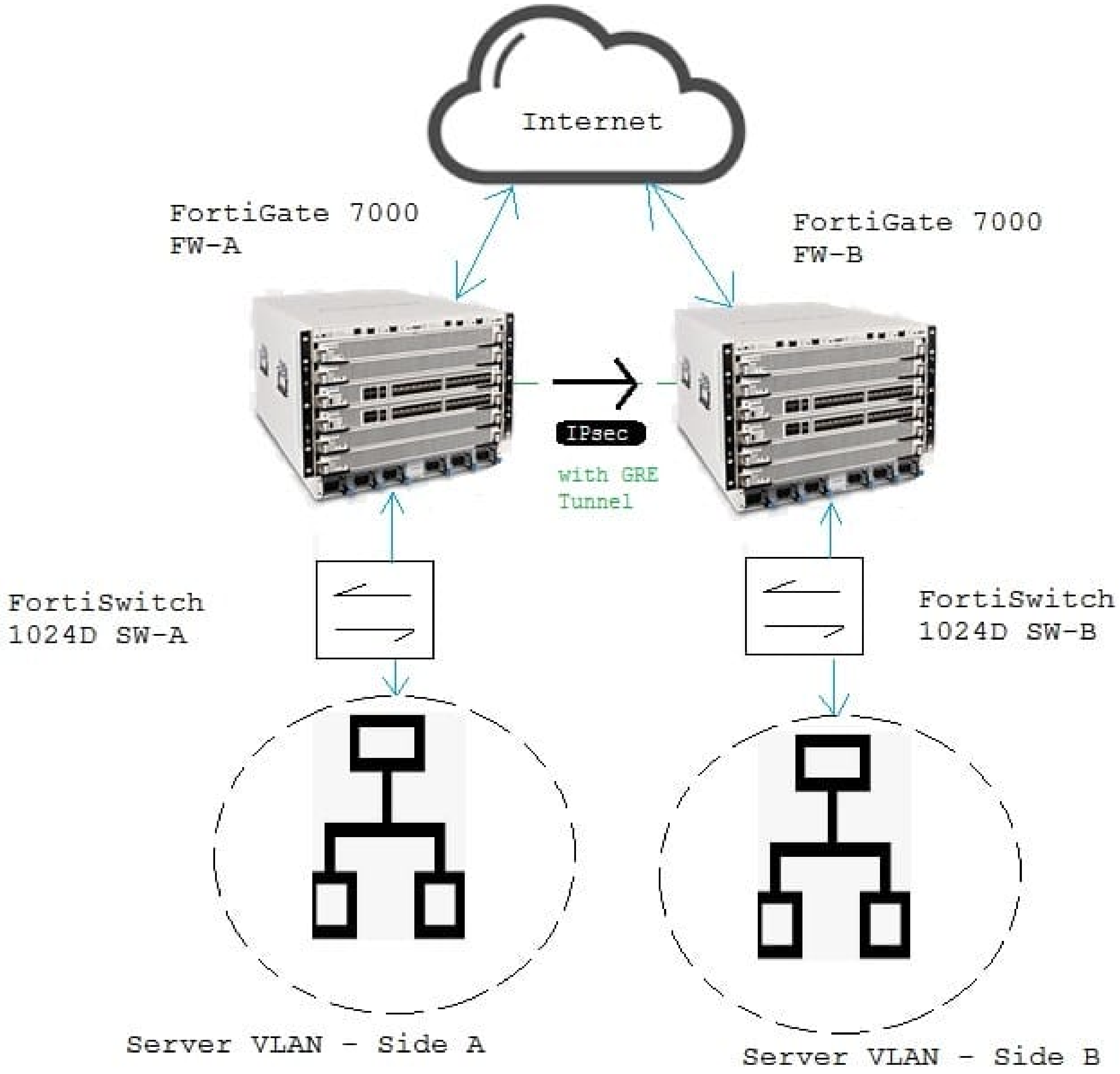
Correct Answer: AD

QUESTION 7

Click the Exhibit button.

You have two data centers a FortiGate 7000-series chassis connected by VPN, and all traffic flows over an established generic routing encapsulation (GRE) tunnel between them.

You are troubleshooting traffic that is traversing between Server VLAN A and Server VLAN B. The performance is lower than expected and all traffic is only on the FPM module in slot 3.



Referring to the exhibit, which action will correct the problem?

A. Referring to the exhibit, which action will correct the problem?

B. NO course of action enables load balancing in this scenario.

C. Change the algorithm so it takes IP source IP, destination IP, and port no account.

D. Configuration a local-balance flow-rule in the CLI to enable load balancing.

Correct Answer: C

QUESTION 8

You have a customer experiencing problem with a legacy L3L4 firewall device and IPV6 SIP VoIP traffic. They devices is dropping SIP packets, consequently, it process SIP voice calls. Which solution would solve the customer\\'s problem?

A. Deploy a FortiVoice and enable IPv6 SIP.

B. Replace their legacy device with a FortiGate and configure it to extract information from the body of the IPv6 packet.

C. Deploy a FotiVoice and enable an IPv6 SIP session helper.

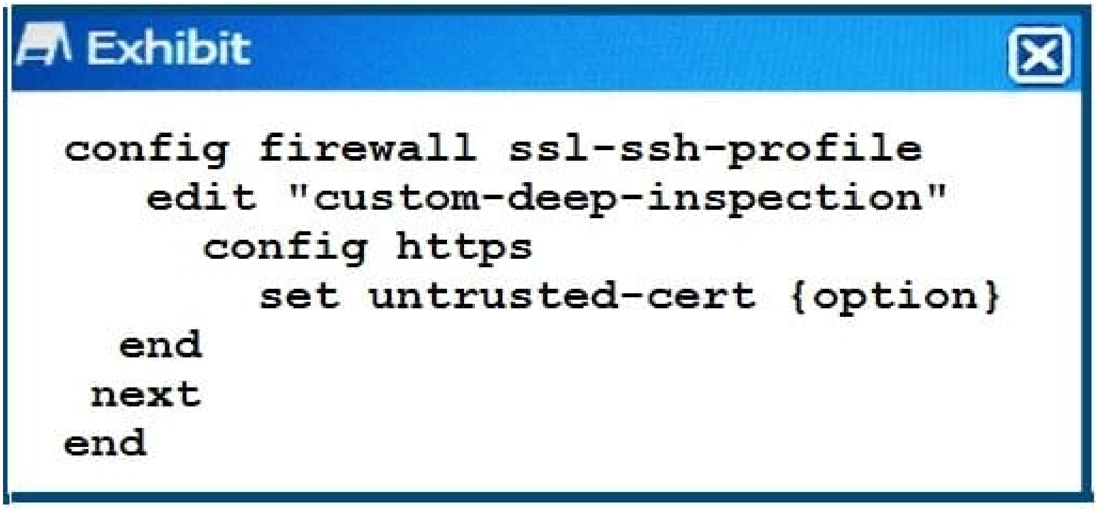
D. Replace their legacy device with a FortiGate and deploy a FortiVoice to extract information from the body of the IPv6 SIP packet

Correct Answer: D

QUESTION 9

Click the Exhibit button.

Referring to the exhibit, which command-line option for deep inspection SSL would have the FortiGate resign all untrusted self-signed certificates with the trusted Fortinet_CA_SSL certificate?



```
config firewall ssl-ssh-profile
   edit "custom-deep-inspection"
     config https
       set untrusted-cert {option}
  end
 next
end
```

A. allow

B. block

C. ignore

D. inspect

Correct Answer: A

QUESTION 10

You have deployed a FortiGate In NAT/Route mode as a secure as a web gateway with a few P-base authentication firewall policies. Your customer reports that some users now have different browsing permission =s from what is expected. All these users are browsing using internet Explorer through Desktop Connection to a Terminal Server. When you took at the Fortigate logs the username for the Terminal Server IP is not consistent.

Which action will correct this problem?

A. Make sure Terminal Service is using the correct DNS ever.

B. Configure FSSO Advanced with LDAP integration

C. Change the FSSO polling mode to windows NetAPI

D. Install the TSCitrix on the terminal server

Correct Answer: B