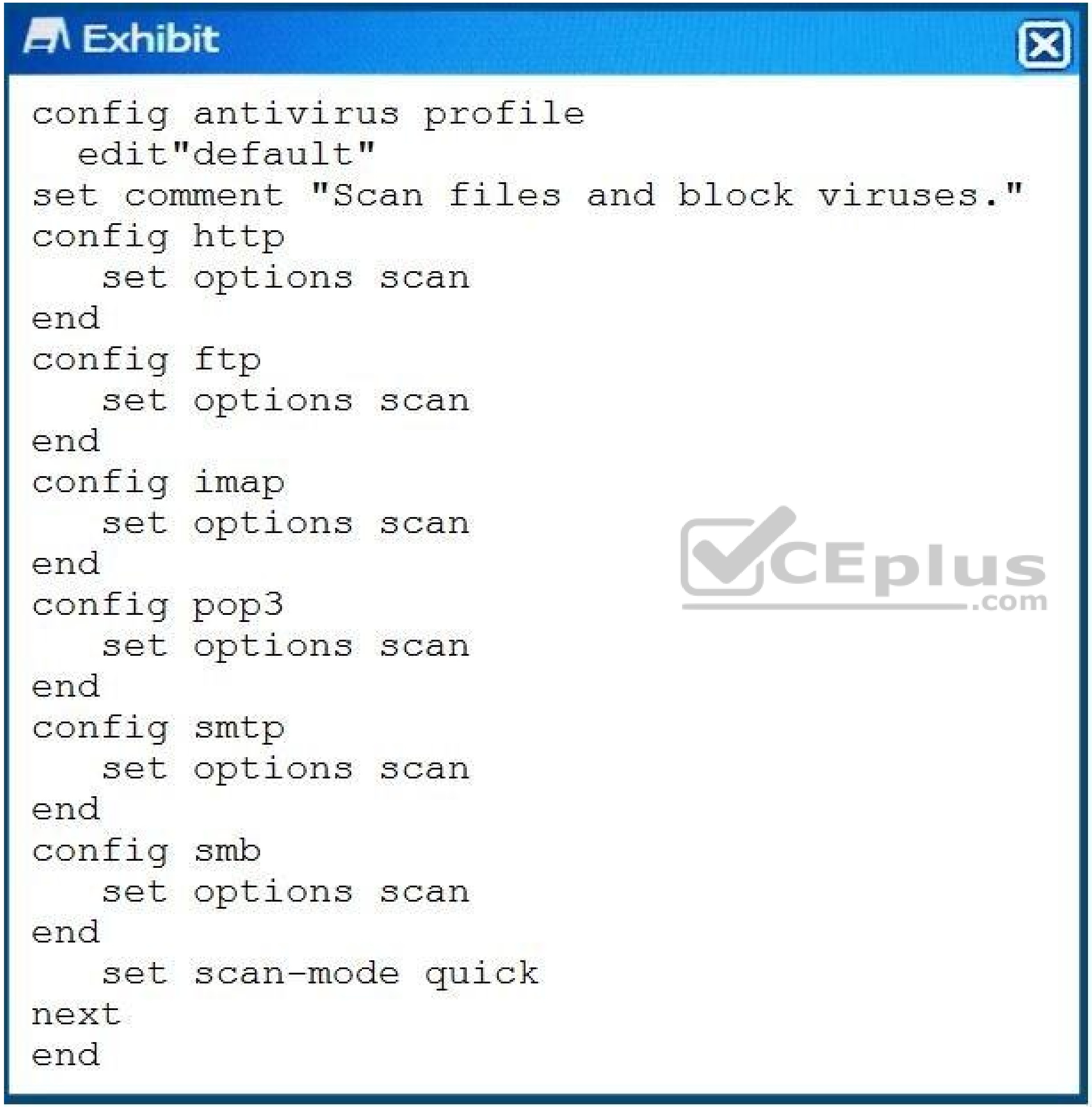
Fortinet.Premium.NSE8_810.by.VCEplus.60q

Number: NSE8_810 VCEplus
Passing Score: 800
Time Limit: 120 min
File Version: 1.3

Exam Code: NSE8_810
Exam Name: Fortinet Network Security Expert 8 Written Exam (NSE8 810 - FortiOS 5.6)
Certification Provider: Fortinet
Corresponding Certification: NSE8

QUESTION 1
Click the Exhibit button.



```
config antivirus profile
  edit"default"
set comment "Scan files and block viruses."
config http
   set options scan
end
config ftp
   set options scan
end
config imap
   set options scan
end
config pop3
   set options scan
end
config smtp
   set options scan
end
config smb
   set options scan
end
   set scan-mode quick
next
end
```

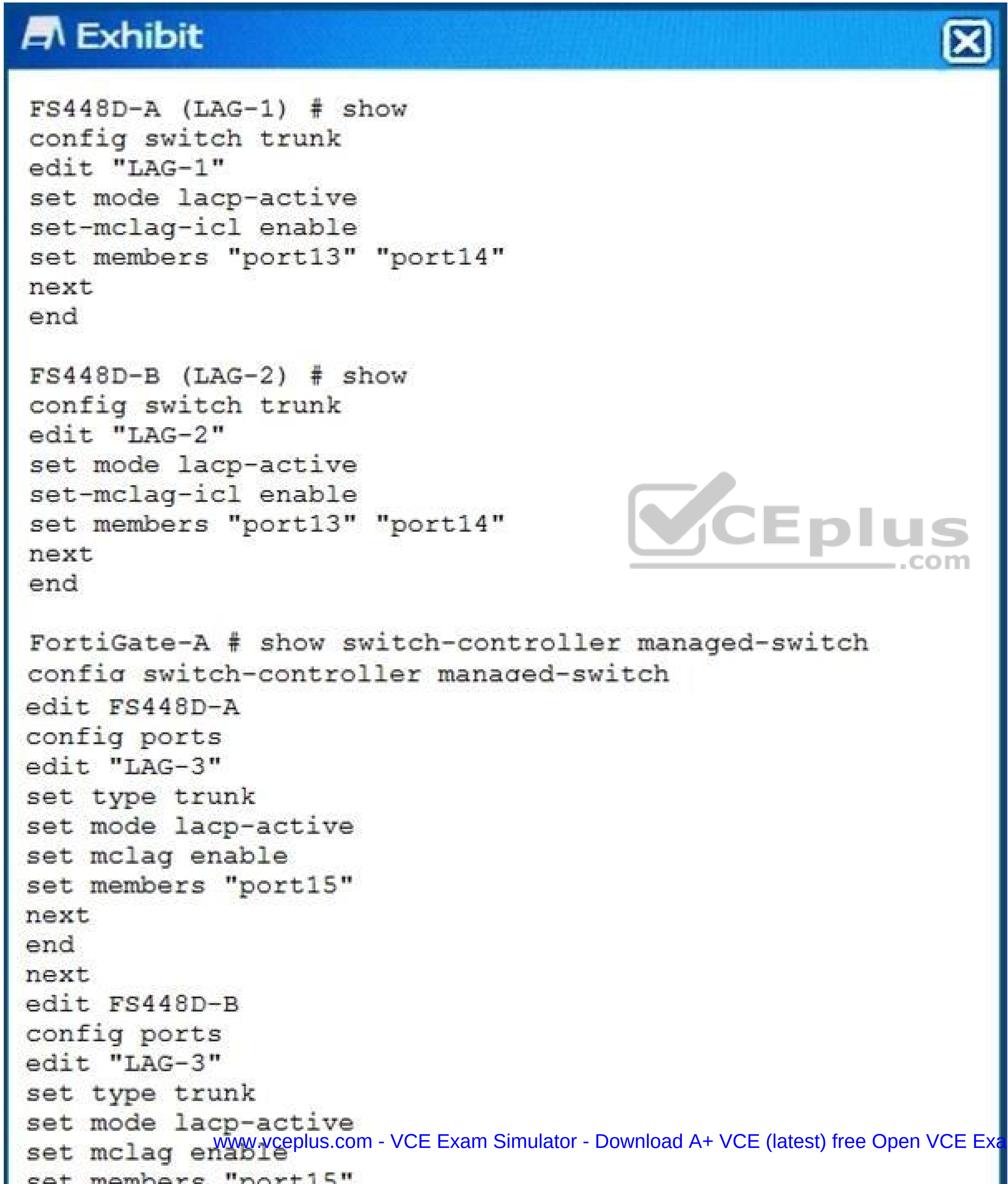
You are working on an entry level model FortiGate that has been configured in flow-based inspection mode with various settings optimized for performance. It appears that the main Internet firewall policy is using the antivirus profile labelled default. Your customer has found that some virus samples are not being caught by the FortiGate.
Referring to the exhibit, what is causing the problem?

A. The set default-db configuration was set to extreme.
B. The set options scan configuration items should have been changed to set options scan avmonitor.
C. The default AV profile was modified to use quick scan-mode.
D. The mobile-malware-db configuration was set to enable.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
Click the Exhibit button.



```
FS448D-A (LAG-1) # show
config switch trunk
edit "LAG-1"
set mode lacp-active
set-mclag-icl enable
set members "port13" "port14"
next
end

FS448D-B (LAG-2) # show
config switch trunk
edit "LAG-2"
set mode lacp-active
set-mclag-icl enable
set members "port13" "port14"
next
end

FortiGate-A # show switch-controller managed-switch
config switch-controller managed-switch
edit FS448D-A
config ports
edit "LAG-3"
set type trunk
set mode lacp-active
set mclag enable
set members "port15"
next
end
next
edit FS448D-B
config ports
edit "LAG-3"
set type trunk
set mode lacp-active
set mclag enable
set members "port15"
```

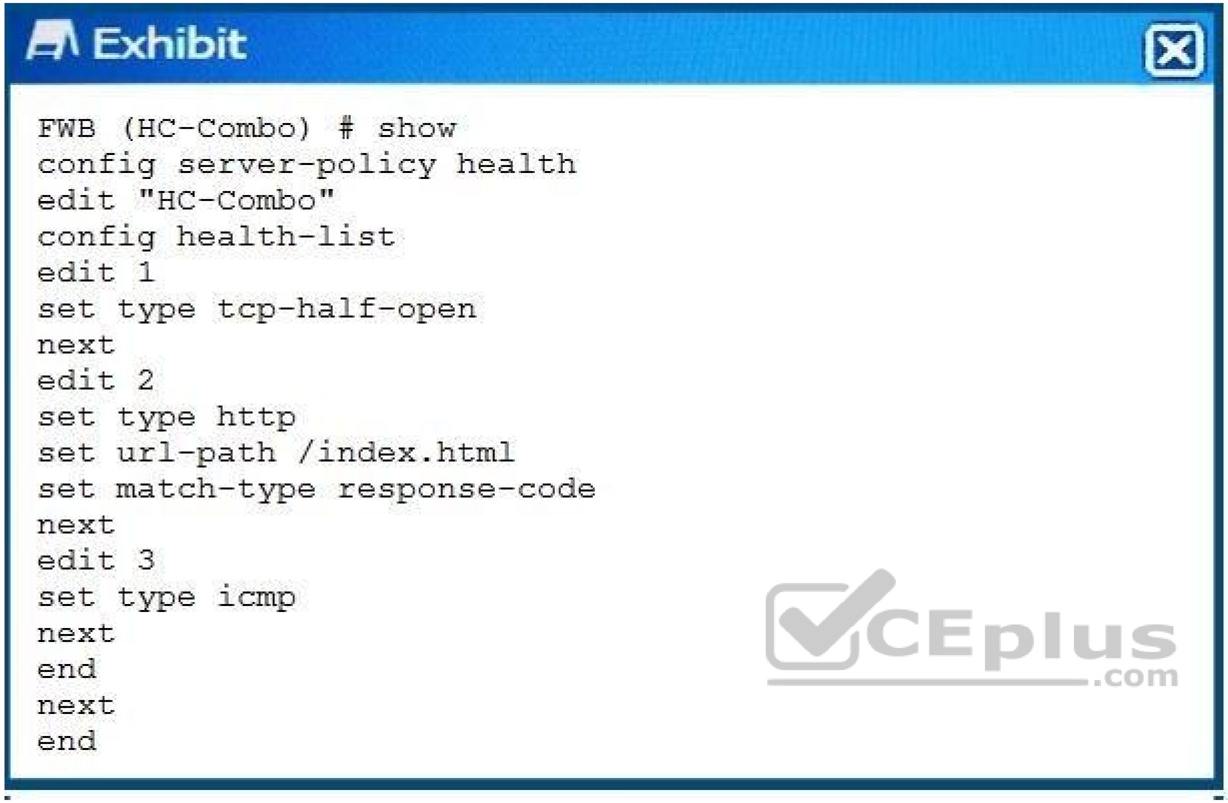
Referring to the exhibit, which two statements are true? (Choose two.)

A. port13 and port14 on FS448D-A should be connected to port13 and port14 on FS448D-B.
B. LAG-1 and LAG-2 should be connected to a single 4-port 802.3ad interface on the FortiGate-A.
C. LAG-3 on switches on FS448D-A and FS448D-B may be connected to a single 802.3ad trunk on another device.
D. LAG-1 and LAG-2 should be connected to a 4-port single 802.3ad trunk on another device.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
Click the Exhibit button.



```
FWB (HC-Combo) # show
config server-policy health
edit "HC-Combo"
config health-list
edit 1
set type tcp-half-open
next
edit 2
set type http
set url-path /index.html
set match-type response-code
next
edit 3
set type icmp
next
end
next
end
```

You created a custom health-check for your FortiWeb deployment.
Referring to the output shown in the exhibit, which statement is true?

A. The FortiWeb must receive an RST packet from the server.
B. The FortiWeb must receive an HTTP 200 response code from the server.
C. The FortiWeb must receive an ICMP Echo Request from the server.
D. The FortiWeb must match the hash value of the page index html.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4

A company has just deployed a new FortiMail in gateway mode. The administrator is asked to strengthen e-mail protection by applying the policies shown below.
-E-mail can only be accepted if a valid e-mail account exists.
-Only authenticated users can send e-mails out.
Which two actions will satisfy the requirements? (Choose two.)

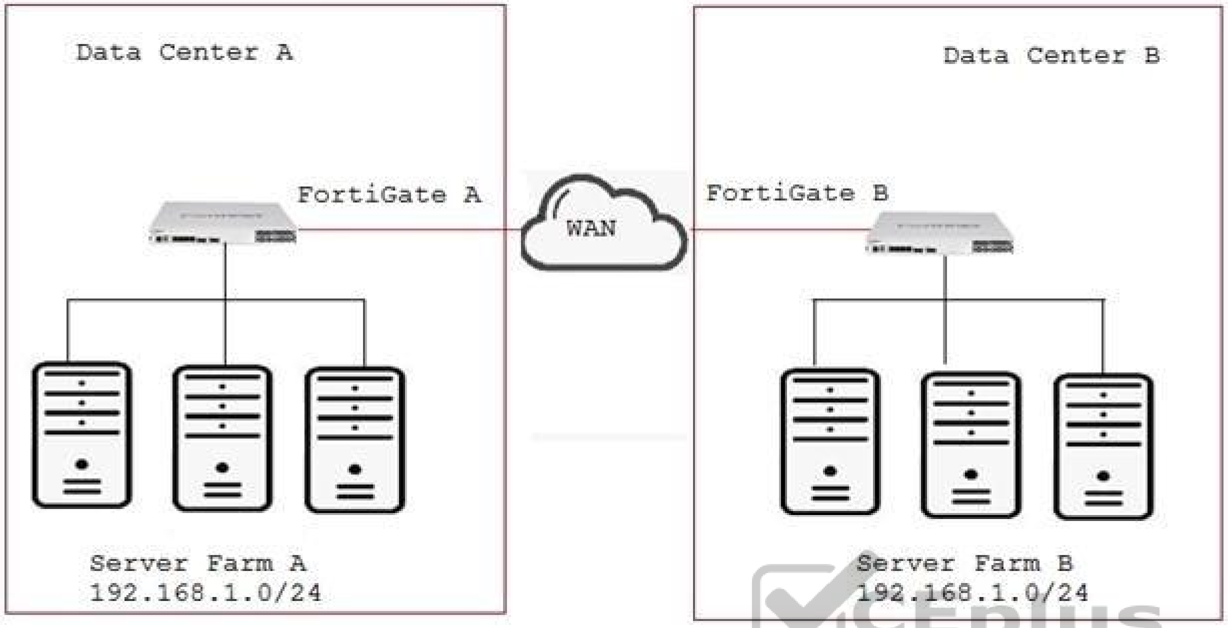
A. Configure recipient address verification.
B. Configure inbound recipient policies.
C. Configure outbound recipient policies.
D. Configure access control rules.

Correct Answer: DA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5

Click the Exhibit button.



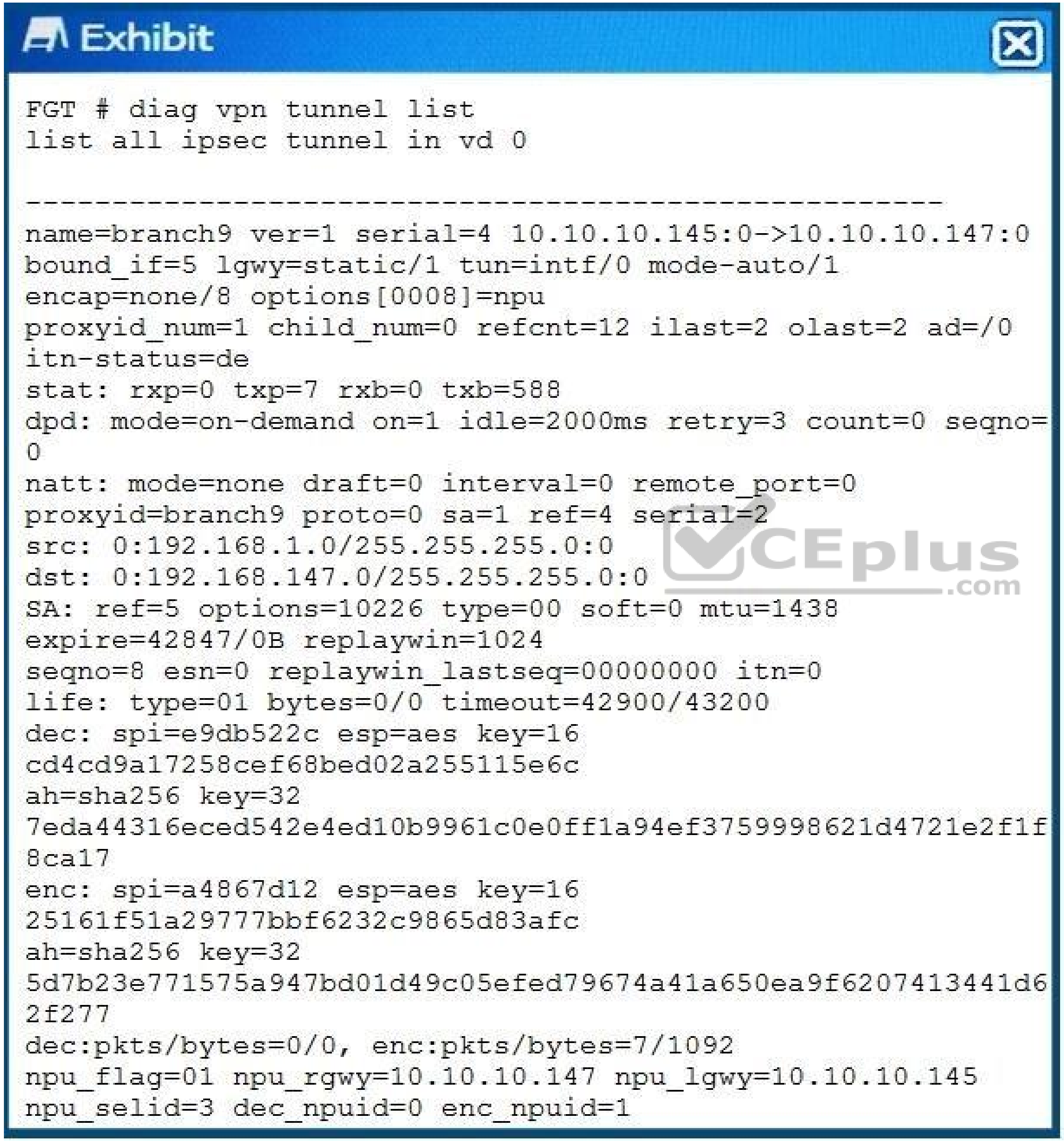
Your company has two data centers (DC) connected using a Layer 3 network. Servers in farm A need to connect to servers in farm B as though they all were in the same Layer 2 segment. What would be configured on the FortiGates on each DC to allow such connectivity?

A. Create an IPsec tunnel with transport-mode encapsulation.
B. Create an IPsec tunnel with tunnel-mode encapsulation.
C. Create an IPsec tunnel with VXLAN encapsulation.
D. Create an IPsec tunnel with VLAN encapsulation.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
Click the Exhibit button.



```
FGT # diag vpn tunnel list
list all ipsec tunnel in vd 0

------------------------------------------------------
name=branch9 ver=1 serial=4 10.10.10.145:0->10.10.10.147:0
bound_if=5 lgwy=static/1 tun=intf/0 mode-auto/1
encap=none/8 options[0008]=npu
proxyid_num=1 child_num=0 refcnt=12 ilast=2 olast=2 ad=/0
itn-status=de
stat: rxp=0 txp=7 rxb=0 txb=588
dpd: mode=on-demand on=1 idle=2000ms retry=3 count=0 seqno=
0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=branch9 proto=0 sa=1 ref=4 serial=2
src: 0:192.168.1.0/255.255.255.0:0
dst: 0:192.168.147.0/255.255.255.0:0
SA: ref=5 options=10226 type=00 soft=0 mtu=1438
expire=42847/0B replaywin=1024
seqno=8 esn=0 replaywin_lastseq=00000000 itn=0
life: type=01 bytes=0/0 timeout=42900/43200
dec: spi=e9db522c esp=aes key=16
cd4cd9a17258cef68bed02a255115e6c
ah=sha256 key=32
7eda44316eced542e4ed10b9961c0e0ff1a94ef3759998621d4721e2f1f
8ca17
enc: spi=a4867d12 esp=aes key=16
25161f51a29777bbf6232c9865d83afc
ah=sha256 key=32
5d7b23e771575a947bd01d49c05efed79674a41a650ea9f6207413441d6
2f277
dec:pkts/bytes=0/0, enc:pkts/bytes=7/1092
npu_flag=01 npu_rgwy=10.10.10.147 npu_lgwy=10.10.10.145
npu_selid=3 dec_npuid=0 enc_npuid=1
```

You configured an IPsec tunnel to a branch office. Now you want to make sure that the encryption of the tunnel is offloaded to hardware.
Referring to the exhibit, which statement is true?

A. Incoming and outgoing traffic is offloaded.
B. Outgoing traffic is offloaded; you cannot determine if incoming traffic is offloaded at this time.
C. Traffic is not offloaded.
D. Outgoing traffic is offloaded; incoming traffic not offloaded.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
You want to access the JSON API on FortiManager to retrieve information on an object. In this scenario, which two methods will satisfy the requirement? (Choose two.)

A. Make a call with the Web browser on your workstation.
B. Make a call with the SoapUPI API tool on your workstation.
C. Download the WSDL file from FortiManager administration GUI.
D. Make a call with the curl utility on your workstation.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
You have a customer with a SCADA environmental control device that is triggering a false-positive IPS alert whenever the device's Web GUI is accessed. You cannot seem to create a functional custom IPS filter to exempt this behavior, and it appears that the device is so old that it does not have HTTPS support.
You need to prevent the false positive IPS alerts from occuring.
In this scenario, which two actions would accomplish this task? (Choose two.)

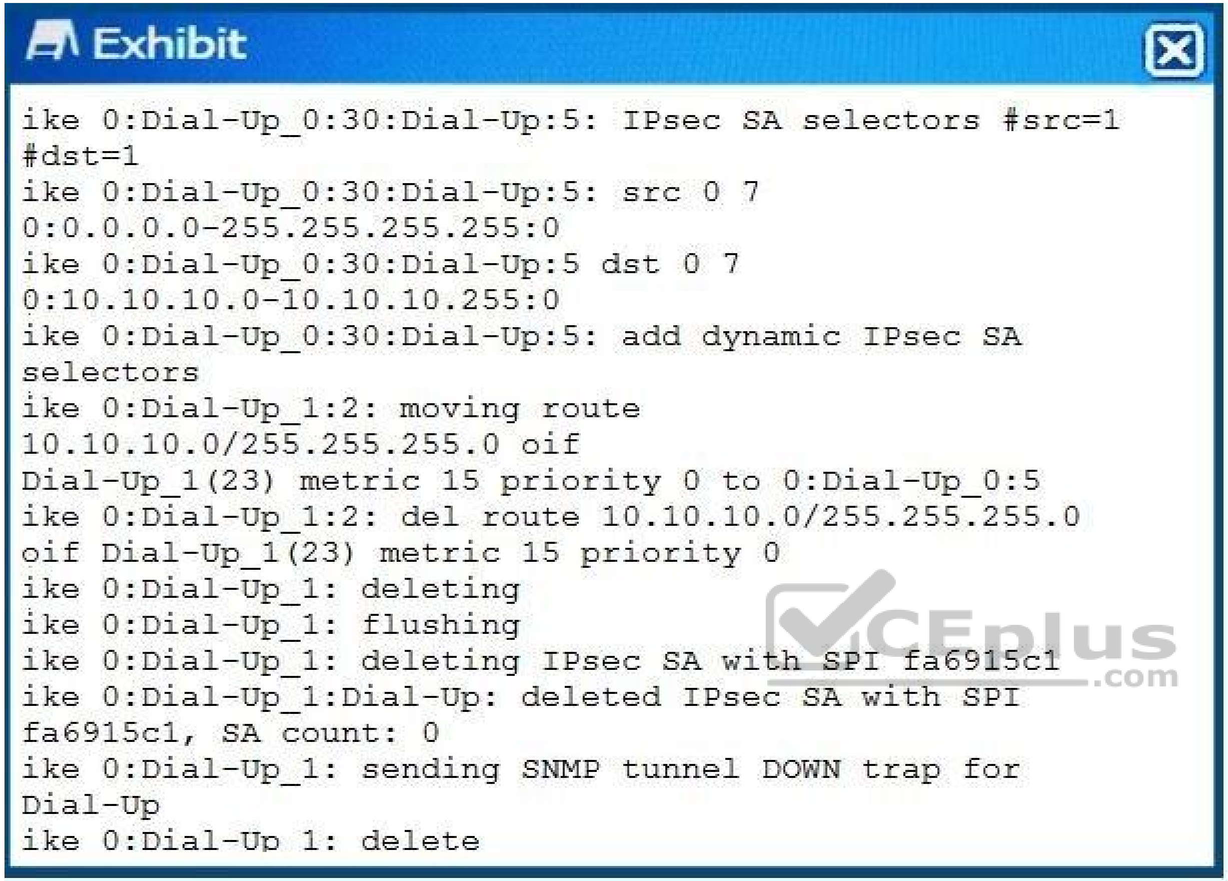
A. Create a very granular firewall policy for that device's IP address which does not perform IPS scanning.

B. Reconfigure the FortiGate to operate in proxy-based inspection mode instead of flow-based.
C. Create a URL filter with the Exempt action for that device's IP address.
D. Change the relevant firewall policies to use SSL certificate-inspection instead of SSL deep-inspection.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
Click the Exhibit button.



```
ike 0:Dial-Up_0:30:Dial-Up:5: IPsec SA selectors #src=1
#dst=1
ike 0:Dial-Up_0:30:Dial-Up:5: src 0 7
0:0.0.0.0-255.255.255.255:0
ike 0:Dial-Up_0:30:Dial-Up:5 dst 0 7
0:10.10.10.0-10.10.10.255:0
ike 0:Dial-Up_0:30:Dial-Up:5: add dynamic IPsec SA
selectors
ike 0:Dial-Up_1:2: moving route
10.10.10.0/255.255.255.0 oif
Dial-Up_1(23) metric 15 priority 0 to 0:Dial-Up_0:5
ike 0:Dial-Up_1:2: del route 10.10.10.0/255.255.255.0
oif Dial-Up_1(23) metric 15 priority 0
ike 0:Dial-Up_1: deleting
ike 0:Dial-Up_1: flushing
ike 0:Dial-Up_1: deleting IPsec SA with SPI fa6915c1
ike 0:Dial-Up_1:Dial-Up: deleted IPsec SA with SPI
fa6915c1, SA count: 0
ike 0:Dial-Up_1: sending SNMP tunnel DOWN trap for
Dial-Up
ike 0:Dial-Up_1: delete
```

A FortiGate is configured for a dial-up IPsec VPN to allow multiple remote FortiGates to connect to it.
However, FortiGates A and B have problems connecting to the VPN. Only one of them can be connected at a time. If site B tries to connect white site A is connected, site A is disconnected. The IKE real time debug shows the output in the exhibit when site A is disconnected.
Which configuration setting should be executed in the dial-up configuration to allow both VPNs to be connected at the same time?

A. set enforce-unique-id disable

B. set add-route enable

C. set single-source disable

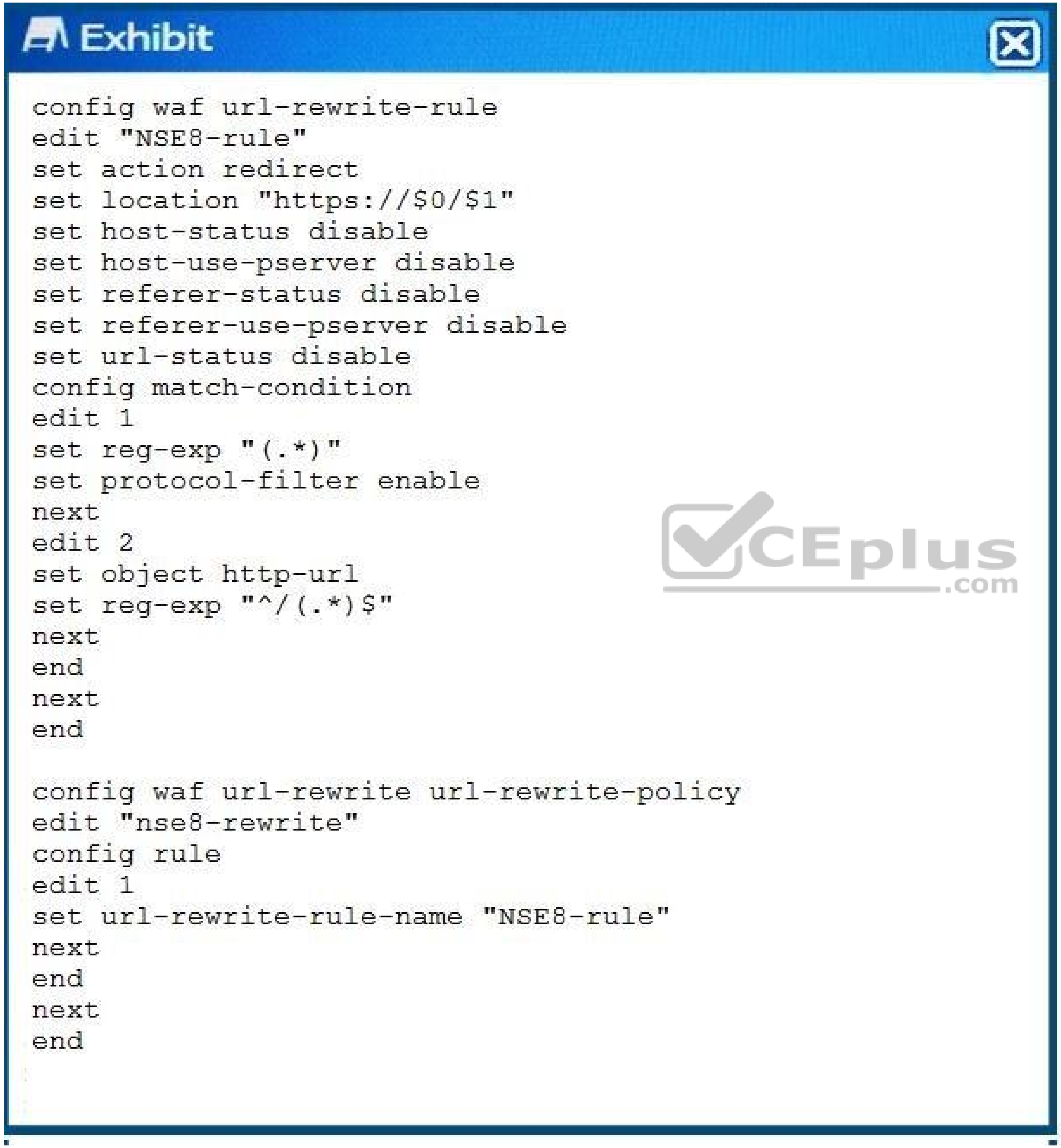
D. set route-overlap allow

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
Click the Exhibit button.



```
config waf url-rewrite-rule
edit "NSE8-rule"
set action redirect
set location "https://$0/$1"
set host-status disable
set host-use-pserver disable
set referer-status disable
set referer-use-pserver disable
set url-status disable
config match-condition
edit 1
set reg-exp "(.*)"
set protocol-filter enable
next
edit 2
set object http-url
set reg-exp "^/(.*)$"
next
end
next
end

config waf url-rewrite url-rewrite-policy
edit "nse8-rewrite"
config rule
edit 1
set url-rewrite-rule-name "NSE8-rule"
next
end
next
end
```

The exhibit shows the steps for creating a URL rewrite policy on a FortiWeb. Which statement represents the purpose of this policy?

A. The policy redirects all HTTP URLs to HTTPS.
B. The policy redirects all HTTPS URLs to HTTP.
C. The policy redirects only HTTPS URLs containing ^/(.*)$ string to HTTP.
D. The policy redirects only HTTPS URLs containing ^/(.*)$ string to HTTPS.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
You want to manage a FortiGate with the FortiCloud service.
The FortiGate shows up in your list of devices on the FortiGate Web Site, but all management functions are either missing or grayed out. Which statement is correct in this scenario?

A. The managed FortiGate is running a version of FortiOS that is either too new or too old for FortiCloud.
B. The managed FortiGate requires that a FortiCloud management license be purchased and applied.
C. You must manually configure system central-management on the FortiGate CLI and set the management type to fortiguard.
D. The management tunnel mode on the managed FortiGate must be changed to normal.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
FortiMail is configured with the protected domain "internal.lab".
Which two envelope addresses will need an access control rule to relay e-mail sent for unauthenticated users? (Choose two.)

A. MAIL FROM: training@fortinet.com;RCPT TO;student@fortinet.com
B. MAIL FROM: student@fortinet.com;RCPT TO;student@internal.lab
C. MAIL FROM: training@internal.lab;RCPT TO;student@internal.lab

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

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

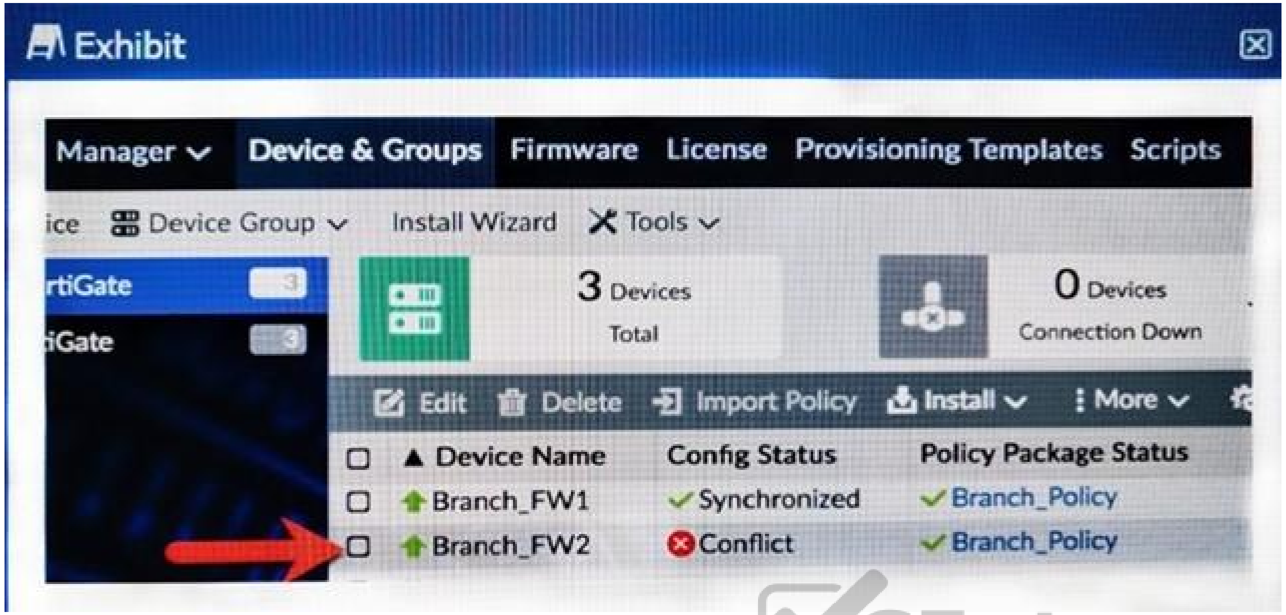
QUESTION 13
You deploy a FortiGate device in a remote office based on the requirements shown below.
-Due to company's security policy, management IP of your FortiGate is not allowed to access the Internet.
- Apply Web Filtering, AntiVirus, IPS and Application control to the protected subnet. - Be managed by a central FortiManager on the head office.
Which action will help to achieve the requirements?

A. Configure a default route and make sure that the FortiGate device can ping to service.fortiguard.net
B. Configure the FortiGuard override server and use the IP address of the FortiManager.
C. Configure the FortiGuard override server and use the IP address of service.fortiguard.net.
D. Configure FortiGuard to use FortiGuard Filtering Port 8888.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
Click the Exhibit button.



☐	▲ Device Name	Config Status	Policy Package Status
☐	Branch_FW1	✓ Synchronized	✓ Branch_Policy
☐	Branch_FW2	☒ Conflict	✓ Branch_Policy

You log into FortiManager, look at the Device Manager window and notice that one of your managed devices is not in normal status. Referring to the exhibit, which two statements correctly describe the affected device's status and result? (Choose two.)

A. The device configuration was changed on the local FortiGate side only; auto-update is disabled.
B. The device configuration was changed on both the local FortiGate side and the FortiManager side; auto-update is disabled.
C. The changed configuration on the FortiGate will remain the next time that the device configuration is pushed form FortiManager.
D. The changed configuration on the FortiGate will be overwritten in favor of what is on the FortiManager the next time that the device configuration is pushed.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
A FortiOS device is used for termination of VPNs for a number of remote spoke VPN units (designated Group A spokes) using a phase 1 main mode dial-up tunnel using pre-shared keys. Your company recently acquired another organization. You are asked to establish VPN connectivity for the newly acquired organization's sites for which new devices will be provisioned (designated Group B spokes). Both existing (Group A) and new (Group B) spoke units are dynamically addressed. You are asked to ensure that spokes from the acquired organization (Group B) have different access permissions that your existing VPN

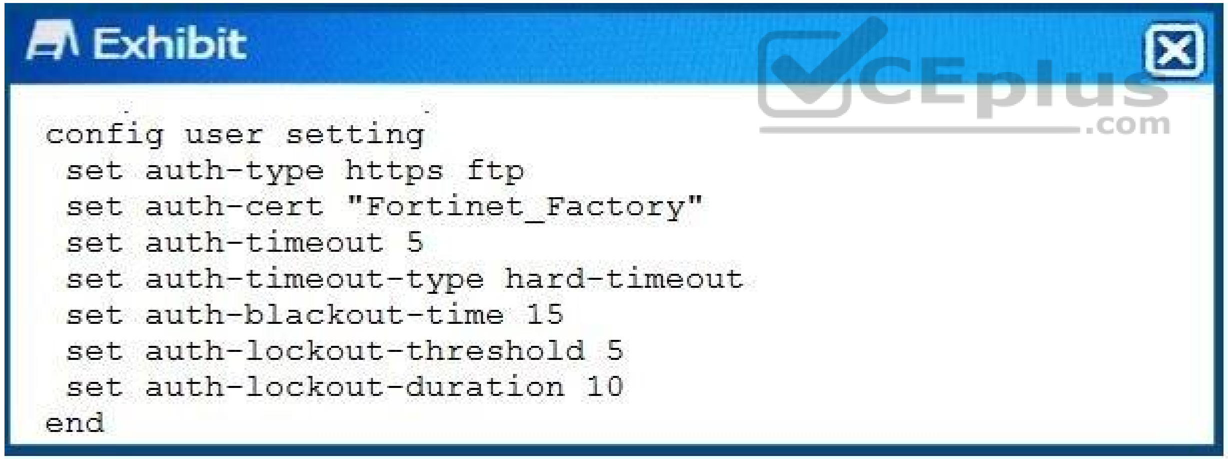
spokes units (Group A). Which two solutions meet the requirements for the new spoke group? (Choose two.)

A. Implement a new phase 1 dial-up main mode tunnel with preshared keys and XAuth. Use identity policies to filter traffic.
B. Implement a new phase 1 dial-up main mode tunnel with a different pre-shared key than Group A spokes. Use standard policies to filter traffic for the new dial-up tunnel.
C. Implement a new phase 1 dial-up main mode tunnel with certificate authentication. Use standard policies to filter traffic for the new dial-up tunnel.
D. Implement separate phase 1 dial-up aggressive mode tunnels with a distinct peer ID. Use standard policies to filter traffic for the new dial-up tunnel.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
Click the Exhibit button.



```
config user setting
 set auth-type https ftp
 set auth-cert "Fortinet_Factory"
 set auth-timeout 5
 set auth-timeout-type hard-timeout
 set auth-blackout-time 15
 set auth-lockout-threshold 5
 set auth-lockout-duration 10
end
```

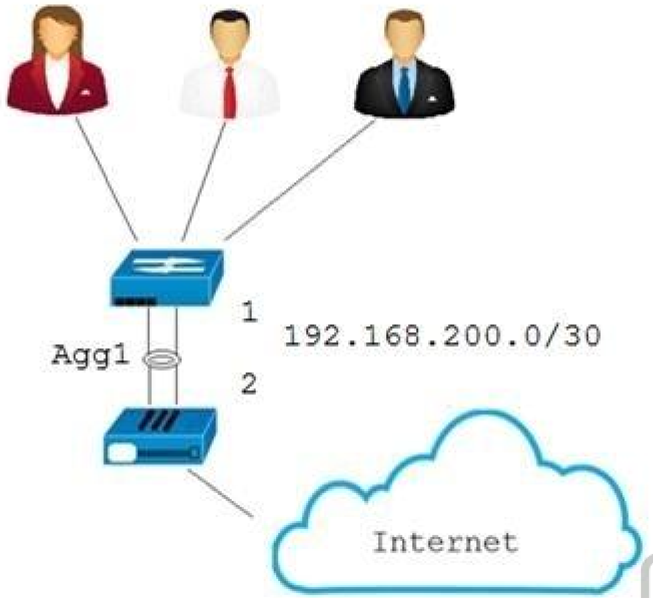
Referring to the exhibit, which two statements are true about local authentication? (Choose two.)

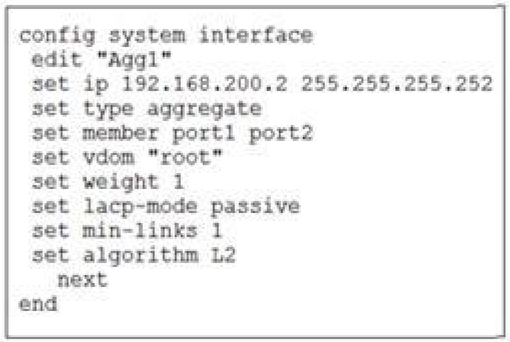
A. The user will be blocked 15 seconds after five login failures.
B. When a ClientHello message indicating a renegotiation is received, the FortiGate will allow the TCP connection.
C. The user's IP address will be blocked 15 seconds after five login failures.
D. After five minutes, the user will need to re-authenticate.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
Click the exhibit.





```
config system interface
 edit "Agg1"
 set ip 192.168.200.2 255.255.255.252
 set type aggregate
 set member port1 port2
 set vdom "root"
 set weight 1
 set lacp-mode passive
 set min-links 1
 set algorithm L2
   next
end
```

You created an aggregate interface between your FortiGate and a switch consisting of two 1 Gbps links as shown in the exhibit. However, the maximum bandwidth never exceeds. 1 Gbps and employees are complaining that the network is slow. After troubleshooting, you notice only one member interface is being used. The configuration for the aggregate interface is shown in the exhibit. In this scenario, which command will solve this problem?

A. config system interface edit Agg1 set min-links 2 end

B. config system interface edit Agg1 set weight 2 end

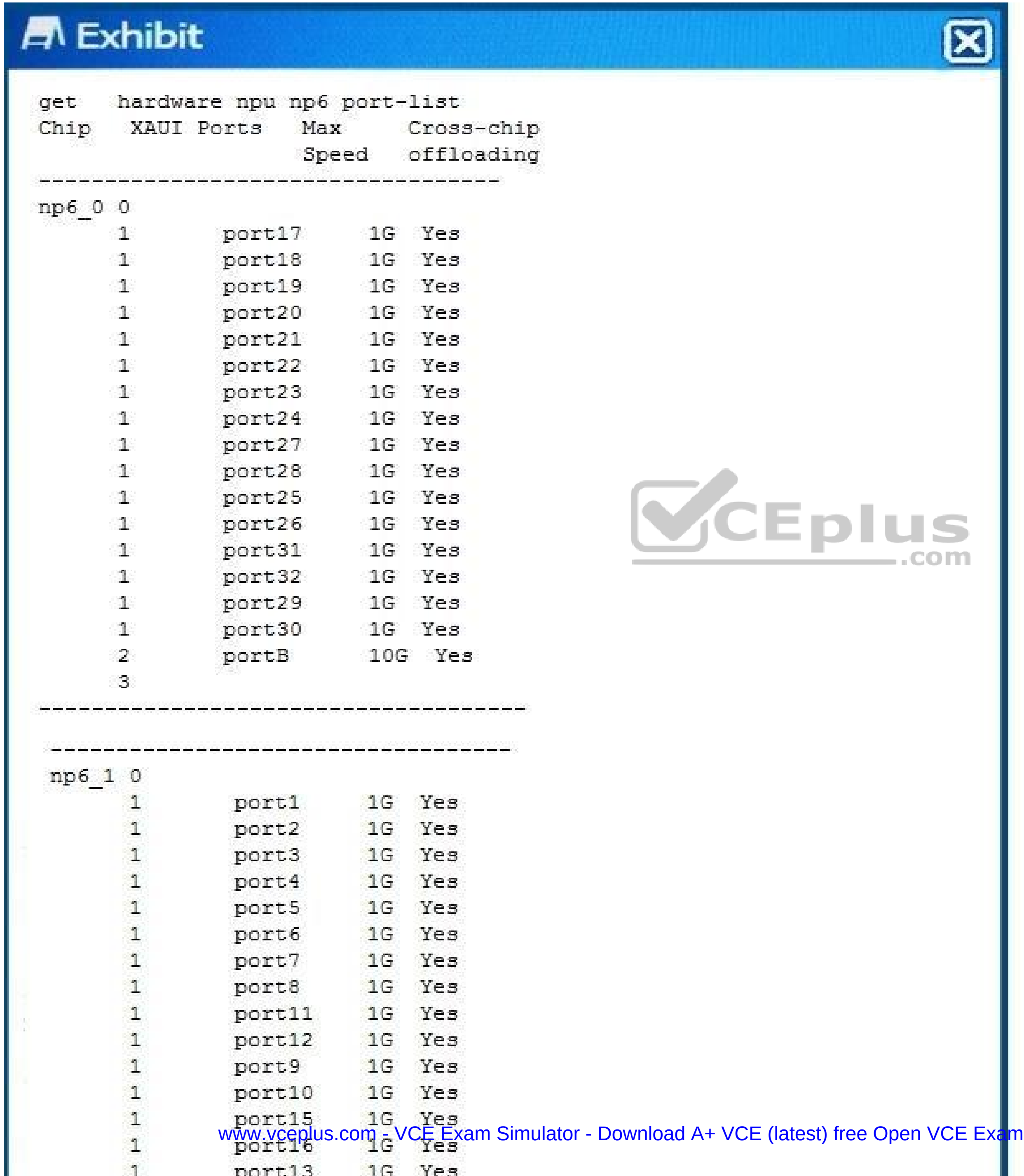
C. config system interface edit Agg1 set Algorithm L4 end

D. config system interface edit Agg1 set lacp-mode active end

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
Click the Exhibit button.



```
get   hardware npu np6 port-list
Chip   XAUI Ports    Max      Cross-chip
                     Speed    offloading
-----------------------------------
np6_0 0
      1       port17     1G   Yes
      1       port18     1G   Yes
      1       port19     1G   Yes
      1       port20     1G   Yes
      1       port21     1G   Yes
      1       port22     1G   Yes
      1       port23     1G   Yes
      1       port24     1G   Yes
      1       port27     1G   Yes
      1       port28     1G   Yes
      1       port25     1G   Yes
      1       port26     1G   Yes
      1       port31     1G   Yes
      1       port32     1G   Yes
      1       port29     1G   Yes
      1       port30     1G   Yes
      2       portB      10G   Yes
      3
-------------------------------------

 -----------------------------------
 np6_1 0
       1       port1     1G   Yes
       1       port2     1G   Yes
       1       port3     1G   Yes
       1       port4     1G   Yes
       1       port5     1G   Yes
       1       port6     1G   Yes
       1       port7     1G   Yes
       1       port8     1G   Yes
       1       port11    1G   Yes
       1       port12    1G   Yes
       1       port9     1G   Yes
       1       port10    1G   Yes
       1       port15    1G   Yes
       1       port16    1G   Yes
       1       port13    1G   Yes
```

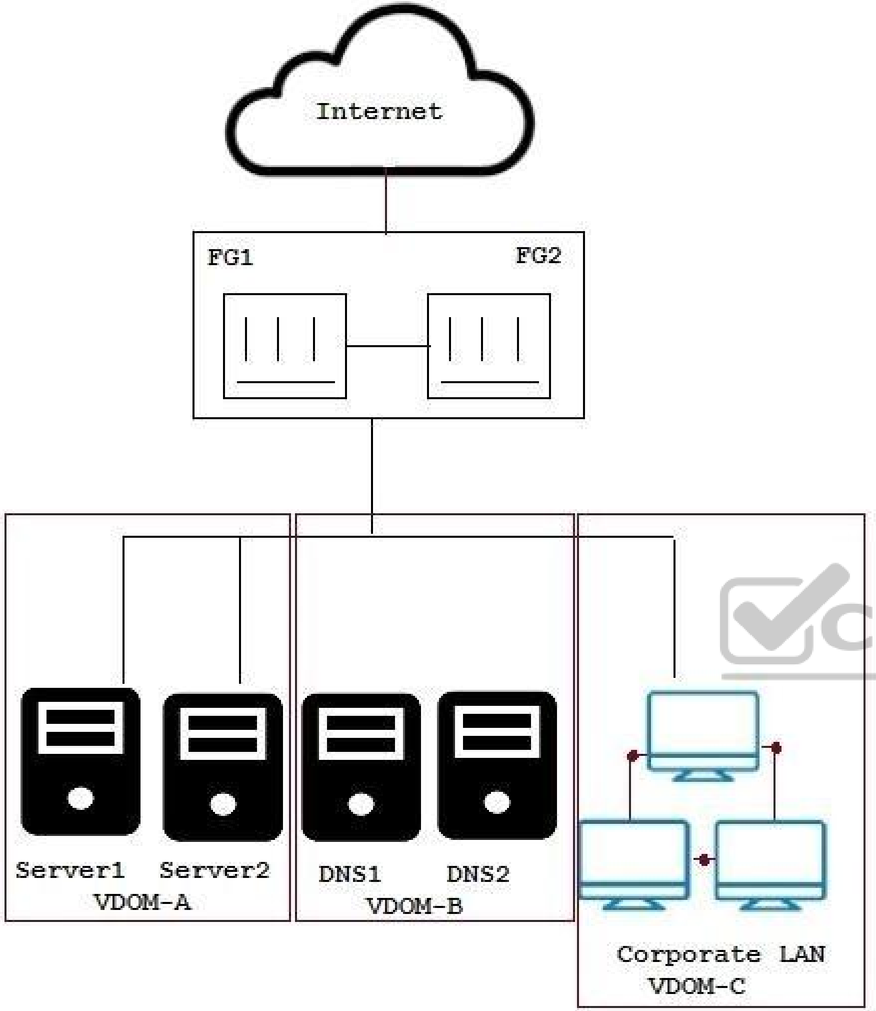
You are trying to configure Link-Aggregation Group (LAG), but ports A and B do not appear on the list of member options. Referring to the exhibit, which statement is correct in this situation?

A. The FortiGate model being used does not support LAG.
B. The FortiGate model does not have an Integrated Switch Fabric (ISF).
C. The FortiGate SFP+ slot does not have the correct module.
D. The FortiGate interfaces are defective and require replacement.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
Click to the Exhibit button.
You need to apply the security features below to the network shown in the exhibit.
-high grade DDoS protection
-Web security and load balancing for Server1 and Server2
-Solution must be PCI DSS compliant
-Enhanced security to DNS 1 and DNS 2



What are three solutions for this scenario? (Choose three.)

A. FortiWeb for VDOM-A
B. FortiDDoS between FG1 and FG2 and the Internet
C. FortiADC for VDOM-A

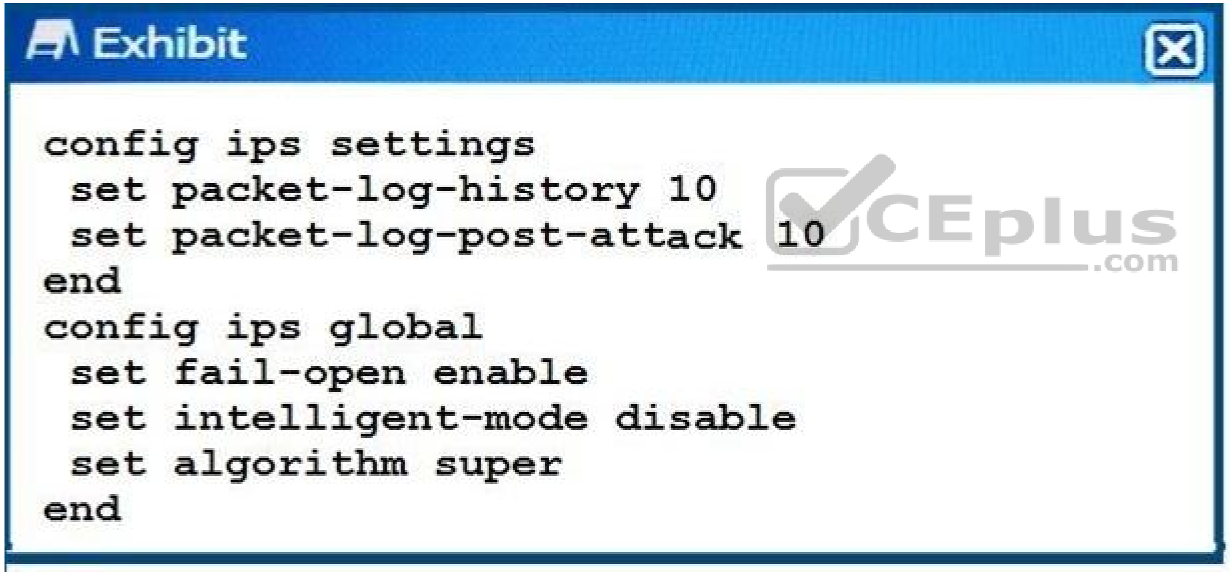
D. FortiADC for VDOM-B

E. FortiDDoS between FG1 and FG2 and VDOMs

Correct Answer: CDE
Section: (none)
Explanation

Explanation/Reference:
Section: (none)
Explanation

QUESTION 20
Click the Exhibit button.



```
config ips settings
 set packet-log-history 10
 set packet-log-post-attack 10
end
config ips global
 set fail-open enable
 set intelligent-mode disable
 set algorithm super
end
```

An Administrator reports continuous high CPU utilization on a FortiGate device due to the IPS engine. The exhibit shows the global IPS configuration. Which two configuration actions will reduce the CPU usage? (Choose two.)

A. Disable fail open

B. Enable intelligent mode

C. Change the algorithm to low

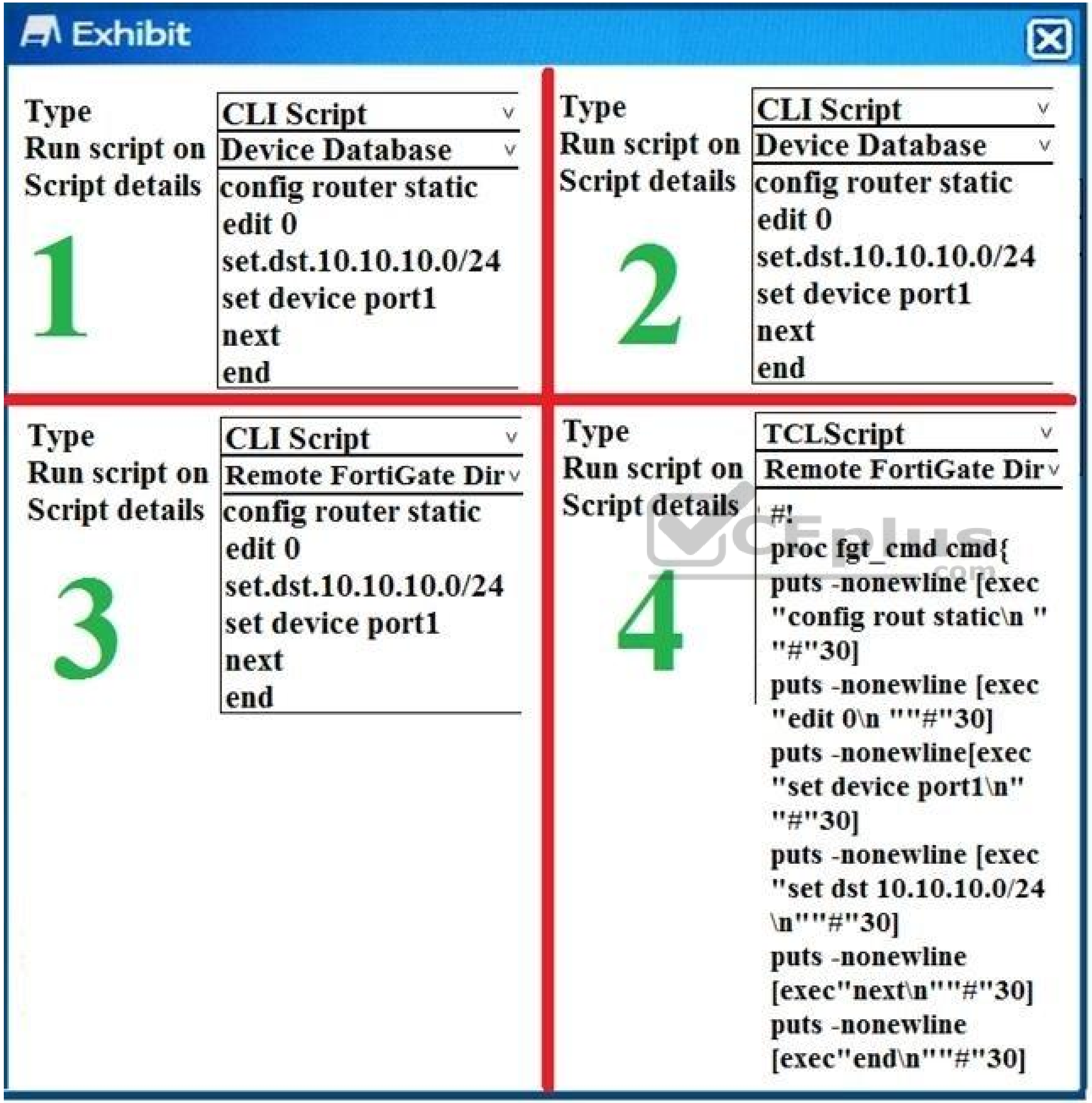
D. Reduce the number of packets being logged

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21

Refer to the Exhibit button.



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]
```

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.)

A. Script 1

B. Script 2

C. Script 3

D. Script 4

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22

You are building a FortiGate cluster which is stretched over two locations. The HA connections for the cluster are terminated on the local switches in the data centers. Once the FortiGates have booted, they do not form a cluster. The network operations inform you that CRC errors are present on the switches where the FortiGates are connected.
What should you do to solve this problem?

A. Replace the cables where the CRC errors occur.

B. Change the ethertype for the HA packets.

C. Set the speed/duplex setting to 1 Gbps / Full Duplex.

D. Place the HA interfaces in dedicated VLANs.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23

You cannot ping the FortiGate's default gateway 10.10.10.1 from the FortiGate CLI. The FortiGate's interface facing the default gateway is wan1 and its IP address is 10.10.10.254/24. During the initial troubleshooting tests, you confirmed that you can ping other IP addresses in the 10.10.10.0/24 subnet from the FortiGate CLI without packets lost. Which two CLI commands will help you to troubleshoot this problem? (Choose two.)

A. diagnose ip arp list

B. diag sniffer packet wan1 'arp and host 10.10.10.1'

C. diagnose hardware deviceinfo nic wan1

D. diagnose debug flow filter saddr 10.10.10.1 Diagnose debug flow trace start 10

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24

You have deployed a FortiGate in NAT/Route mode as a Secure Web Gateway with a few IP-based authentication firewall policies. Your customer reports that some users now have different browsing permissions from what is expected. All these users are browsing using Internet Explorer through a Remote Desktop Connection to a Terminal Server.
When you look at the FortiGate logs, the username for the Terminal Server IP is not consistent.
Which action will correct this problem?

A. Make sure the Terminal Server is using the correct DNS server.

B. Configure FSSO Advanced with LDAP integration.

C. Change the FSSO Polling mode to Windows NetAPI.

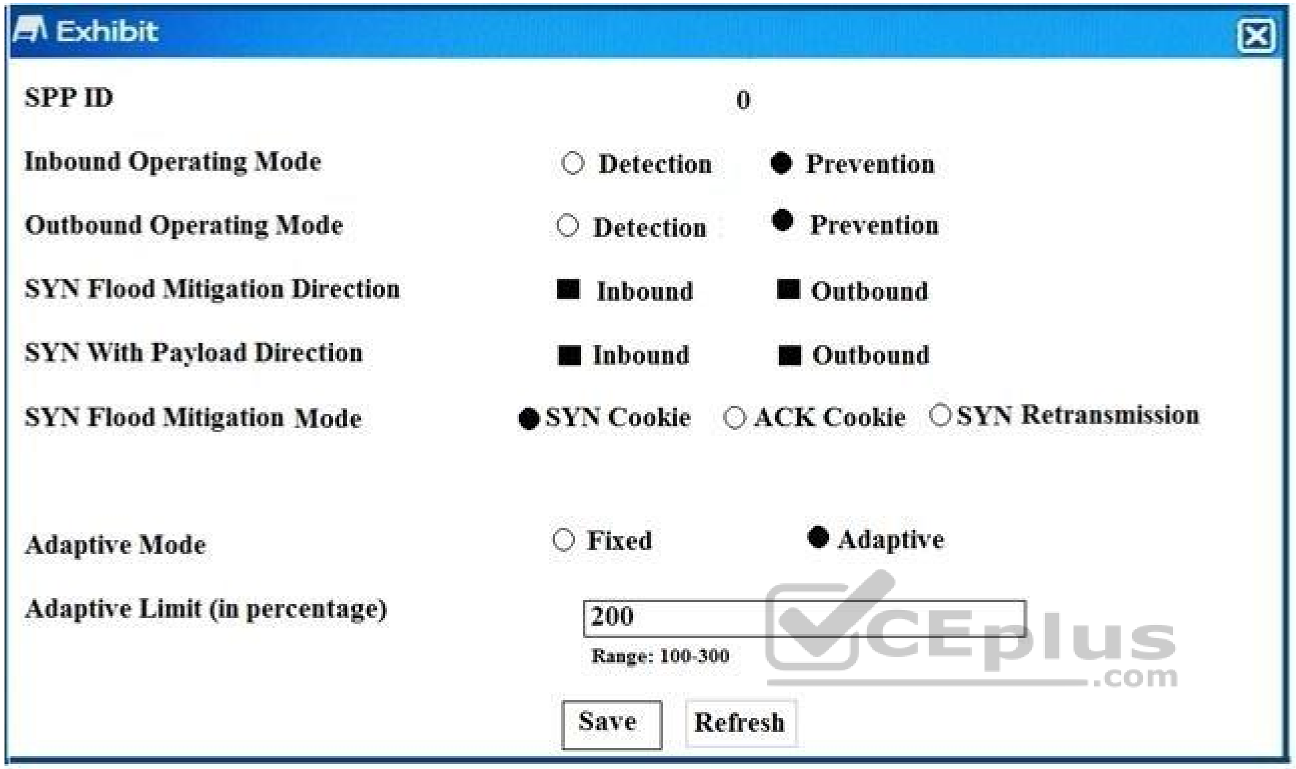
D. Install the TS/Citrix agent on the terminal server.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25

Click the Exhibit button.



Exhibit

SPP ID	0		
Inbound Operating Mode	○ Detection	● Prevention	
Outbound Operating Mode	○ Detection	● Prevention	
SYN Flood Mitigation Direction	■ Inbound	■ Outbound	
SYN With Payload Direction	■ Inbound	■ Outbound	
SYN Flood Mitigation Mode	● SYN Cookie	○ ACK Cookie	○ SYN Retransmission
Adaptive Mode	○ Fixed	● Adaptive	
Adaptive Limit (in percentage)	200 Range: 100-300		

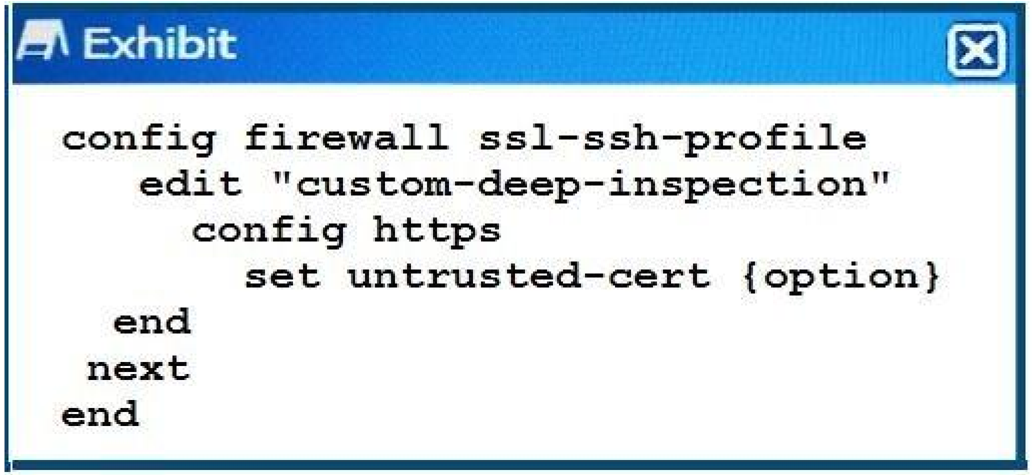
The exhibit shows the configuration of a service protection profile (SPP) in a FortiDDoS device.
Which two statements are true about the traffic matching being inspected by this SPP? (Choose two.)

A. Traffic that does not match any SPP policy will be inspected by this SPP.
B. FortiDDoS will not send a SYN/ACK if a SYN packet is coming from an IP address that is not in the legitimate IP (LIP) address table.
C. FortiDDoS will start dropping packets as soon as the traffic exceeds the configured minimum threshold.
D. SYN packets with payloads will be dropped.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
Click the Exhibit button.



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

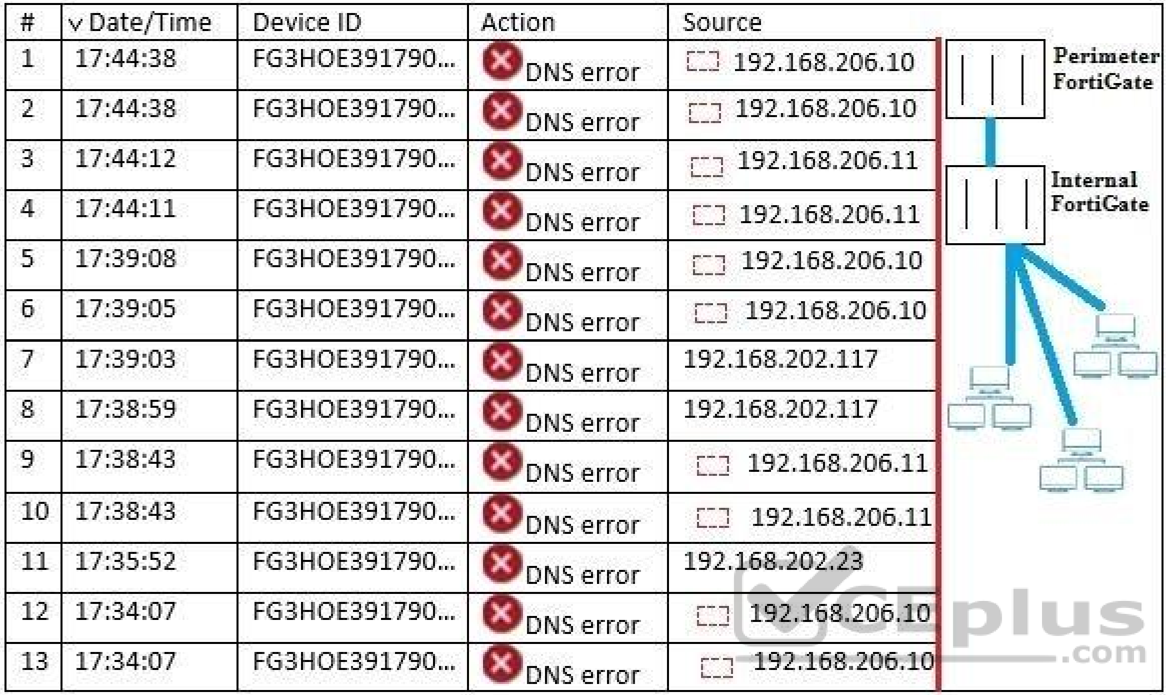
Referring to the exhibit, which command-line option for deep inspection SSL would have the FortiGate re-sign all untrusted self-signed certificates with the trusted Fortinet_CA_SSL certificate?

A. allow
B. back
C. ignore
D. inspect

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
Click the Exhibit button.
You have deployed several perimeter FortiGates with internal segmentation FortiGates behind them. All FortiGate devices are logging to FortiAnalyzer. When you search the logs in FortiAnalyzer for denied traffic, you see numerous log messages, as shown in the exhibit, on your perimeter FortiGates only.



#	Date/Time	Device ID	Action	Source
1	17:44:38	FG3HOE391790...	DNS error	192.168.206.10
2	17:44:38	FG3HOE391790...	DNS error	192.168.206.10
3	17:44:12	FG3HOE391790...	DNS error	192.168.206.11
4	17:44:11	FG3HOE391790...	DNS error	192.168.206.11
5	17:39:08	FG3HOE391790...	DNS error	192.168.206.10
6	17:39:05	FG3HOE391790...	DNS error	192.168.206.10
7	17:39:03	FG3HOE391790...	DNS error	192.168.202.117
8	17:38:59	FG3HOE391790...	DNS error	192.168.202.117
9	17:38:43	FG3HOE391790...	DNS error	192.168.206.11
10	17:38:43	FG3HOE391790...	DNS error	192.168.206.11
11	17:35:52	FG3HOE391790...	DNS error	192.168.202.23
12	17:34:07	FG3HOE391790...	DNS error	192.168.206.10
13	17:34:07	FG3HOE391790...	DNS error	192.168.206.10

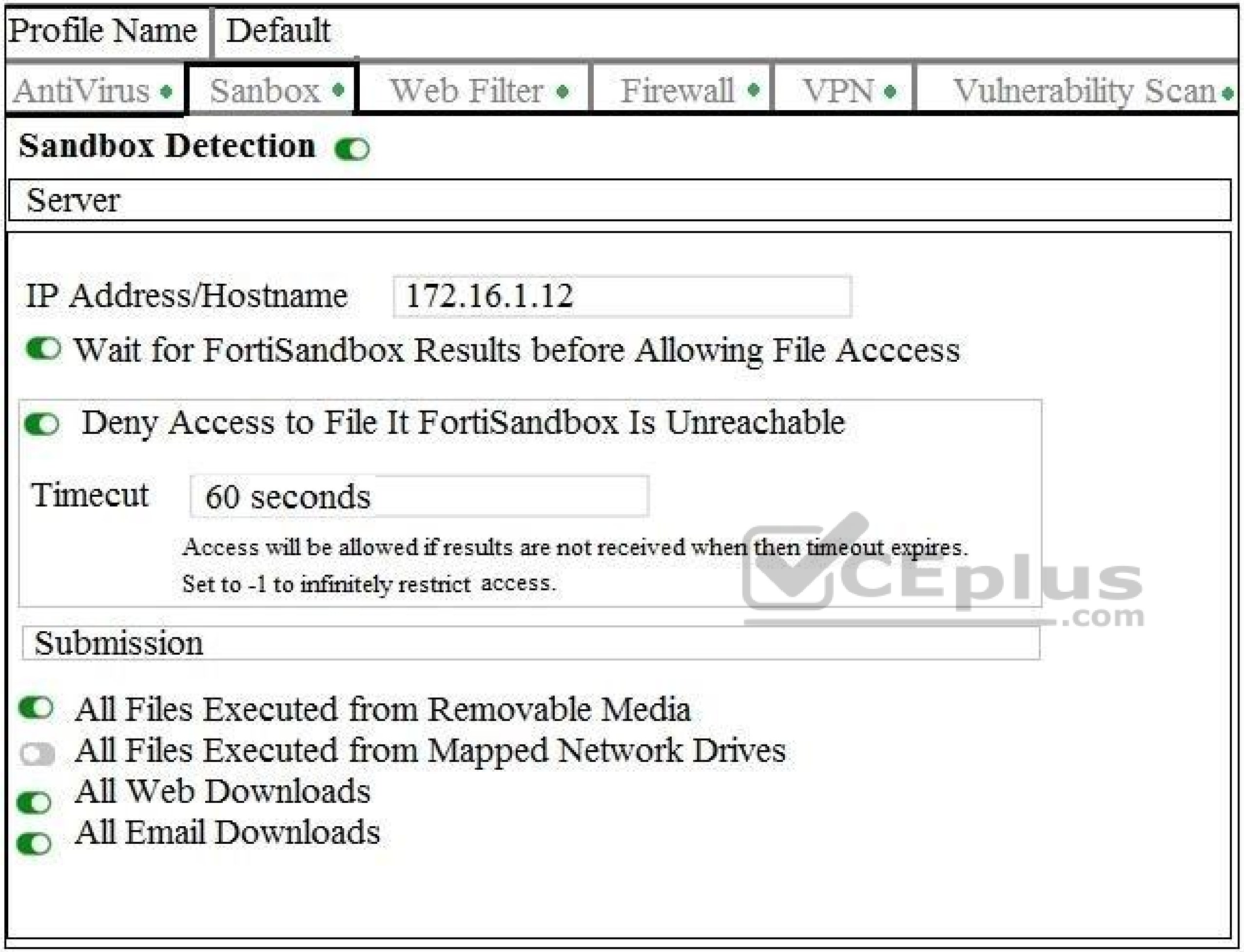
Which two actions would reduce the number of these log messages? (Choose two.)

A. Apply an application control profile to the perimeter FortiGates that does not inspect DNS traffic to the outbound firewall policy.
B. Configure the internal FortiGates to communicate to FortiGates using port 8888.
C. Disable DNS events logging from FortiGate in the config log fortianalyzer filter section.
D. Remove DNS signatures from the IPS profile applied to the outbound firewall policy.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
Click the Exhibit button.



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

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

A. Files executed from a mapped network drive will not be inspected by the FortiClient 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 is reachable.
D. The user will not be able to access a Web downloaded file when the FortiSandbox is unreachable.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
You are asked to implement a single FortiGate 5000 chassis using Session-aware Load Balance Cluster (SLBC) with Active "" Passive FortinControllers. Both FortiControllers have the configuration shown below, with the rest of the configuration set to the default values:
Ñonfig system ha set mode dual set password fortinetnse8 set group-id 5 set chassis-id 1
set minimize-chassis-failover enable set hbdev "b1"
end
Both FortiControllers show Master status. What is the problem in this scenario?

A. The management interface of both FortiControllers was connected on the same work.
B. The priority should be set higher for FortiController on slot-1.
C. The b1 interface of the two FortiControllers do not see each other.
D. The chassis ID settings on FortiController on slot 2 should be set to 2.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
Click the Exhibit button.
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.) 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

A. Disable the sync feature on port3; then configure specific IPs for port3 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 port3 to the VDOM, then configure specific IPs for port3 on both cluster members.
D. Allow administrative access in the HA heartbeat interfaces.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

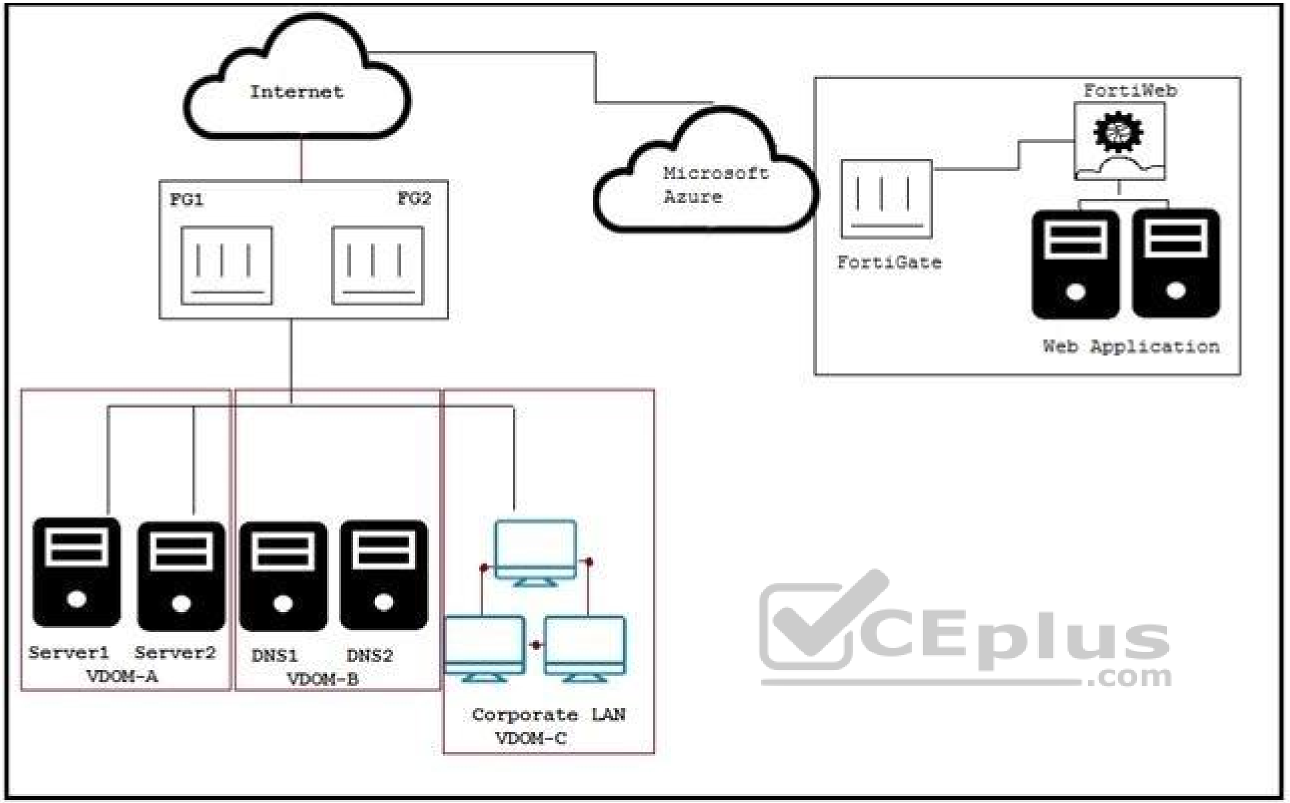
QUESTION 31
You configured an outgoing firewall policy with a Web filter profile for accessing the Internet. The access to URL https://www.it-acme.com and all Web sites belonging to the same category should be blocked. You notice that the Web server presents a certificate with CN=www.acme.com site is categorized as "Information Technology" and the www.acme.com site is categorized as "Business". Which statement is correct in this scenario?

A. Category "Information technology" needs to be blocked, the FortiGate is able to inspect the URL with HTTPS sessions.
B. Category "Business" needs to be blocked, the certificate name takes precedence over the SNI.
C. SSL inspection must be configured to deep-inspection, the category "Information Technology" needs to be blocked.
D. Category "Information Technology" needs to be blocked, the SNI takes precedence over the certificate name.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
Click the Exhibit button. A customer has just finished their Azure deployment to secure a Web application behind a FortiGate and a FortiWeb. Now they want to add components to protect against advanced threats (zero day attacks), centrally manage the entire environment, and centrally monitor Fortinet and non-Fortinet products. Which Fortinet solutions will satisfy these requirements?



A. Use FortiAnalyzer for monitoring in Azure, FortiSIEM for management, and FortiSandbox for zero day attacks on their local network.
B. Use FortiAnalyzer for monitoring in Azure, FortiSIEM for management, and FortiGate for zero day attacks on their local network.
C. Use FortiManager for management in Azure, FortiSIEM for monitoring, and FortiSandbox for zero day attacks on their local network.
D. Use FortiSIEM for monitoring in Azure, FortiManager for management, and FortiGate for zero day attacks on their local network.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference: