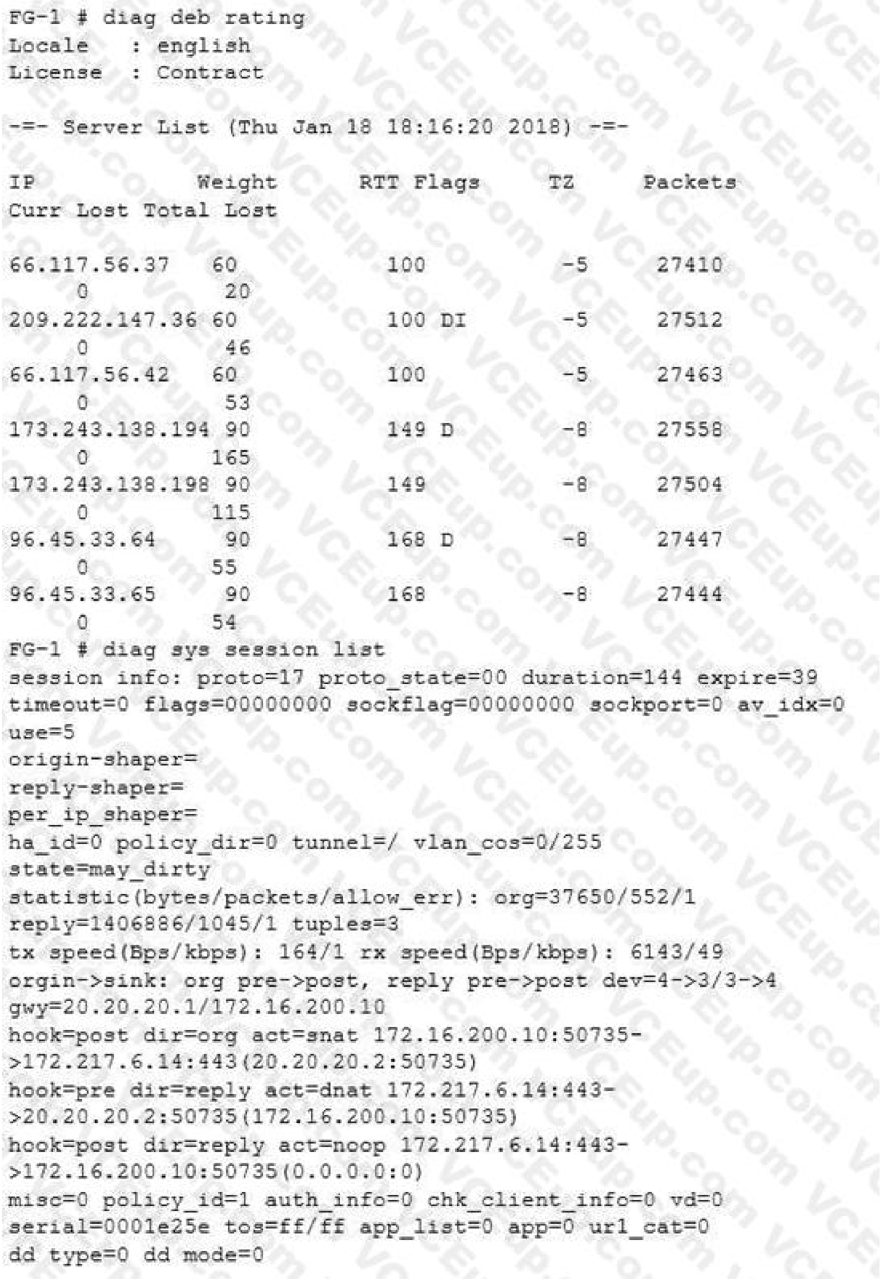
Fortinet.Premium.NSE8_811 .65q

Number: NSE8_811
Passing Score: 800
Time Limit: 120 min
File Version: 1.7

Exam Code: NSE8_811
Exam Name: Fortinet NSE 8 Written Exam (NSE8_811)
Website: https://VCEup.com/

QUESTION 1
Click the Exhibit button.
You configured AV and Web filtering for your outgoing Internet connections. You later noticed that not all Web sessions are being inspected and you start troubleshooting the problem.
Referring to the exhibit, what would cause this problem?



```
FG-1 # diag deb rating
Locale    : english
License   : Contract

-=- Server List (Thu Jan 18 18:16:20 2018) -=-

IP              Weight       RTT Flags     TZ      Packets
Curr Lost Total Lost

66.117.56.37   60           100           -5     27410
     0          20
209.222.147.36 60           100 DI        -5     27512
     0          46
66.117.56.42   60           100           -5     27463
     0          53
173.243.138.194 90          149 D         -8     27558
     0         165
173.243.138.198 90          149           -8     27504
     0         115
96.45.33.64      90         168 D         -8     27447
     0         55
96.45.33.65      90         168           -8     27444
     0         54
FG-1 # diag sys session list
session info: proto=17 proto_state=00 duration=144 expire=39
timeout=0 flags=00000000 sockflag=00000000 sockport=0 av_idx=0
use=5
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty
statistic(bytes/packets/allow_err): org=37650/552/1
reply=1406886/1045/1 tuples=3
tx speed(Bps/kbps): 164/1 rx speed(Bps/kbps): 6143/49
orgin->sink: org pre->post, reply pre->post dev=4->3/3->4
gwy=20.20.20.1/172.16.200.10
hook=post dir=org act=snat 172.16.200.10:50735-
>172.217.6.14:443(20.20.20.2:50735)
hook=pre dir=reply act=dnat 172.217.6.14:443-
>20.20.20.2:50735(172.16.200.10:50735)
hook=post dir=reply act=noop 172.217.6.14:443-
>172.16.200.10:50735(0.0.0.0:0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=0001e25e tos=ff/ff app_list=0 app=0 url_cat=0
dd type=0 dd mode=0
```

A. The Web session is using QUIC which a not inspected by the FortiGate
B. These are problem with the connection to the Web filter servers, therefore the Web session cannot be categorized.
C. The SSL inspection options are not set to inspection
D. Web filtering is not licensed, therefore no inspection occurs.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2

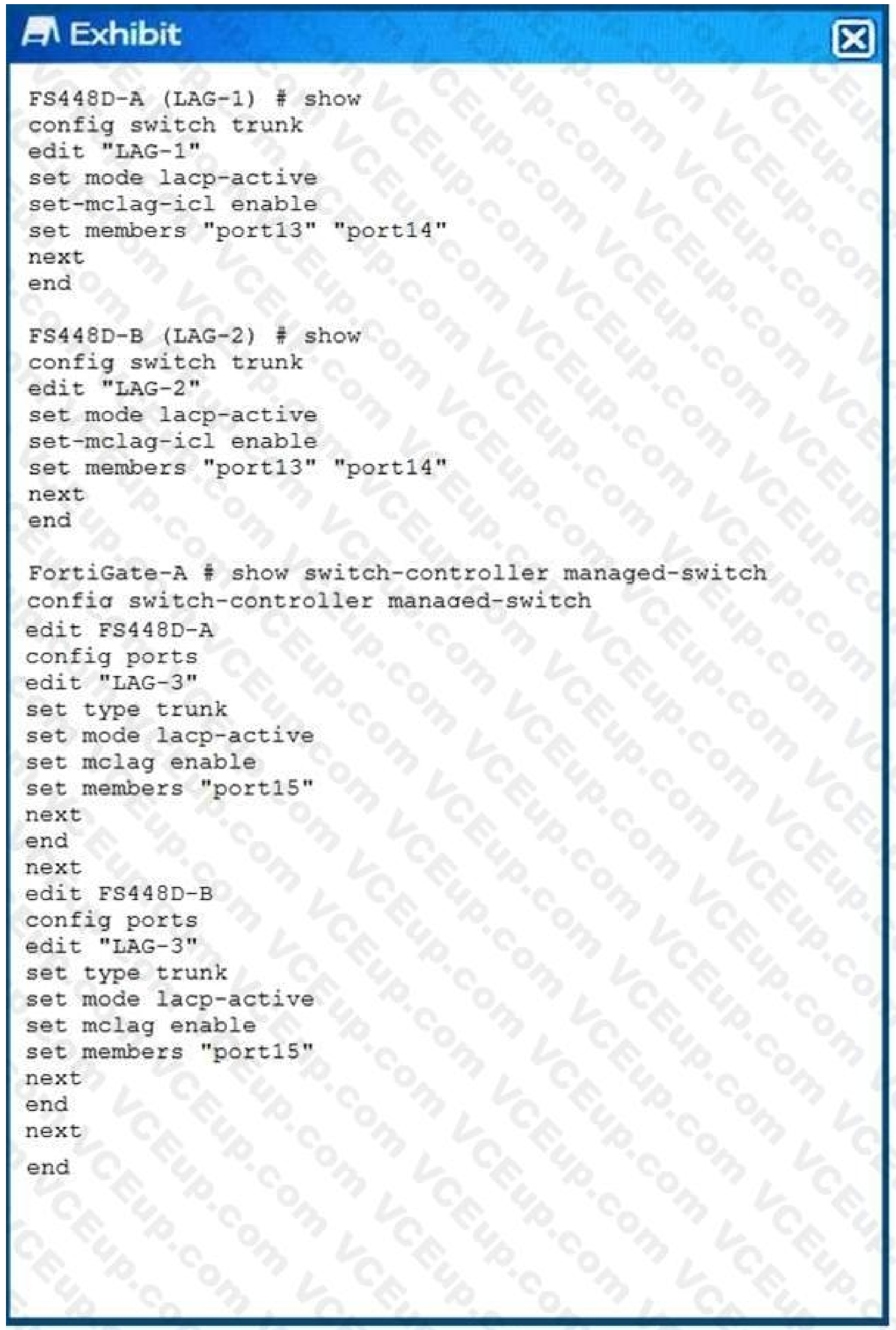
You are administrating the FortiGate 5000 and FortiGate 7000 series products. You want to access the HTTPS GU of the blade located n logical slot of the secondary chassis in a high-availability cluster.
Which URL will accomplish this task?

A. https//192.168.1.99.44302
B. https//192.168.1.99.44313
C. https//192.168.1.99.44322
D. https//192.168.1.99.44323

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
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"
next
end
next
end
```

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: AC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://help.fortinet.com/fos50hlp/56/Content/FortiOS/fortigate-managingfortiswitch/Stacking.htm

QUESTION 4
A customer wants to integrate their on-premise FortiGate with their Azure infrastructure.
Which two components must be in place to configure the Azure Fabric connector? (Choose two.)

A. FortiGate-VM virtual appliance deployed on-premise.
B. An inbound policy from the Azure FortiGate-VM virtual appliance.
C. An outbound policy from the Azure FortiGate-VM virtual appliance.
D. A FortiGate-VM virtual appliance deployed in Azure.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
You cannot the FortiGales default gateway 10.10.10 .1 from the FortiGate CLI. The FortiGate interface facing the default gateway is wan 1 and its IP address 10.10 .10 K74 During the troubleshooting, tests, you confirmed that you can plug 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 debug flow filter saddr 10.10.10.1 diagnose debug flow trace start 10
B. diagnose hardware deviceinfo nic wan1
C. diagnose ip arp list
D. diag sniffer packet wan1 'arp and host 10.10.10.1'

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
An organization has one central site and three remote sites. A FortiSIEM has been installed on the central site and now all devices across the remote sites must be centrally monitored by the FortiSIEM at the central site.
Which action will reduce the WAN usage by the monitoring system?

A. Enable SD-WAN FEC (Forward Error Correction) on the FortiGate at the remote site.
B. Install both Supervisor and Collector on each remote site.
C. Install local Collectors on each remote site.
D. Disable real-time log upload on the remote sites.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

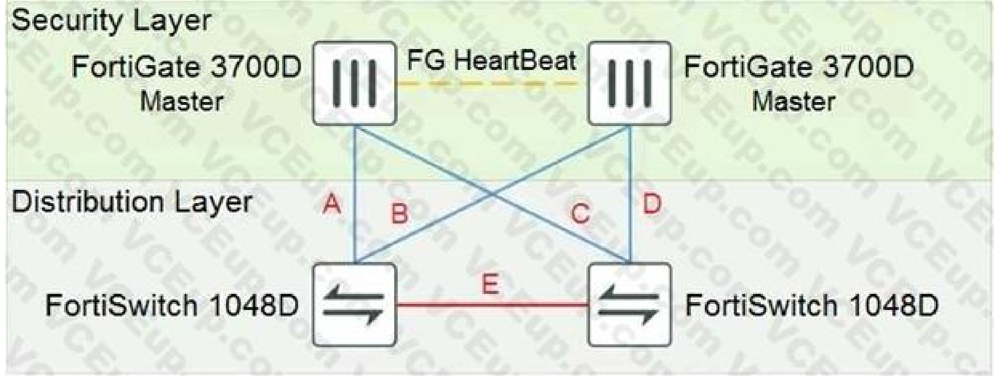
QUESTION 7
A customer is looking for a way to remove javascripts, macros and hyperlinks from documents traversing the network without affecting the integrity of the content. You propose to use the Content disarm and reconstruction (CDR) feature of the FortiGate.
Which two considerations are valid to implement CDR in this scenario? (Choose two.)

A. The inspection mode of the FortiGate is not relevant for CDR to operate.
B. CDR is supported on HTTPS, SMTPS, and IMAPS if deep inspection is enabled.
C. CDR can only be performed on Microsoft Office Document and PDF files.
D. Files processed by CDR can have the original copy quarantined on the FortiGate.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
Refer to the exhibit.



The exhibit shows a full-mesh topology between FortiGate and FortiSwitch devices. To deploy this configuration, two requirements must be met:
• 20 Gbps full duplex connectivity is available between each FortiGate and the FortiSwitch devices
• The FortiGate HA must be in AP mode
Referring to the exhibit, what are two actions that will fulfill the requirements? (Choose two.)

A. Configure the master FortiGate with one LAG and FortiLink split interface disabled on ports connected to cables A and C and make sure the same ports are used for cables B and D on the slave.
B. Configure the master FortiGate with one LAG and FortiLink split interface enabled on ports connected to cables A and C and make sure the same ports are used for cables B and D on the slave.
C. Configure both FortiSwitch devices as peers with ICL over cable E, create one MCLAG on ports connected to cables A and C, and create another MCLAG on ports connected to cables B and D.
D. Configure both FortiSwitch devices as peers with ISL over cable E, create one MCLAG on ports connected to cables A and C, and create another MCLAG on ports connected to cables B and D.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

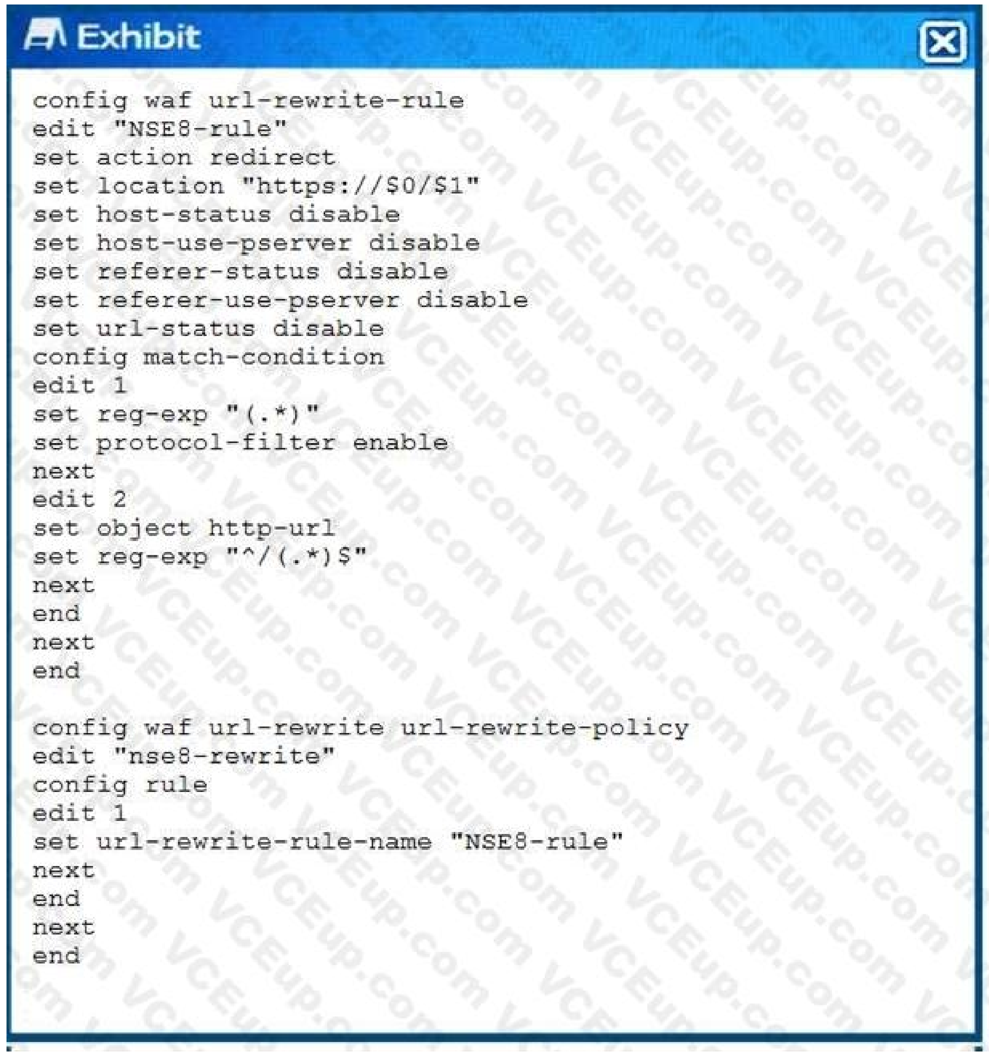
QUESTION 9
You want to manage a FortiCloud service. The FortiGate shows up in your list devices on the FortiCloud Web site, but all management functions are either missing or grayed out.
Which statement a correct in this scenario?

A. The managed FcrtGate a running a version of ForflOS that is either too new or too for FortCloud.
B. The managed FortiGate requires that a FortiCloud management license be purchased and applied.
C. You must manually configure system control-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 10
Exhibit



```
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
```

Click the Exhibit button. 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 the ˆ/ (. *) S string to HTTP.
D. The pokey redirects only HTTP URLs containing theˆ/ (.*)S string to HTTPS.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://help.fortinet.com/fweb/581/Content/FortiWeb/fortiwebadmin/application_delivery.htm#application_delivery_1557589163_940788

QUESTION 11
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

Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://help.fortinet.com/fddos/4-3-0/FortiDDoS/Understanding_FortiDDoS_Prevention_Mode.htm

QUESTION 12
You are building a FortiGala cluster which is stretched over two locations. The HA connections for the cluster are terminated on the data centers. Once the FortiGates have booted, they do form a cluster.
The network operators inform you that CRC eoors are present on the switches where the FortiGAtes are connected.
What would you do to solve this problem?

A. Replace the caables where the CRC errors occur.
B. Change the ethertype for the HA packets.
C. Set the speedduplex setting to 1 Gbps /Full Duplex.
D. Place the HA interfaces in dedicated VLANs.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://help.fortinet.com/fos60hlp/60/Content/FortiOS/fortigate-highavailability/HA_failoverHeartbeat.htm#Heartbea

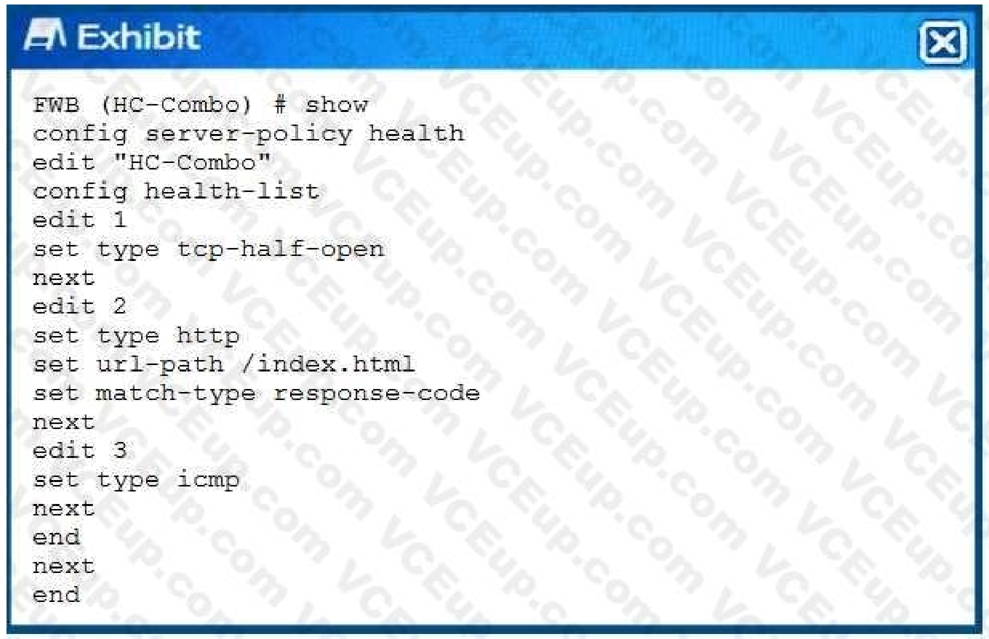
QUESTION 13
You want to access the JSON API on FortiManager to retrieve information on an object.
In this scenario, which two methods will satisfy the requirement? (Choose two.)

A. Make a call with the Web browser on your workstation.
B. Make a call with the SoapUI 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: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
Exhibit



Exhibit

```
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
```

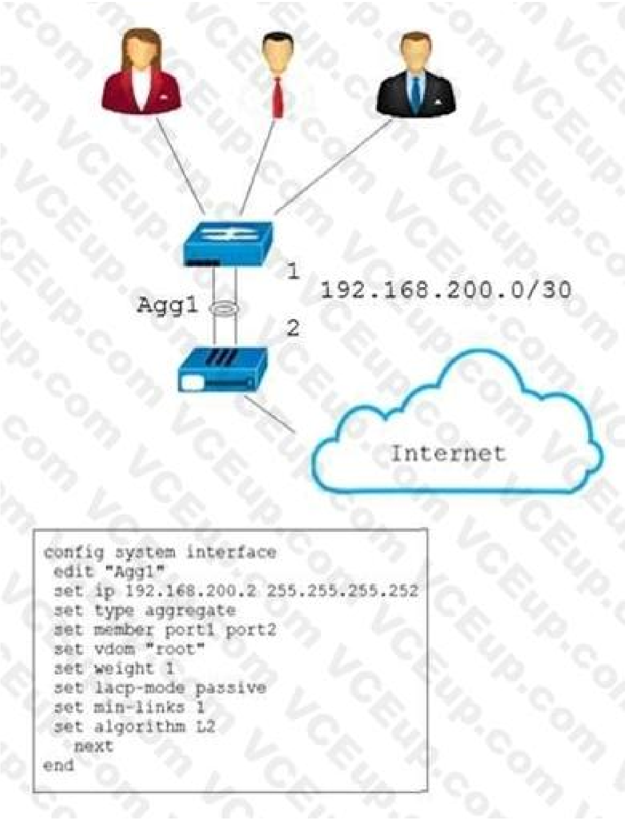
You created a custom health-check for your FortiWeb deployment.
Referring to the output shown in the exhibit, which statement is true?

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: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
Click the exhibit.
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.



```
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
```

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

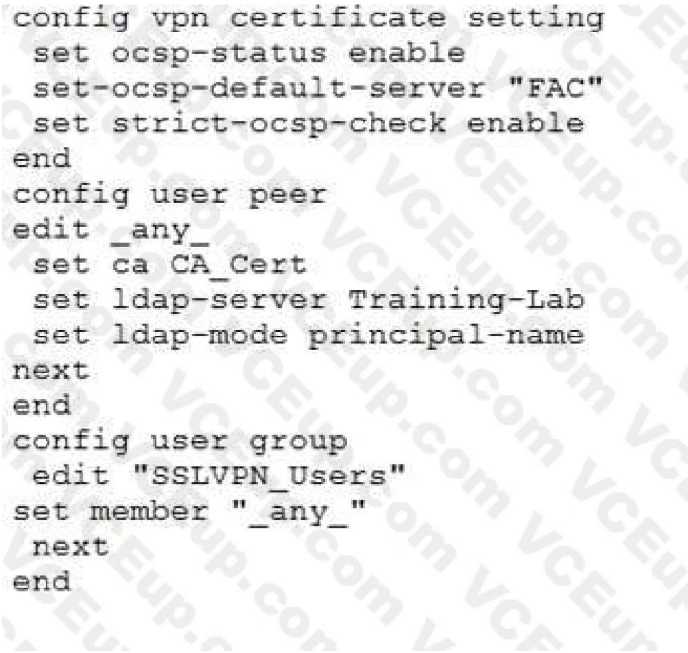
C. config system interface
edit Agg1
set Algorithm L4
end

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
Click the exhibit button.
A FortiGate device is configured to authenticate SSL VPN users using digital certificates. Part of the FortiGate configuration is shown in the exhibit.
Which two statements are true in this scenario? (Choose two.)



```
config vpn certificate setting
 set ocsp-status enable
 set-ocsp-default-server "FAC"
 set strict-ocsp-check enable
end
config user peer
edit _any_
 set ca CA_Cert
 set ldap-server Training-Lab
 set ldap-mode principal-name
next
end
config user group
 edit "SSLVPN_Users"
set member "_any_"
 next
end
```

A. The authentication will fail if the OCSP server is down.

B. OCSP is used to verify that the user-signed certificate has not expired.

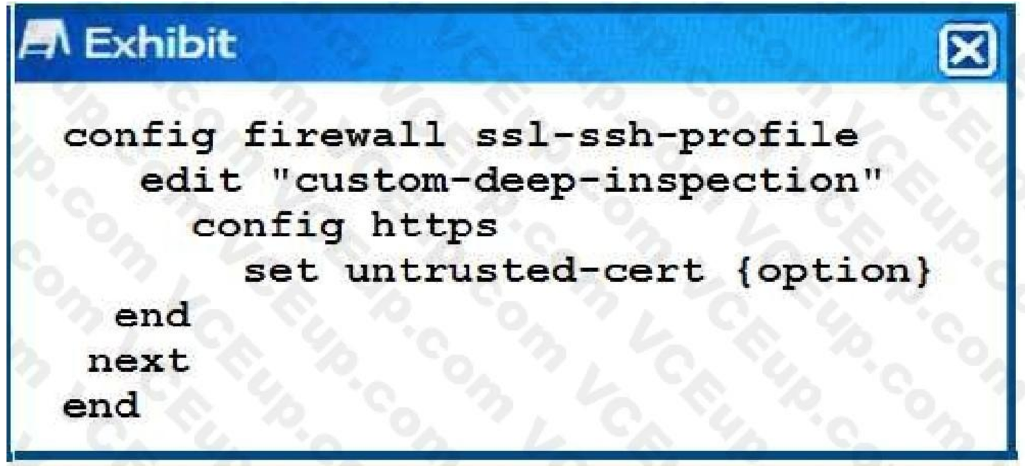
C. The authentication will fail if the certificate does not contain user principle name (UPN) information.

D. The authentication will fail if the user certificate does not contain the CA_Cert string in the Failed.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://kb.fortinet.com/kb/documentLink.do?externalID=FD48218
https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/751987/ssl-vpn-with-ldapintegrated-certificate-authentication

QUESTION 17
Click the Exhibit button.
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?



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

A. allow

B. block

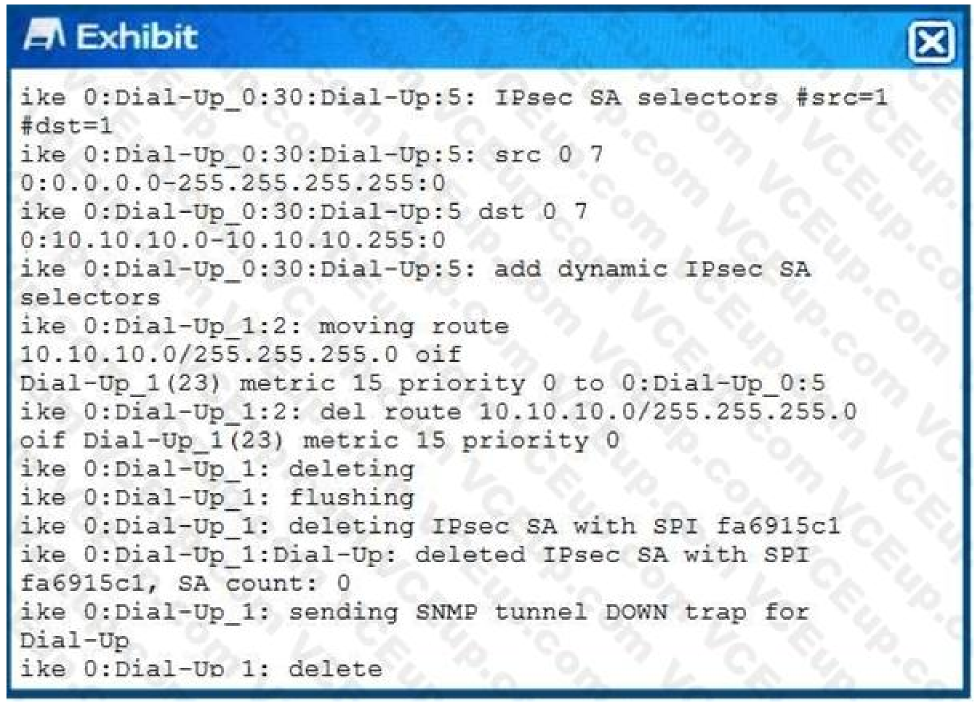
C. ignore

D. inspect

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://help.fortinet.com/cli/fos60hlp/60/Content/FortiOS/fortiOS-cli-ref/config/firewall/ssl-sshprofile.htm

QUESTION 18
Exhibit
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-router enable
C. set single-source disable
D. set router-overlap allow

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://docs.fortinet.com/document/fortigate/6.0.0/cli-reference/487941/vpn-ipsec-phase2-interface-phase2

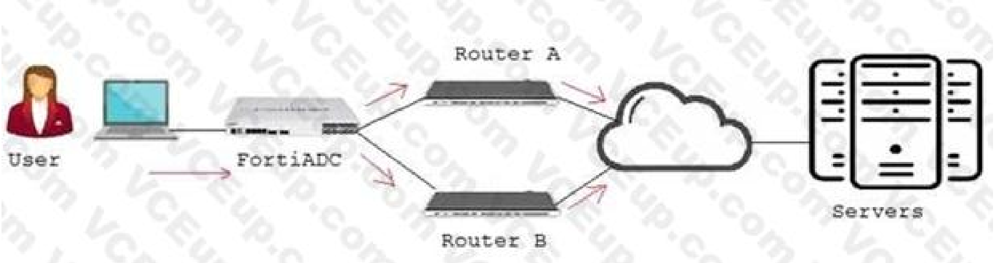
QUESTION 19
A customer wants to enable SYN Rood mitigation in a FortiDDoS device. The FortiDDoS must reply with one SYN/ACK packet per SYN packet ftom a new source IP address. Which SYN packet from a new source IP address.
Which SYN flood mitigation mode must the customer use?

A. SYN cookie
B. SYN/ACK cookie
C. ACK cookie
D. SYN retransmission

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
Click the Exhibit button.



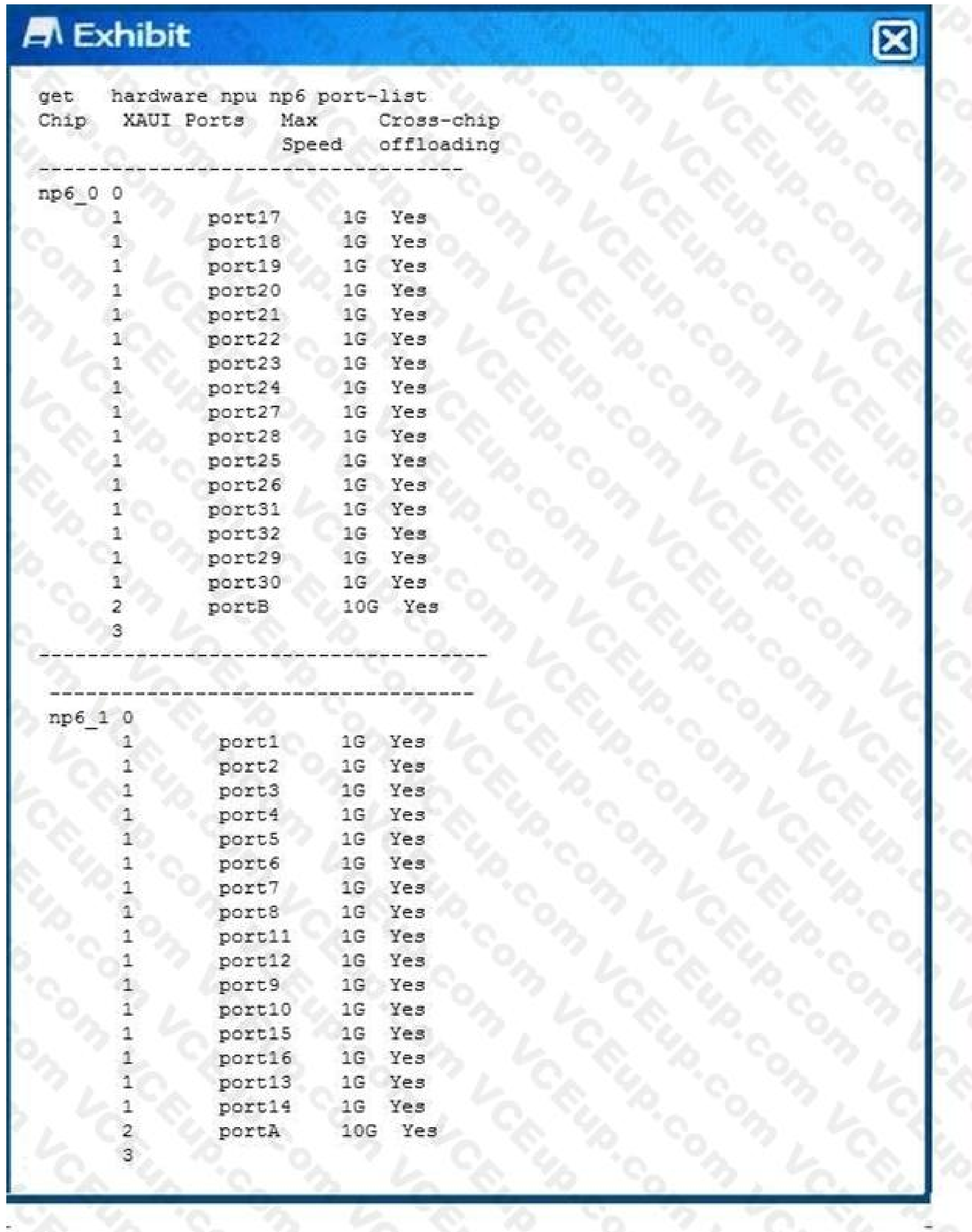
Referring to the exhibit, a FortiADC is load balancing IPv4 traffic between two next-hop routers. The FortiADC does not know the IP addresses of the servers. Also, the FortiADC is doing Layer 7 content inspection and modification.
In this scenario, which application delivery control is configured in the FortiADC?

A. Layer 2
B. Layer 3
C. Laye.4
D. Layer 7

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
Exhibit
Click the Exhibit button.
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?



Exhibit

```
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
       1       port14    1G  Yes
       2       portA     10G  Yes
       3
```

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:
Explanation:
https://kb.fortinet.com/kb/microsites/search.do?cmd=displayKC&docType=kc&externalId=FD41406

QUESTION 22
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?

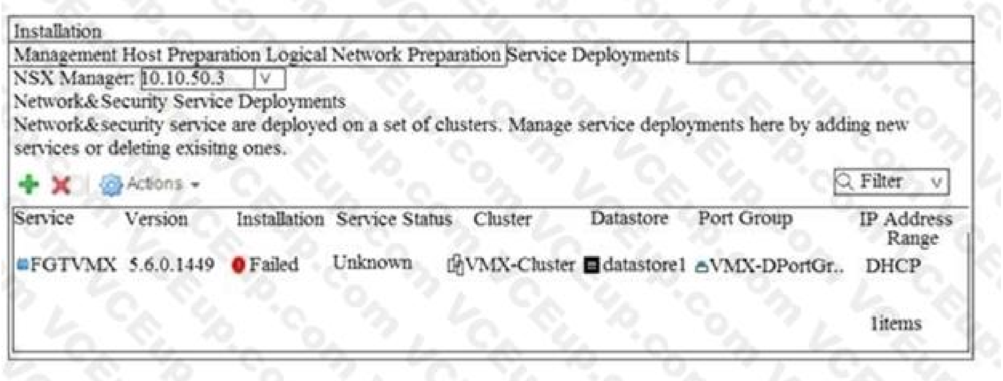
A. Make sure Terminal Service is using the correct DNS ever.

B. Configure FSSO Advanced with LDAP integration
C. Change the FSSO polling mode to windows NetAPI
D. Install the TS/Citrix on the terminal server

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
Exhibit



Installation

Management Host Preparation Logical Network Preparation Service Deployments

NSX Manager: 10.10.50.3

Network&Security Service Deployments

Network&security service are deployed on a set of clusters. Manage service deployments here by adding new services or deleting exisitng ones.

Service	Version	Installation	Service Status	Cluster	Datastore	Port Group	IP Address Range
FGTVMX	5.6.0.1449	Failed	Unknown	VMX-Cluster	datastore1	VMX-DPortGr..	DHCP

1items

When deploying a new FortiGate-VMX Security node, an administrator received the error message shown in the exhibit In this scenario, which statement is correct?

A. The NSX Manager is not able to connect on the FortiGate Service Manager RestAPI service.
B. The vCenter is not able to locate the FortiGate-VMX OVF file.
C. The FortiGate Service Manager does not have the proper permission to register the FortiGate-VMX Service.
D. The vCenter cannot connect to the FortiGate Service Manager.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

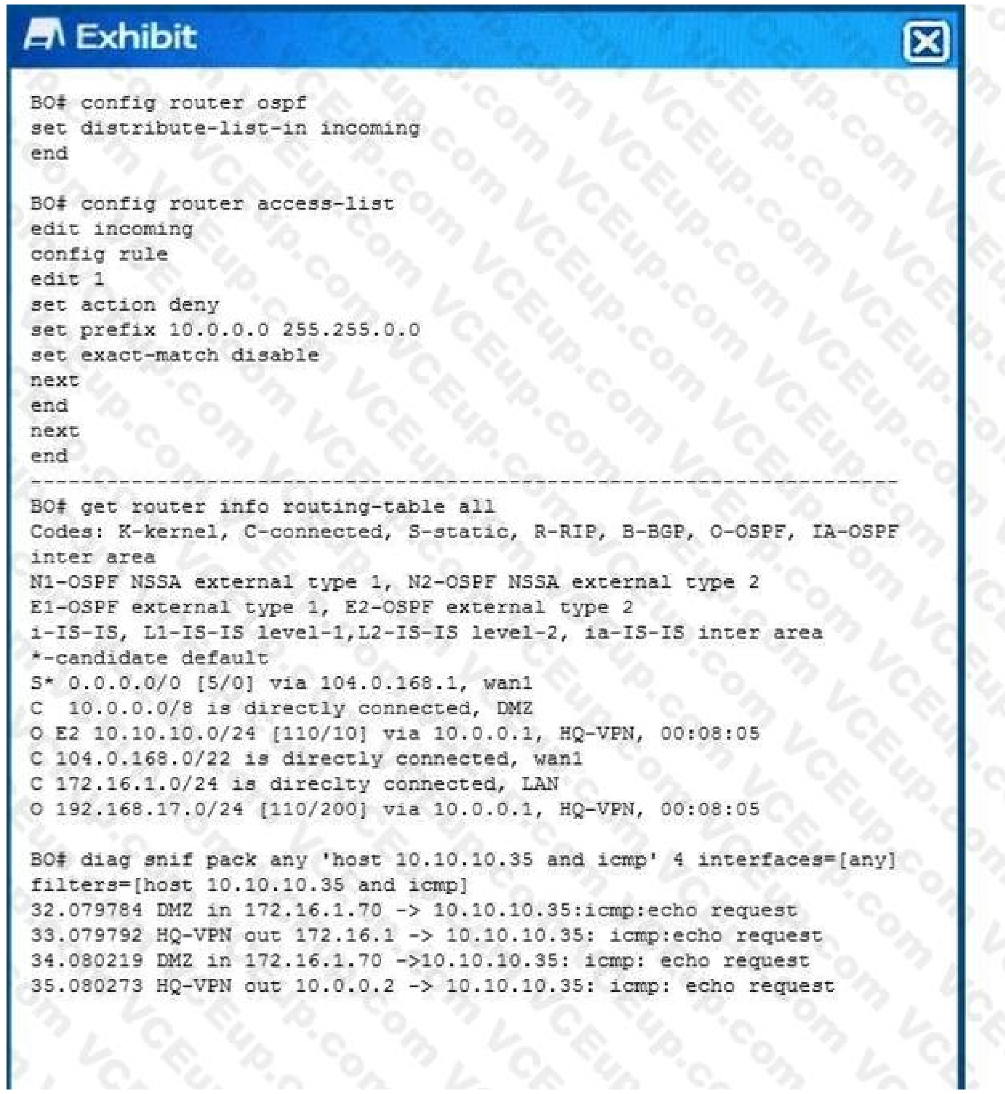
QUESTION 24
You have a customer experiencing problem with a legacy L3L4 firewall device and IPV6 SIP VoIP traffic. They devices is dropping SIP packets, consequently, it process SIP voice calls. Which solution would solve the customer's problem?

A. Replace their legacy device with a FortiGate and deploy a FortiVoice to extract information from the body of the IPv6 SIP packet.
B. Deploy a FortiVoice and enable IPv6 SIP.
C. Deploy a FortiVoice and enable an IPv6 SIP session helper.
D. Replace their legacy device with a FortiGate and configure it to extract information from the body of the IPv6 SIP packet.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
Click the exhibit.
A VPN IPsec is connecting the headquarters office (HQ) with a branch office (BO) and OSPF is used to redistribute routes between the offices. After deployment, a server with IP address 10.10.10.35 located on the DMZ network of the BO FortiGate, was reported unreachable from hosts located on the LAN network of the same FortiGate.



```
BO# config router ospf
set distribute-list-in incoming
end

BO# config router access-list
edit incoming
config rule
edit 1
set action deny
set prefix 10.0.0.0 255.255.0.0
set exact-match disable
next
end
next
end
---------------------------------------------------------------------
BO# get router info routing-table all
Codes: K-kernel, C-connected, S-static, R-RIP, B-BGP, O-OSPF, IA-OSPF
inter area
N1-OSPF NSSA external type 1, N2-OSPF NSSA external type 2
E1-OSPF external type 1, E2-OSPF external type 2
i-IS-IS, L1-IS-IS level-1,L2-IS-IS level-2, ia-IS-IS inter area
*-candidate default
S* 0.0.0.0/0 [5/0] via 104.0.168.1, wan1
C  10.0.0.0/8 is directly connected, DMZ
O E2 10.10.10.0/24 [110/10] via 10.0.0.1, HQ-VPN, 00:08:05
C 104.0.168.0/22 is directly connected, wan1
C 172.16.1.0/24 is direclty connected, LAN
O 192.168.17.0/24 [110/200] via 10.0.0.1, HQ-VPN, 00:08:05

BO# diag snif pack any 'host 10.10.10.35 and icmp' 4 interfaces=[any]
filters=[host 10.10.10.35 and icmp]
32.079784 DMZ in 172.16.1.70 -> 10.10.10.35:icmp:echo request
33.079792 HQ-VPN out 172.16.1 -> 10.10.10.35: icmp:echo request
34.080219 DMZ in 172.16.1.70 ->10.10.10.35: icmp: echo request
35.080273 HQ-VPN out 10.0.0.2 -> 10.10.10.35: icmp: echo request
```

Referring to the exhibit, which statement is true?

A. The ICMP packets are Being blocked by an implicit deny policy.
B. The incoming access list should have an accept action instead deny action to solve the problem.
C. A directly connected subnet is being partially superseded by an OSPF redistributed subnet.
D. Enabling NAT on the VPN firewall policy will solve the problem.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

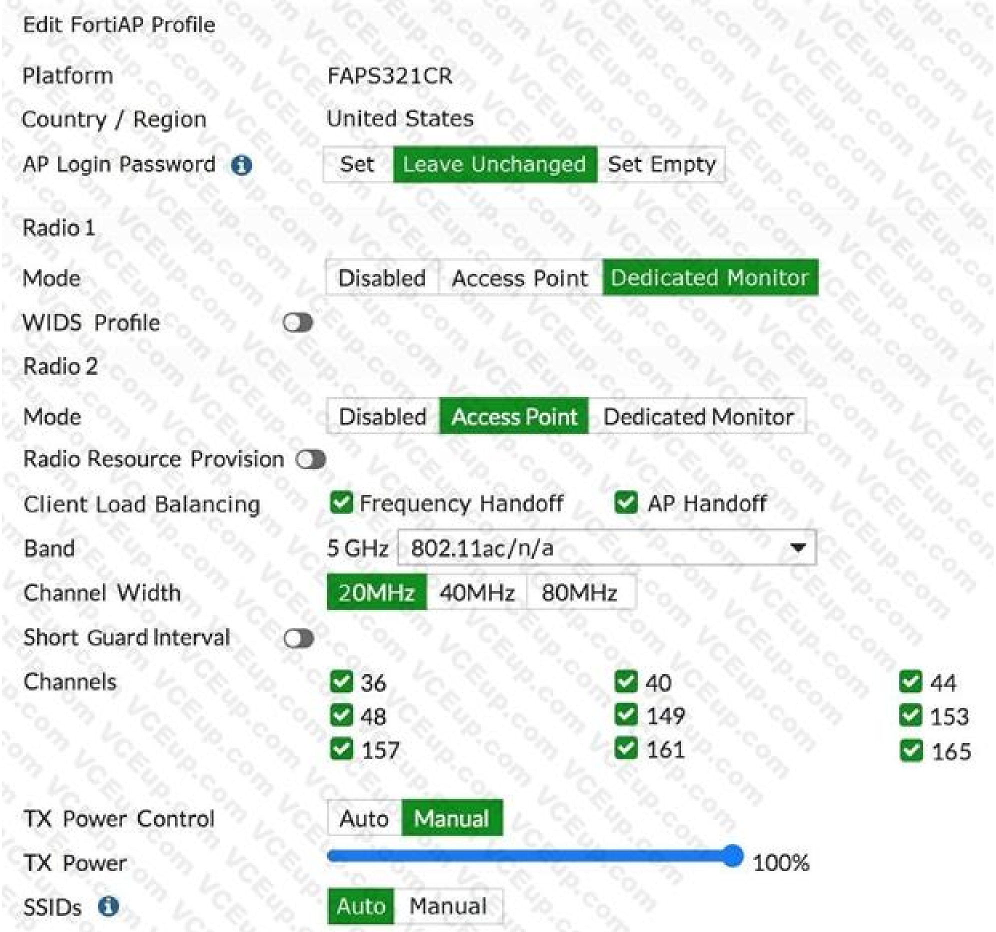
QUESTION 26
A customer has a SCADA environmental control device that is triggering a false-positive IPS alert whenever the Web GUI of the device is accessed. You cannot create a functional custom IPS filter to exempt this behavior, and it appears that the device is so old that it does not have HTTPS support.
You need to prevent the false positive IPS alerts from occurring.
In this scenario, which two actions will accomplish this task? (Choose two.)

A. Create a URL filter with the Exempt action for that device IP address.
B. Change the relevant firewall policies to use SSL certificate-inspection instead of SSL deepinspection.
C. Create a very specific firewall policy for that device IP address which does not perform IPS scanning.
D. Reconfigure the FortiGate to operate in proxy-based inspection mode instead of flow-based.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
Refer to the exhibit.



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

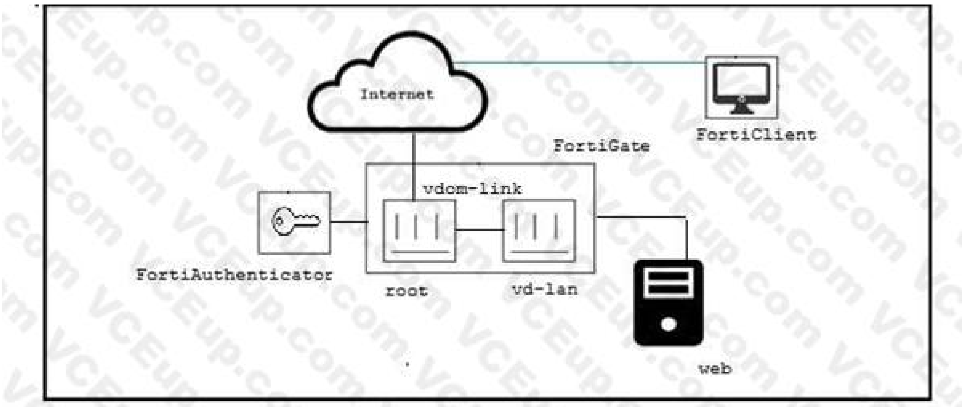
The FortiAP profile used by the FortiGate managed AP is shown in the exhibit.
Which two statements in this scenario are correct? (Choose two.)

A. Interference will be prevented between FortiAP devices using this profile.
B. This profile will map specific SSIDs available to the FortiAP devices.
C. All FortiAP devices using this profile will have Radio 1 monitor wireless clients.
D. All FortiAP devices using this profile will have Radio 1 scan rogue access points.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://docs.fortinet.com/document/fortiap/6.2.0/fortiwifi-and-fortiap-configurationguide/140799/creating-a-fortiap-profile

QUESTION 28
Exhibit



The exhibit shows a topology where a FortiGate is two VDOMS, root and vd-vlasn. The root VDCM provides SSL-VPN access, where the users authenticated by a FortiAuthenticatator. The vd-lan VDOM provids internal access to a Web server. For the remote users to access the internal web server, there are a few requirements, which are shown below.
--At traffic must come from the SSI-VPN
--The vd-lan VDOM only allows authenticated traffic to the Web server.
-- Users must only authenticate once, using the SSL-VPN portal.
-- SSL-VPN uses RADIUS-based authentication. referring to the exhibit, and the requirement describe above, which two statements are true?
(Choose two.)

A. vd-lan authentication messages from root using FSSO.
B. vd-lan connects to Fort authenticator as a regular FSSO client.
C. root is configured for FSSO while vd-lan is configuration for RSSO.
D. root sends “RADIUS Accounting Messages" to FortiAuthenticator.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

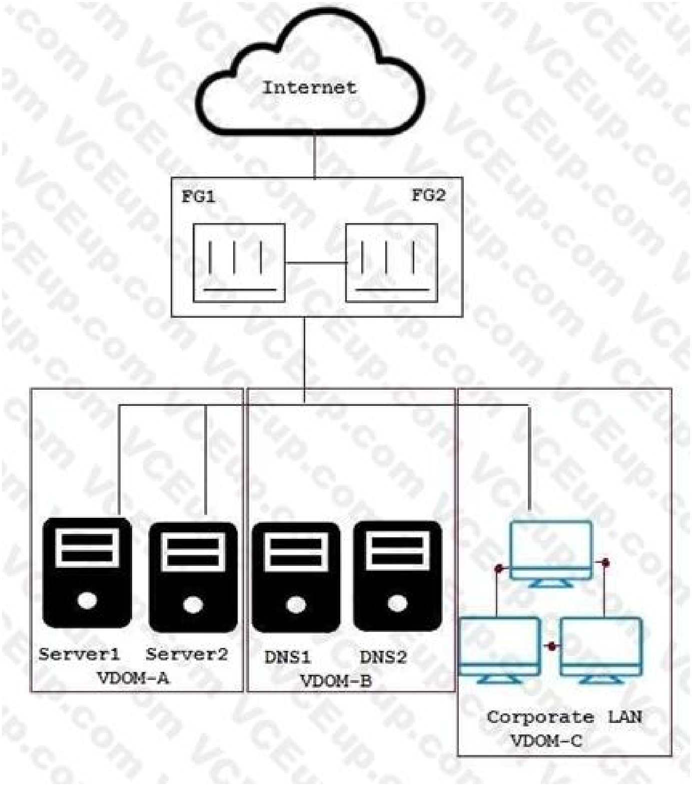
QUESTION 29
Your client wants to use a central RADIUS server for management authentication when connecting to the FortiGate GUL and provide different levels of access for different types of employees.
Which three actions required providing the requested functionality? (Choose three.)

A. Create a wildcard administrator on the FortiGate.
B. Enable radius-vdom-override in the CLI.
C. Create multiple administrator profiles with matching RADIUS VSAs.
D. Enable accprofile-override in the CLI.
E. Set the RADIUS authentication type to MS-CHAPv2.

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://kb.fortinet.com/kb/documentLink.do?externalID=FD36127

QUESTION 30
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. FortiDDoS between FG1 and FG2 and the Internet
B. FortiADC for VDOM-A
C. FortiWeb for VDOM-A
D. FortiADC for VDOM-B
E. FortiDDoS between FG1 and FG2 and VDOMs

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:

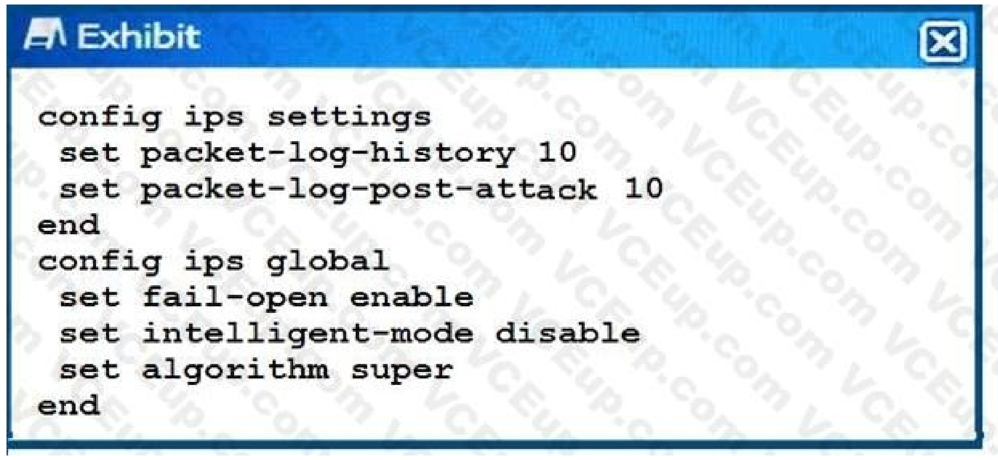
QUESTION 31
In a FortiGate 5000 series, two FortiControllers are working as an SLBC cluster in a-p mode. The configuration shown below is applied. config load-balance session-setup set tcp-ingress enable end When statement is true on how new TCP sessions are handled by the Distributor Processor (DP)?

A. The new session added the DP session table is automatically deleted, if the traffic is denied by the processing worker.
B. No new session is added is the DP session table until the processing worker accepts the traffic.
C. A new session added m the DP session table remains in the table remain in the traffic is denied by the procession worker.
D. A new session added in the OP session table remains is the table only if traffic is traffic is accepted by the processing worker.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
Exhibit



```
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
```

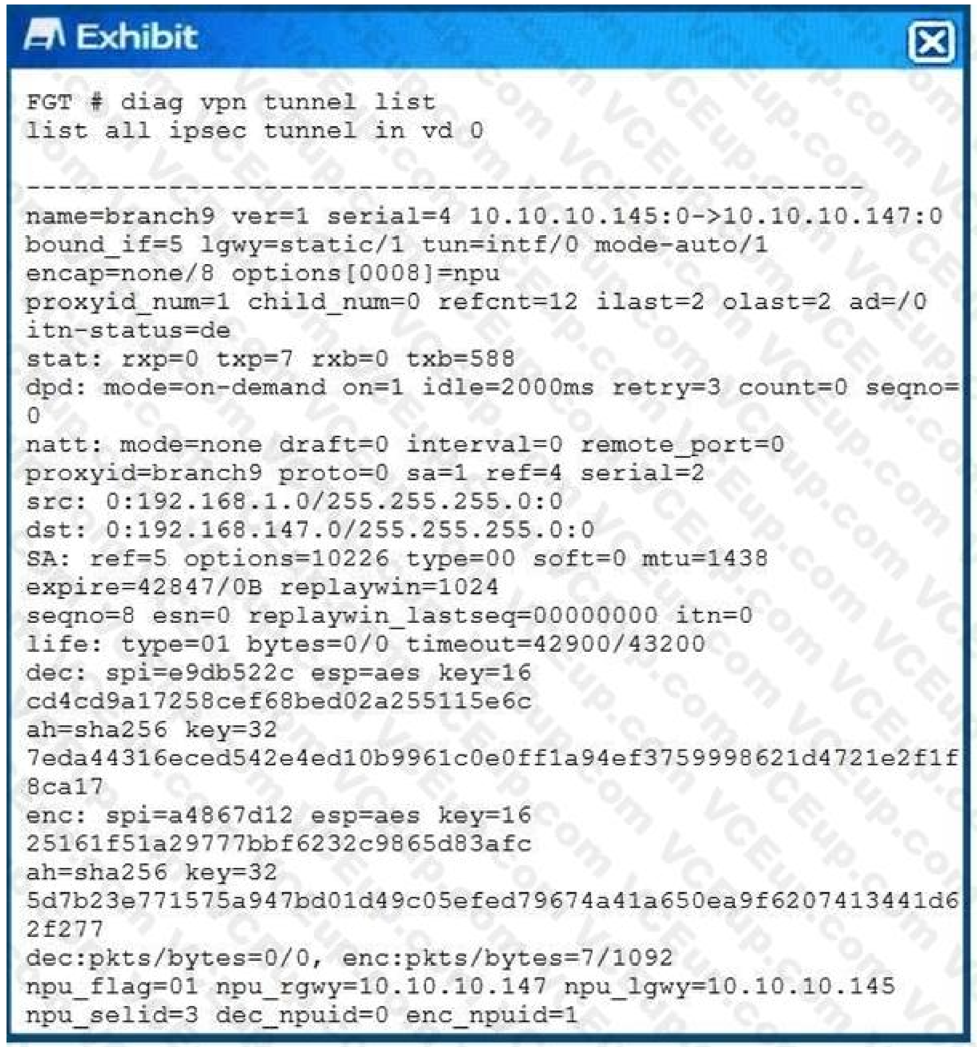
An Administrator reports continuous high CPU utilization on a FortiGate device due to the IPS engine.
The exhibit shows the global IPS configuration. Which two configuration actions will reduce the CPU usage? (Choose two.)

A. Disable fail open.
B. Enable intelligent mode.
C. Change the algorithm to low.
D. Reduce the number of packets logged.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
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.

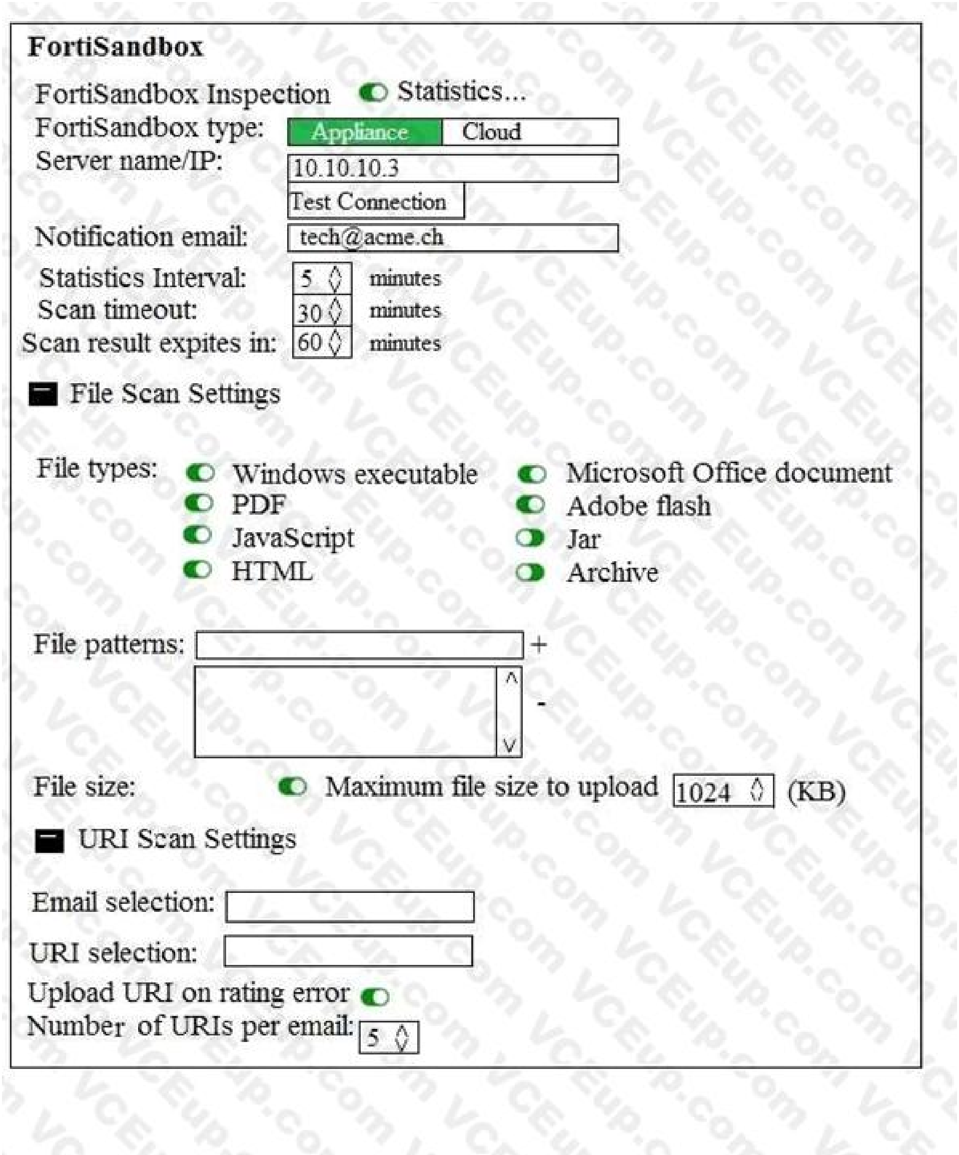
C. Traffic is not offloaded.

D. Outgoing traffic is offloaded: incoming traffic not offloaded.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://kb.fortinet.com/kb/documentLink.do?externalID=FD36203

QUESTION 34
Click the Exhibit button.
You have installed a FortiSandbox and configured it in your FortiMail. Referring to the exhibit, which two statements are correct? (Choose two.)



FortiSandbox

FortiSandbox Inspection ● Statistics...

FortiSandbox type: [✓ Appliance] Cloud

Server name/IP: 10.10.10.3

Test Connection

Notification email: tech@acme.ch

Statistics Interval: 5 minutes

Scan timeout: 30 minutes

Scan result expires in: 60 minutes

File Scan Settings

File types:
- ● Windows executable
- ● PDF
- ● JavaScript
- ● HTML
- ● Microsoft Office document
- ● Adobe flash
- ○ Jar
- ○ Archive

File patterns:

File size: ● Maximum file size to upload 1024 (KB)

URI Scan Settings

Email selection:

URI selection:

Upload URI on rating error ●

Number of URIs per email: 5

A. FortiMail will cache the results for 30 minutes.

B. FortiMail will wait for 30 minutes to obtain the scan results.

C. If the FortiSandbox with IP 10.10 10 3 is not available, the e-mail will be checked by the FortiCloud Sandbox.

D. If FortiMail is not able to obtain the results from the fortiGuard quenes. URIs will not be checked by the FortiSandbox.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

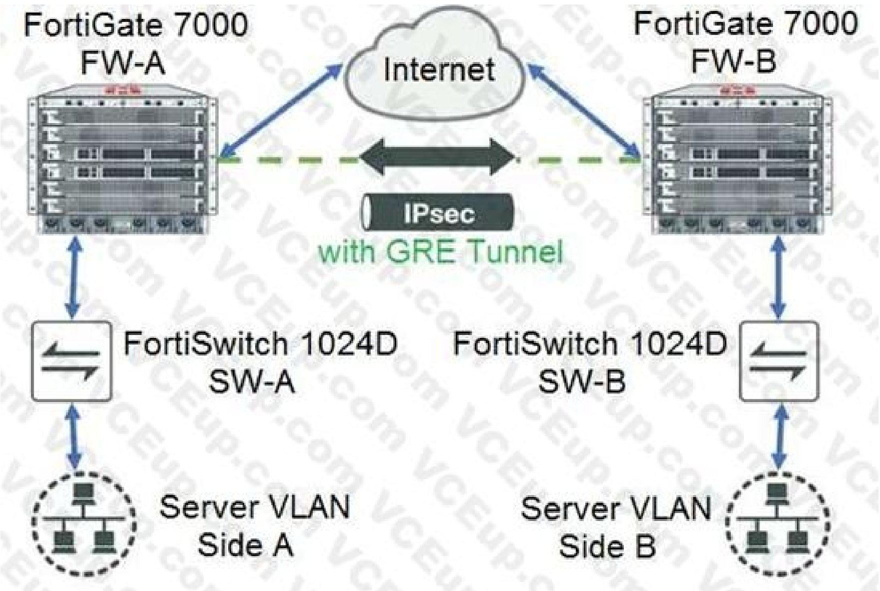
QUESTION 35
A FortiGate with the default configuration shown below is deployed between two IP telephones. FortiGate receives the INVITE request shown in the exhibit from Phone A (internal) to Phone B (external).
NVITE sip:PhoneB@172.20.120.30 SIP/2.0
Via: SIP/2.0/UDP 10.31.101.20:5060
From: PhoneA <sip:PhoneA@10.31.101.20>
To: PhoneB <sip:PhoneB@172.20.120.30>
Call-ID: 314159@10.31.101.20
CSeq: 1 INVITE
Contact: sip:PhoneA@10.31.101.20 v=0 o=PhoneA 5462346 332134 IN IP4 10.31.101.20 c=IN IP4 10.31.101.20 m=audio 49170 RTP 0 3 Which two statements are correct after the FortiGate receives the packet? (Choose two.)

A. NAT takes place only in the SIP application layer.
B. A pinhole will be opened to accept traffic sent to the FortiGate WAN IP address.
C. NAT takes place at both the network and SIP application layers.
D. A pinhole is not required to accept traffic sent to the FortiGate WAN IP address.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
Refer to the exhibit.



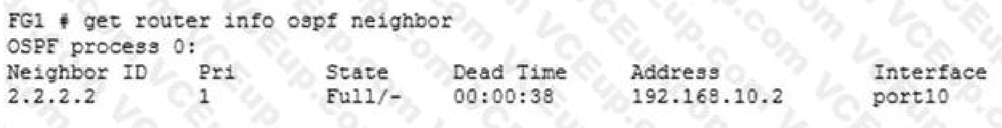
You have two data centers with a FortiGate 7000-series chassis connected by VPN. All traffic flows over an established generic routing encapsulation (GRE) tunnel between them. You are troubleshooting traffic that is traversing between Server VLAN A and Server VLAN B. The performance is lower than expected and you notice all traffic is only going through the FPM in slot 3 while nothing through the FPM in slot 4.
Referring to the exhibit, which statement is true?

A. Removing traffic shaping from the firewall policy allowing this traffic will allow for load-balancing to the other module.
B. Changing the algorithm to take source IP, destination IP and port into account will load balance this traffic to the other module.
C. There is no way to load-balance the traffic in this scenario.
D. Configuring a load-balance flow-rule in the CLI will load-balance this traffic.

Correct Answer: D
Section: (none)
Explanation

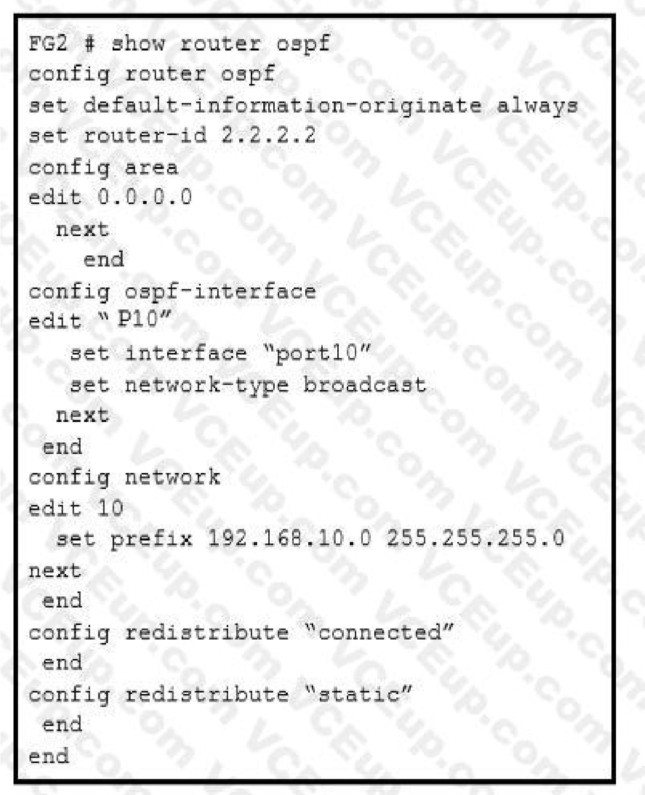
Explanation/Reference:

QUESTION 37
Click the Exhibit button.
Your customer is using dynamic routing to exchange the default route between two FortiGates using OSPFv2. The output of the get router info ospf neighbor command shows that the neighbor is up, but the default route does not appear in the routing neighbor shown below:



```
FG1 # get router info ospf neighbor
OSPF process 0:
Neighbor ID     Pri        State       Dead Time      Address           Interface
2.2.2.2         1          Full/-      00:00:38       192.168.10.2      port10
```

According to the exhibit, what is causing the problem?



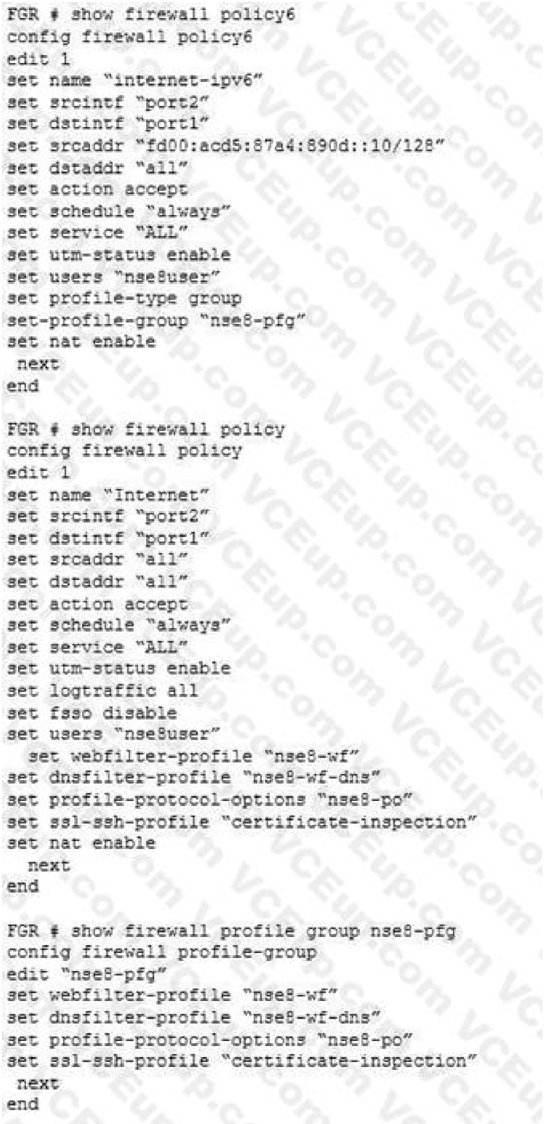
```
FG2 # show router ospf
config router ospf
set default-information-originate always
set router-id 2.2.2.2
config area
edit 0.0.0.0
  next
    end
config ospf-interface
edit " P10"
   set interface "port10"
   set network-type broadcast
  next
 end
config network
edit 10
  set prefix 192.168.10.0 255.255.255.0
next
 end
config redistribute "connected"
 end
config redistribute "static"
 end
end
```

A. A prefix for the detail route is missing
B. OSPF requires the redistribution of connected networks.
C. There is an OSPF interface network-type mismatch.
D. FG2 is within the wrong OSPF area.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
Click the Exhibit button. Referring to the exhibit, which two statements are true? (Choose two.)



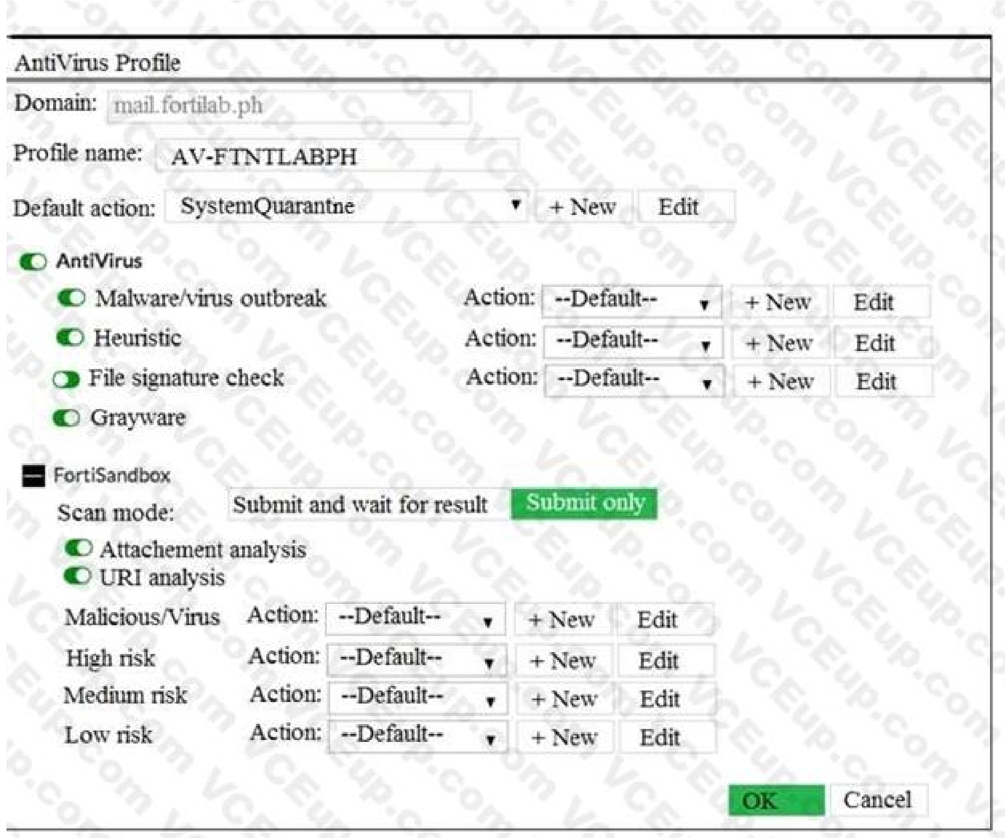
```
FGR # show firewall policy6
config firewall policy6
edit 1
set name "internet-ipv6"
set srcintf "port2"
set dstintf "port1"
set srcaddr "fd00:acd5:87a4:890d::10/128"
set dstaddr "all"
set action accept
set schedule "always"
set service "ALL"
set utm-status enable
set users "nse8user"
set profile-type group
set-profile-group "nse8-pfg"
set nat enable
 next
end

FGR # show firewall policy
config firewall policy
edit 1
set name "Internet"
set srcintf "port2"
set dstintf "port1"
set srcaddr "all"
set dstaddr "all"
set action accept
set schedule "always"
set service "ALL"
set utm-status enable
set logtraffic all
set fsso disable
set users "nse8user"
  set webfilter-profile "nse8-wf"
set dnsfilter-profile "nse8-wf-dns"
set profile-protocol-options "nse8-po"
set ssl-ssh-profile "certificate-inspection"
set nat enable
  next
end

FGR # show firewall profile group nse8-pfg
config firewall profile-group
edit "nse8-pfg"
set webfilter-profile "nse8-wf"
set dnsfilter-profile "nse8-wf-dns"
set profile-protocol-options "nse8-po"
set ssl-ssh-profile "certificate-inspection"
 next
end
```

A. The IPv4 traffic for nse8user is filtered using the DNS profile.
B. The IPv6 traffic for nse8user is filtered using the DNS profile.
C. The IPv4 policy is allowing security profile groups.
D. The Web traffic for nse8user is being filtered differently in IPv4 and IPv6.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
Click the Exhibit button.
Referring to the exhibit, what will happen if FortiSandbox categorizes an e-mail attachment submitted by FortiMail as a high risk?



AntiVirus Profile

Domain: mail.fortilab.ph

Profile name: AV-FTNTLABPH

Default action: SystemQuarantne ▾ + New Edit

AntiVirus

- Malware/virus outbreak Action: --Default-- ▾ + New Edit
- Heuristic Action: --Default-- ▾ + New Edit
- File signature check Action: --Default-- ▾ + New Edit
- Grayware

FortiSandbox

Scan mode: Submit and wait for result [✓ Submit only]

- Attachement analysis
- URI analysis

Malicious/Virus	Action:	--Default-- ▾	+ New	Edit
High risk	Action:	--Default-- ▾	+ New	Edit
Medium risk	Action:	--Default-- ▾	+ New	Edit
Low risk	Action:	--Default-- ▾	+ New	Edit

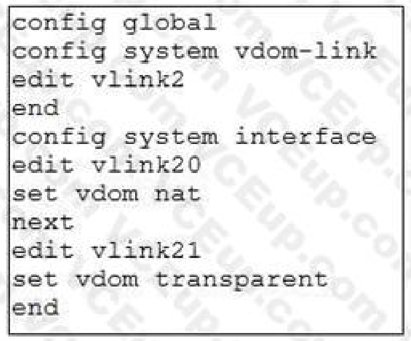
OK Cancel

A. The high-risk file will be discarded by attachment analysis.
B. The high-risk tile will go to the system quarantine.
C. The high-risk file will be received by the recipient.
D. The high-risk file will be discarded by malware/virus outbreak protection.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
Click the Exhibit button.
What are two ways to establish communication between an existing NAT VDOM and a new transparent VDOM? (Choose two.)



```
config global
config system vdom-link
edit vlink2
end
config system interface
edit vlink20
set vdom nat
next
edit vlink21
set vdom transparent
end
```

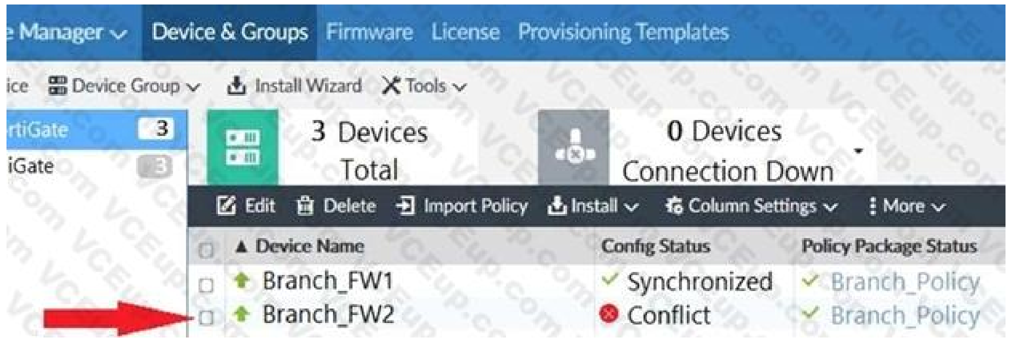
A. Set the set ip 10.10.10. i command to vlink2l.
B. Set type ppp to the vdom-link, vlink2.
C. Set the not ip 10.I0.I0.1 command to vlink20.

D. Set type ethernet to the vdom-link, vlink2.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://help.fortinet.com/fos50hlp/52data/Content/FortiOS/fortigate-virtual-domains-52/inter-VDOM.htm#NAT

QUESTION 41
Refer to the exhibit.



Device Name	Config Status	Policy Package Status
Branch_FW1	✓ Synchronized	✓ Branch_Policy
Branch_FW2	● Conflict	✓ Branch_Policy

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

A. The device configuration was changed on the local FortiGate side only; auto-update is disabled.

B. The changed configuration on the FortiGate will remain the next time that the device configuration is pushed from FortiManager.

C. The device configuration was changed on both the local FortiGate side and the FortiManager side; autoupdate is disabled.

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: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
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-mails 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.

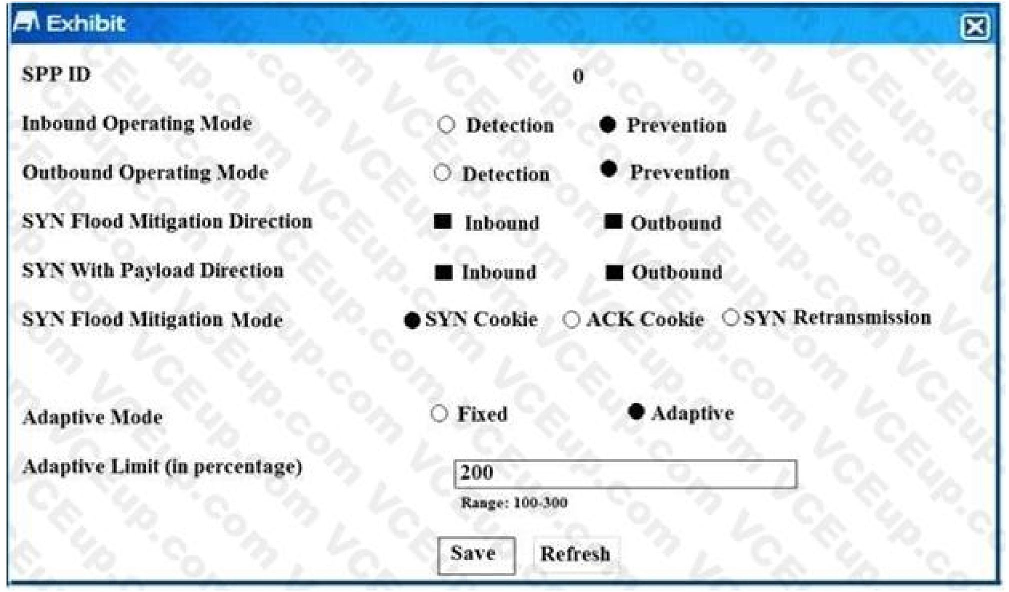
D. Configure access control rules.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
Exhibit
Click the Exhibit button.
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.)



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		

A. Traffic that does match any spp policy will not be inspection by this spp.
B. FortiDDos will not send a SYNACK if a SYN packet is coming from an IP address that is not the legtimate IP (LIP) address table.
C. FortiDooS will start dropping packets as soon as the traffic executed the configured maintain threshold.
D. SYN packets with payloads will be drooped.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://help.fortinet.com/fddos/4-3-0/FortiDDoS/Configuring_SPP_settings.htmSYN cookie—Sends a SYN/ACK with a cookie value in the TCP sequence field. If it receives an ACKback with the right cookie, an RST/ACK packet is sent and the IP address is added to the legitimate IPaddress table. If the client then retries, it succeeds in making a TCP connection.
So apparently, the very first SYN/ACK with a cookie value is sent when the IP address is not in the legitimate IP address table yet.

QUESTION 44
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@fortinet 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@fortinet.com

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://help.fortinet.com/fmail/5-3-6/admin/index.html#page/FortiMail_Online_Help/policy_09_10.html

QUESTION 45
You must create a high Availability deployment with two FortiWebs in Amazon Services (AWS): each on different Availability Zones(AZ) from the same region. At the same time, each FortiWeb should be able to deliver content from the Web server of both of the AZs. Which deployment would will this requirement?

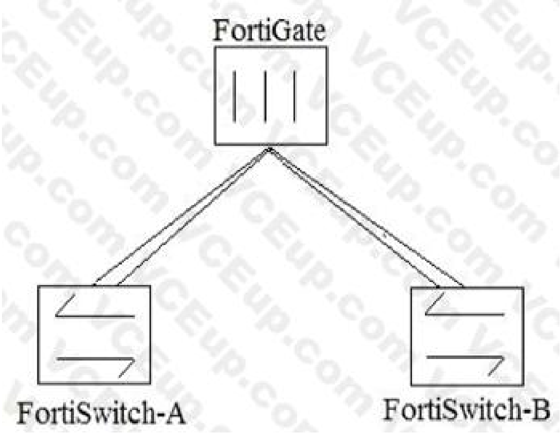
A. Configure the FortiWebs Active-Active Ha mode and use AWS Router 53 load Router balance the internal Web servers.
B. Configure the FortiWebs in Active-Active HA mode and use AWS Elastic load Balancer (ELB) for the internal Web servers.
C. Use AWS Router 53 to load balance FortiWebs in standone mode and use AWS Virtual private Cloud (VPC) peering to load balance the internal Web servers.

D. Use AWS Elastic load Balancer (ELB) for both FortiWebs in standdone mode and the internal Web servers in an ELB sandwich.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-aws-automatically-scalecloud-security.pdf

QUESTION 46
Click the Exhibit button. An administrator implements a multi-chassis link aggregation (MCLAG) solution using two FortiSwitch 448Ds and one FortiGate 3700D. As describes in the network topology shown in the exhibit, two links are connected to each FortiSwitch. What is requires to implement this solution? (Choose two.)

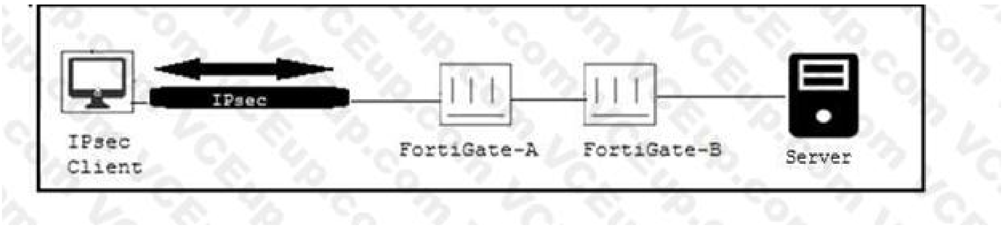


A. Replace the FortiGate as this one does not have an ISF.
B. Create two separate link aggregated (LAG) interfaces on the FortiGate side for each FortiSwitch.
C. Add set fortilink-split-interface disable on the FortiLink interface.
D. An ICL link between both FortiSwitch devices needs to be added.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
Click the Exhibit button.



Only users authenticated in FortiGate-B can reach the server. A customer wants to deploy a single sign-on solution for IPsec VPN users. Once a user is connected and authenticated to the VPN in FortiGate-A, the user does not need to authenticate again in FortiGate –B to reach the server.
Which two actions satisfy this requirement? (Choose two.)

A. Use Kerberos authentication.
B. FortiGate-A must generate a RADUIS accounting packets.
C. Use FortiAuthenticator.
D. Use the Collector Agent.

Correct Answer: BC
Section: (none)

Explanation

Explanation/Reference:

QUESTION 48
A FortOS devices is used for termination of VPNs for number of remote spoke VPN units (designated group A spokes) using a phase 1 main mode dial-up tunnel using pre-shared. Your company recently acquired another organization. You are asked establish VPN correctively for the newly acquired organization's sites which new devices will be provisioned (designated Group B spokes). Both exiting
(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 permission than your existing VPN spokes (Group A).
Which two solutions meet the represents for the new spoke group? (Choose two.)

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

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

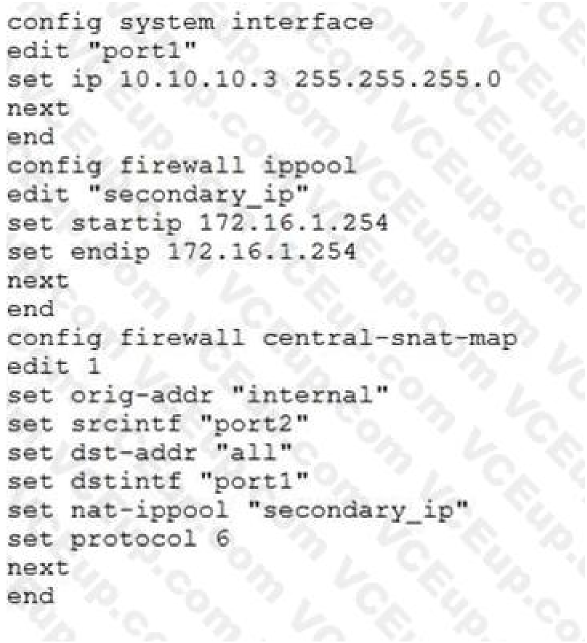
QUESTION 49
You configured a firewall policy with only a Web filter profile for accessing the Internet. Access to websites belonging to the "Information Technology" category are blocked and to the "Business" category are allowed. SSL deep inspection is not enabled on this policy.
A user wants to access the website https://www.it-acme.com which presents a certificate withCN=www.acme.com. The it-acme.com domain is categorized as "Information Technology" and theacme.com domain is categorized as "Business".
Which statement regarding this scenario is correct?

A. The FortiGate is able to read the URL within HTTPS sessions when using SSL certificate inspectionso the website will be blocked by the "Information Technology".
B. The website will be blocked by category "Information Technology" as the SNI takes precedence over the certificate name.
C. The website will be allowed by category "Business" as the certificate name takes precedence over the URL.
D. Only with SSL deep inspection enabled will the FortiGate be able to categorized this website.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
Click the Exhibit button.
Central NAT was configured on a FortiGate firewall. A sniffer shows ICMP packets out to a host on the Internet egresses with the port1 IP address instead of the virtual IP(VIP) that was configured.
Referring to the exhibit, which configuration will ensure that ICMP traffic is also translated?



```
config system interface
edit "port1"
set ip 10.10.10.3 255.255.255.0
next
end
config firewall ippool
edit "secondary_ip"
set startip 172.16.1.254
set endip 172.16.1.254
next
end
config firewall central-snat-map
edit 1
set orig-addr "internal"
set srcintf "port2"
set dst-addr "all"
set dstintf "port1"
set nat-ippool "secondary_ip"
set protocol 6
next
end
```

A. config firewall ippool edit “secondry_ip” set arp-intf ‘port1’ next end

B. config firewall central-snat-map edit 1 set protocol 1 next end

C. config firewall central-snat-map edit 1 unset protocol next end

D. config firewall central-snat-map edit 1 set orig-addr “all” next end

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
A company has just rolled out new remote sites and now you need to deploy a single firewall policy to all of these sites to allow Internet access using FortiManager. For this particular firewall policy, the source address object is called LAN, but its value will change according to the site the policy is being installed.
Which statement about creating the object LAN is correct?

A. Create a new object called LAN and enable per-device mapping.

B. Create a new object called LAN and promote it to the global database.

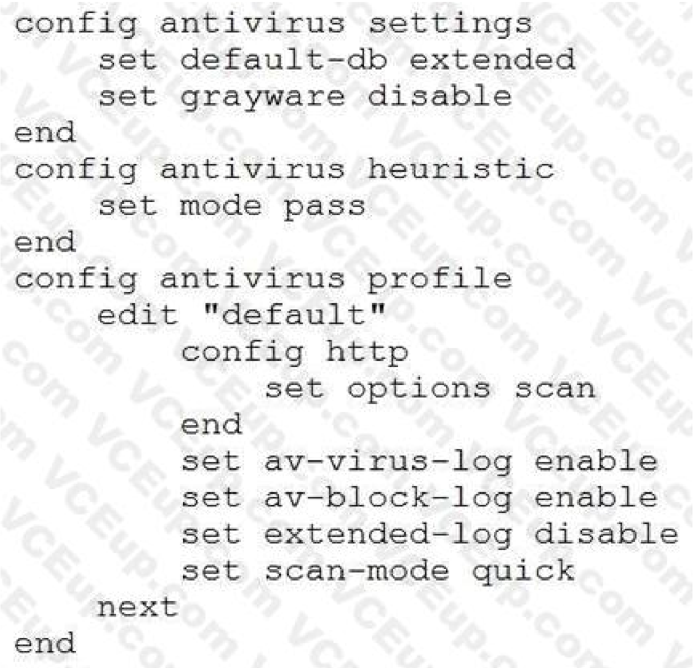
C. Create a new object called LAN and use it as a variable on a TCL script.

D. Create a new object called LAN and set meta-fields per remote site.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
Refer to the exhibit.



```
config antivirus settings
    set default-db extended
    set grayware disable
end
config antivirus heuristic
    set mode pass
end
config antivirus profile
    edit "default"
        config http
            set options scan
        end
        set av-virus-log enable
        set av-block-log enable
        set extended-log disable
        set scan-mode quick
    next
end
```

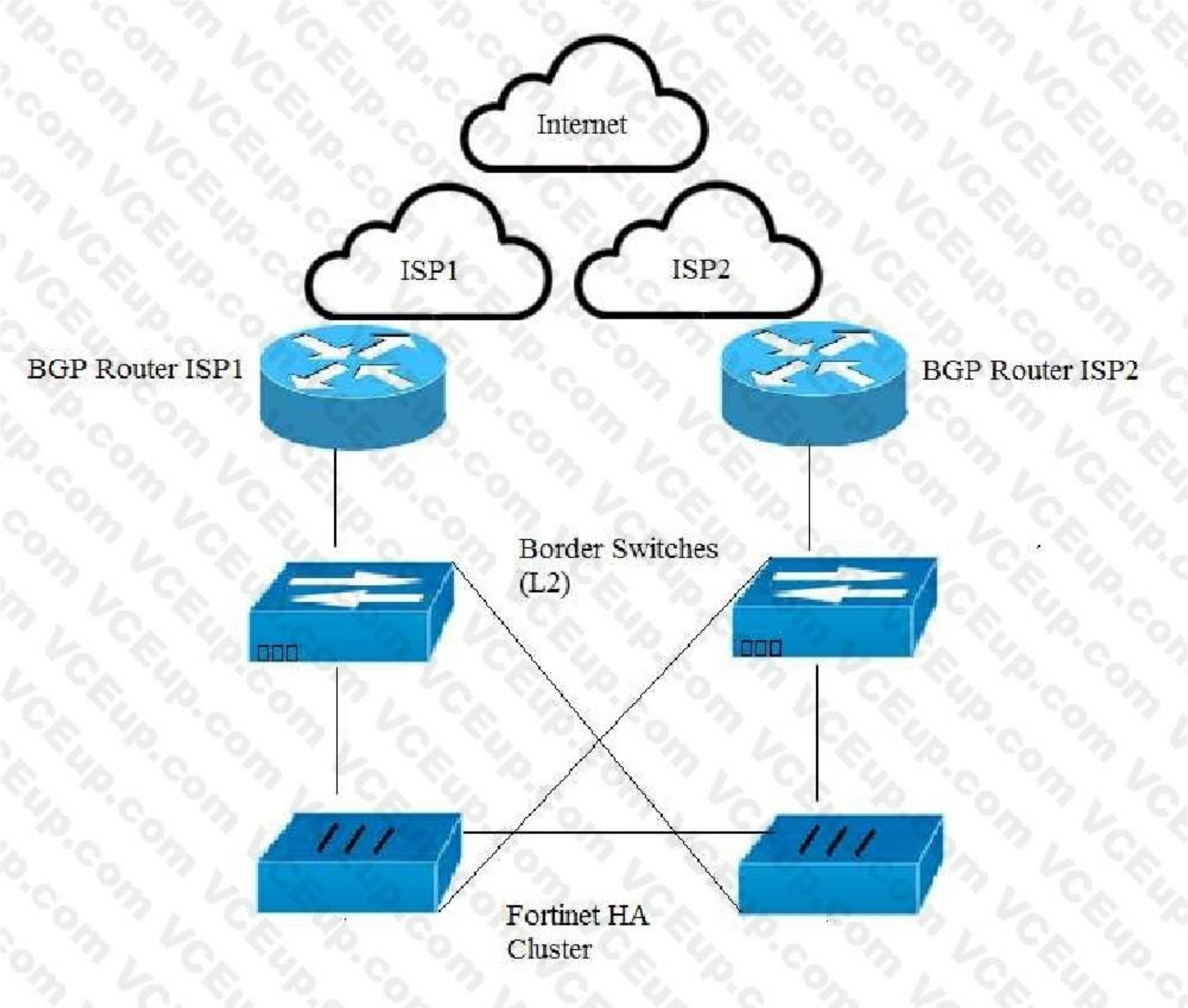
You are working on FortiGate 61E operating in flow-based inspection mode with various settings optimized for performance. The main Internet firewall policy is using the "default" antivirus profile.
You found that some executable virus samples files downloaded over HTTP are not being blocked bythe FortiGate.
Referring to the exhibit, how can this be fixed?

A. Change the set scan-mode configuration to full.
B. Disable the emulator feature.
C. Change the set default-db configuration to extreme.
D. Add set content-disarm enable to the configuration.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
Exhibit



An organization has a FortiGate cluster that is connected to two independent ISPs. You must configure the FortiGate failover for a single ISP failure to occur without disruption.
Referring to the exhibit, which two FortiGate BGP features are enabled to accomplish this task?
(Choose two.)

A. EBGP multipath
B. Graceful restart
C. Synchronization
D. BFD

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
An old router has been replaced by a FortiWAN device. The FortiWAN has inherited the router's management IP address and now the network administrator needs to remove the old router from the FortiSIEM configuration.
Which two statements are true about this operation? (Choose two.)

A. FortiSIEM will discover a new device for the FortiWAN with the same IP.
B. The old router will be completely deleted from FortiSIEM's CMDB.
C. FotiSEIM needs a special syslog for FortiWAN.
D. FortiSIM will move the old router device into the Decommission folder.

Correct Answer: AD

Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://www.fortinetguru.com/2017/05/fortisiem-decommissioning-a-device/

QUESTION 55
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
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 in the head office.
Which action will help to achieve the requirements?

A. Configure a default route and make sure that the FortiGate device can pmg to service fortiguard net.

B. Configure the FortiGuard override server and use the IP address of the FortiManager

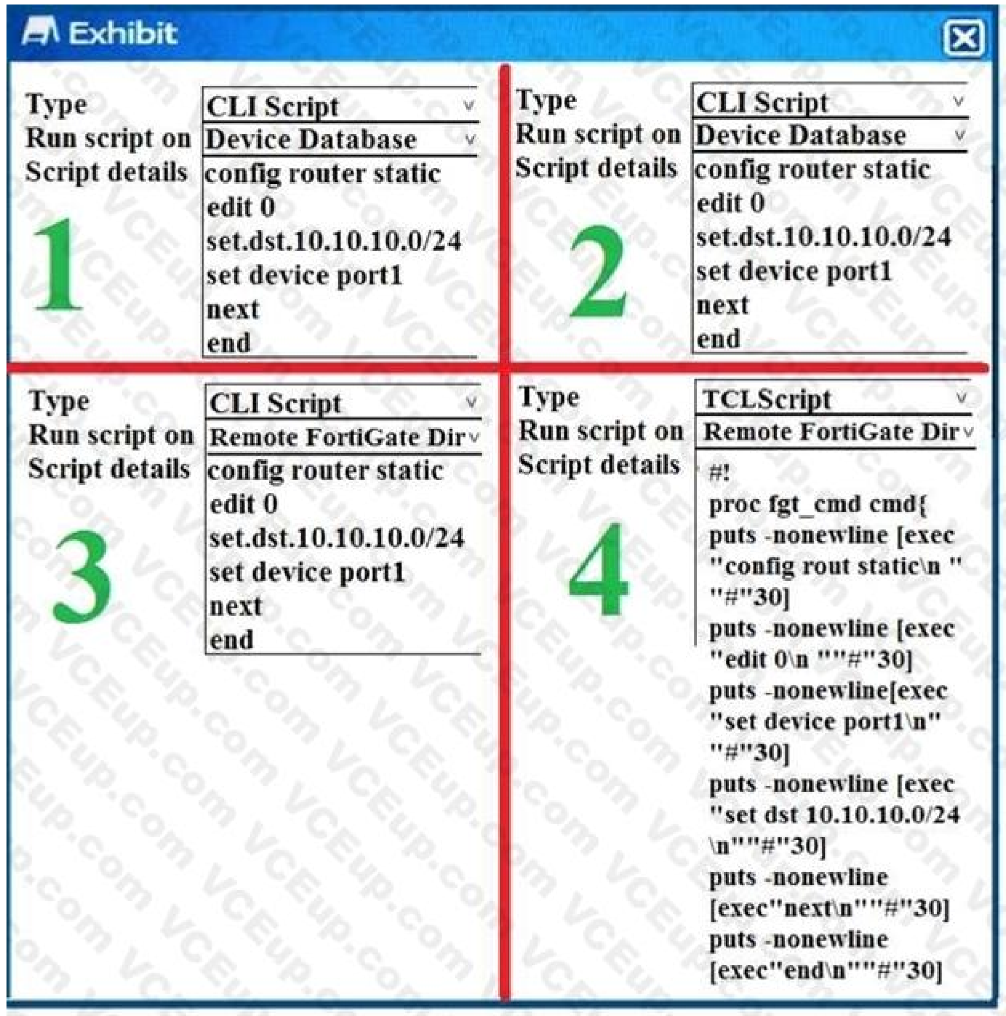
C. Configure the FortiGuard override server and use the IP address of service, fortiguard net.

D. Configure FortiGate to use FortiGuard Filtering Port 8888.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
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.)



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
```

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
```

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
```

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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
You configure an outgoing firewall policy with a web filter for accessing the internet. The access to URL https// itacm.co and web belonging to the same category should be blocked. You notice that the Web server presents a certificate with CN=www acme.com. The www.it.acme site is as " information Technology and the www.acme.com site is categorized as "Business".
Which statements is correct in this scenario?

A. Category "information Technology" needs to blocked, the FortiGate is able to inspection the URL with HTTPS sessions.
B. Category "Business" need a to be block: 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: D
Section: (none)
Explanation

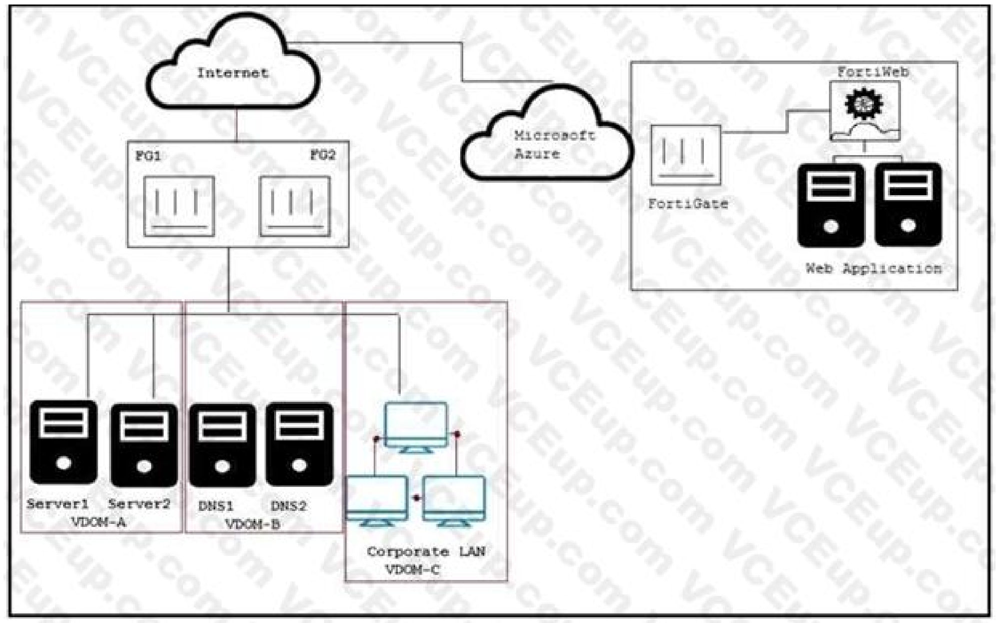
Explanation/Reference:

Explanation:

“FortiOS parses TLS server name indication (SNI) from TSL Client Hello. When this value has been retrieved, it will be used for non-deep web filtering inspection, in preference to the existing HTTPS Server CN web filtering.”

QUESTION 59

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 FotiAnalyzer lor monitor in Azure, FortiSIEM for managemnet, and FortiSandbox for zero day attacks on their local network.

B. Use Fortianalyzer for monitor Azure, FortiSiEM for management, and FortiGate has zero day attacks on their local network.

C. Use FortiManager for management in Azure, FortSIEM for monitoring and FcrtiSandbox for zero day attacks on their local network.

D. Use FortiSIEM for management Azure, FortiManager for management, and FortrGate for zero day attacks on their local network.

Correct Answer: C

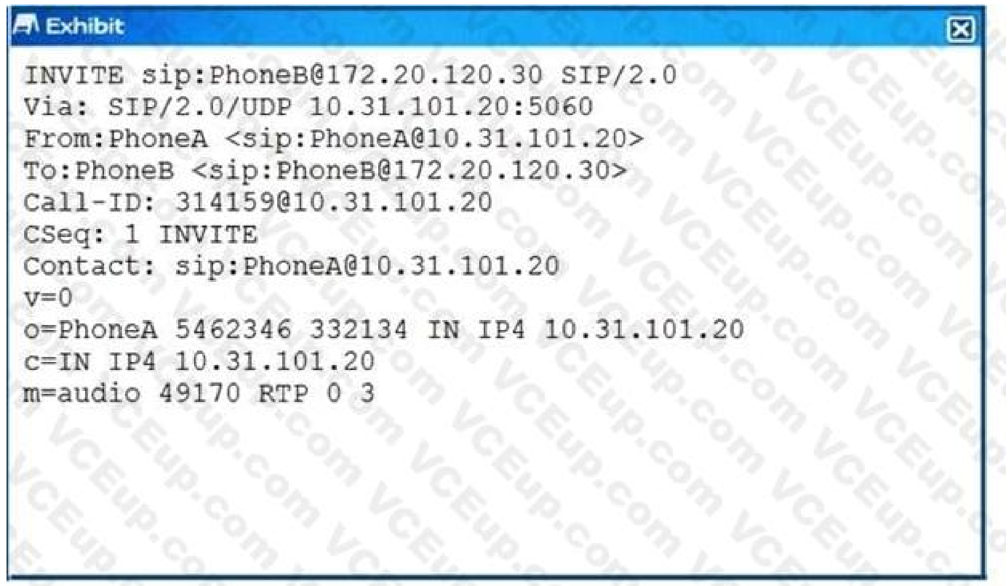
Section: (none)

Explanation

Explanation/Reference:

QUESTION 60

Click the Exhibit button.



```
INVITE sip:PhoneB@172.20.120.30 SIP/2.0
Via: SIP/2.0/UDP 10.31.101.20:5060
From:PhoneA <sip:PhoneA@10.31.101.20>
To:PhoneB <sip:PhoneB@172.20.120.30>
Call-ID: 314159@10.31.101.20
CSeq: 1 INVITE
Contact: sip:PhoneA@10.31.101.20
v=0
o=PhoneA 5462346 332134 IN IP4 10.31.101.20
c=IN IP4 10.31.101.20
m=audio 49170 RTP 0 3
```

Click the Exhibit button.
A FortiGate with the default configuration is deployed between two IP phones. FortiGate receives the INVITE request shown in the exhibit form Phone A (internal)to Phone B (external). Which two actions are taken by the FortiGate after the packet is received? (Choose two.)

A. A pinhole will be opened to accept traffic sent to FortiGate's WAN IP address and ports 49169 and 49170.

B. a pinhole will be opened to accept traffic sent to FortiGate's WAN IP address and ports 49l70 and 49171.

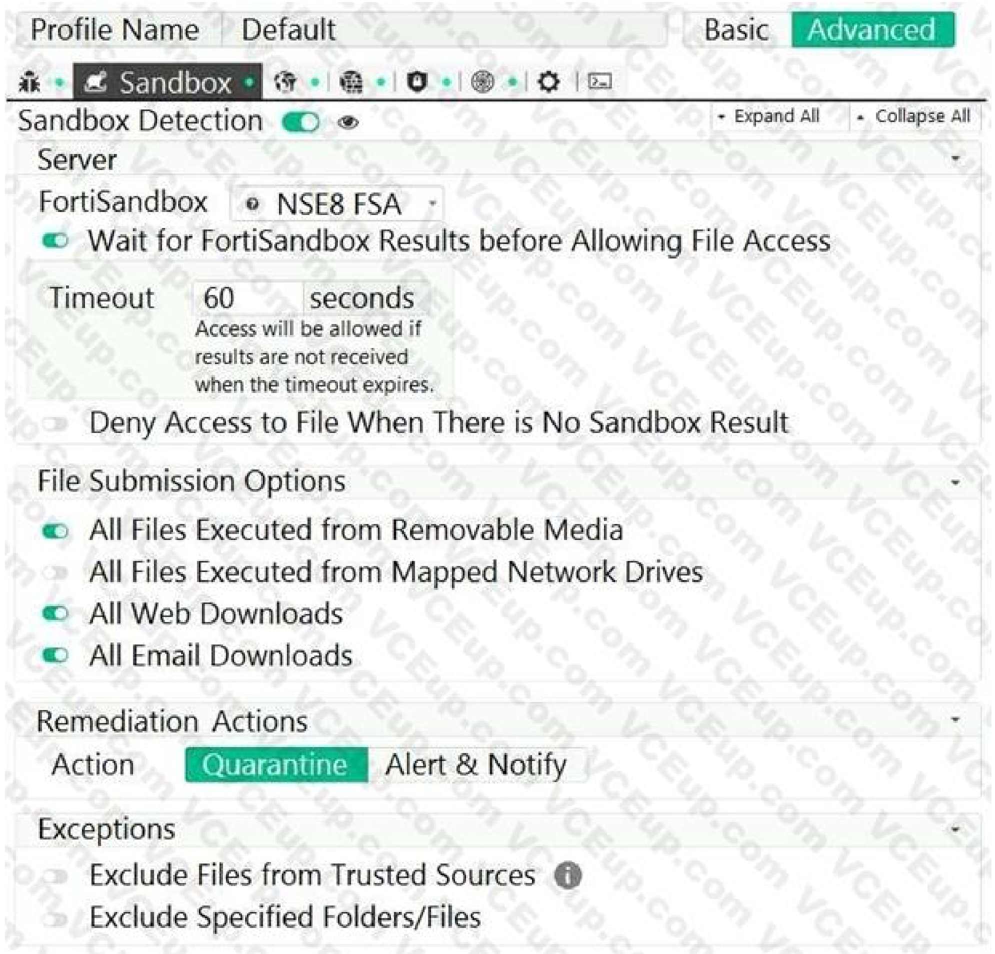
C. The phone A IP address will be translated lo the WAN IP address in all INVITE header fields and the m: field of the SDP statement.

D. The phone A IP address will be translated for the WAN IP address in all INVITE header fields and the SDP statement remains intact.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
“Also, the FortiGate must translate the addresses contained in the SIP headers and SDP body of the SIP messages The RTP port number as defined in the SIP message and an RTCP port number, which is the RTP port number plus 1”

QUESTION 61



Profile Name Default

Basic [✓ Advanced]

Sandbox

Sandbox Detection ●

Expand All · Collapse All

Server

FortiSandbox: NSE8 FSA

● Wait for FortiSandbox Results before Allowing File Access

Timeout: 60 seconds

Access will be allowed if results are not received when the timeout expires.

○ Deny Access to File When There is No Sandbox Result

File Submission Options

- ● All Files Executed from Removable Media
- ○ All Files Executed from Mapped Network Drives
- ● All Web Downloads
- ● All Email Downloads

Remediation Actions

Action: [✓ Quarantine] Alert & Notify

Exceptions

- ○ Exclude Files from Trusted Sources
- ○ Exclude Specified Folders/Files

Anti-Virus Real-Time Protection is enabled without any exclusions.

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

A. Access to a downloaded file will always be allowed after 60 seconds when the FortiSandbox is reachable.

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

C. Files executed from a mapped network drive will not be inspected by the FortiClient endpoint AntiVirus engine.

D. If the Real-Time Protection does not detect a virus, the user will be able to access a downloaded file when the FortiSandbox is unreachable.

Correct Answer: BD

Section: (none)

Explanation

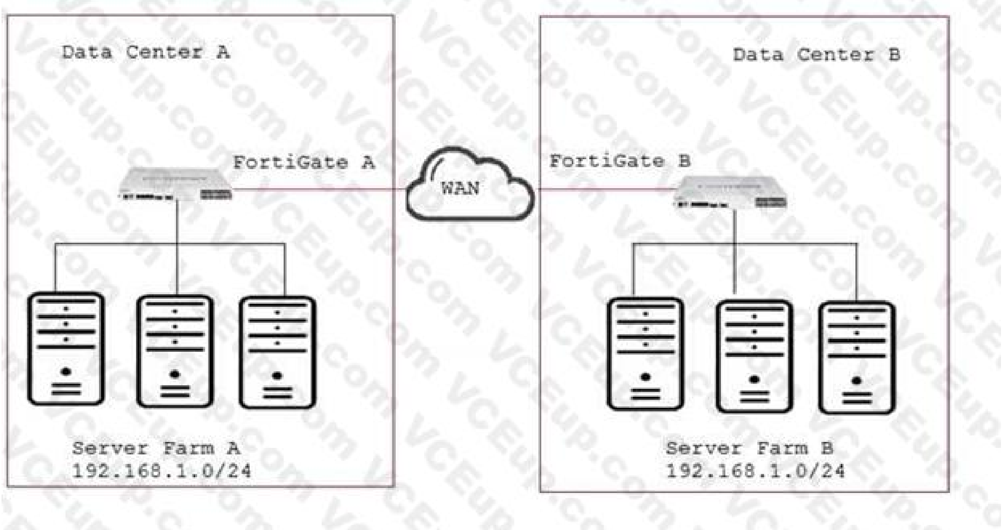
Explanation/Reference:

Explanation:

https://docs.fortinet.com/document/forticlient/6.0.0/ems-administration-guide/324667/sandboxdetection

QUESTION 62

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 Mode encapsulation.

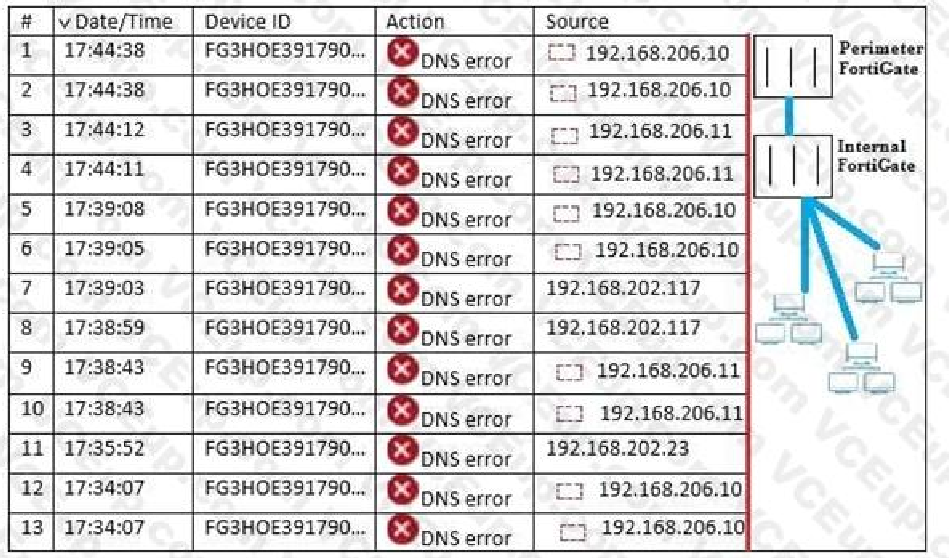
C. Create an IPsec tunnel with VXLAN encapsulation.

D. Create an IPsec tunnel with VLAN encapsulation.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://kb.fortinet.com/kb/documentLink.do?externalID=FD40170

QUESTION 63
Exhibit
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.



#	v 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 lo the perimeter FortiGates that does not inspect DNS traffic to the outbound firewall policy.

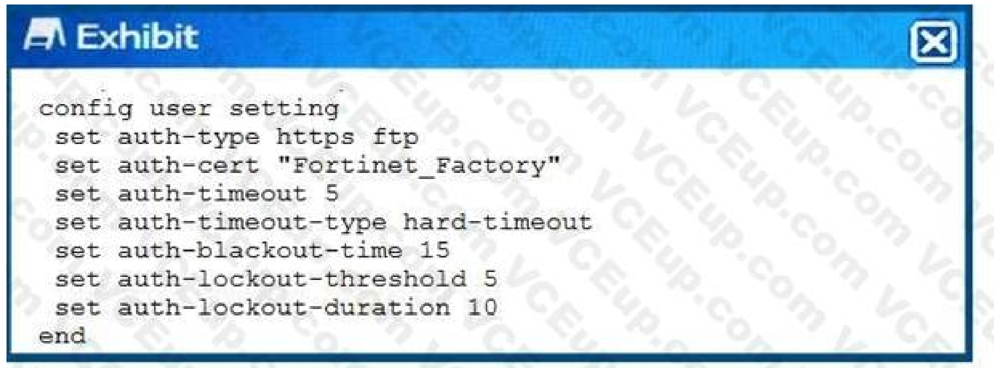
B. Configure the internal ForbGates to communicate to ForpGuard using port 8888.

C. Disable DNS events logging horn ForirGate In the config log fortianalyser filter section.
D. Remove DNS signature* <rom the IPS protte appfced to the outbound firewall policy.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://kb.fortinet.com/kb/documentLink.do?externalID=FD40788

QUESTION 64
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 FortiGate will allow the TCP connection when a ClientHello message indicating a renegotiation is received.
B. The user's IP address will be blocked 15 seconds after five login failures.
C. The user will be blocked 15 seconds after five login failures.
D. The user will need to re-authenticate after five minutes.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
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:
?onfig 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 FotiControllers was connected on the some network.
B. The priority should be set higher for ForControllers on slot-1.
C. The b1 interface the two FortiConrollers do not see each other.
D. The chassis ID settings on FotiControllers on slot 2 should be set to 2.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference: