Exam Questions NSE8_810

Fortinet Network Security Expert 8 Written Exam (810)

https://www.2passeasy.com/dumps/NSE8_810/

NEW QUESTION 1
Exhibit

Exhibit

```
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 man Internet Firewall policy using the antivirus profile labeled 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 configure was set to extreme.
B. The set options scan configuration items should have been changed to not option scan avmonitor.
C. The default AV profile was modified to use quick scan-mode.
D. The mobile-malware-db configuration was set to enabl

Answer: A

NEW QUESTION 2
Exhibit

Exhibit

```
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=20000ms 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
6d4ed9a17258cef68bed02a255115e6c
       ah=sha256 key=32
7eda44316eced542e4eb10b9961c0e0ff1a94ef3759998621d4721e2f1f8ca17
  enc: spi=a4867d12 esp=aes key=16
25161f51a29777bbf6232c9865d83afc
       ah=sha256 key=32
5d7b23e771575a947bd01d49c05efed79674a41a650e39f620713441d62f277
  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 offloade

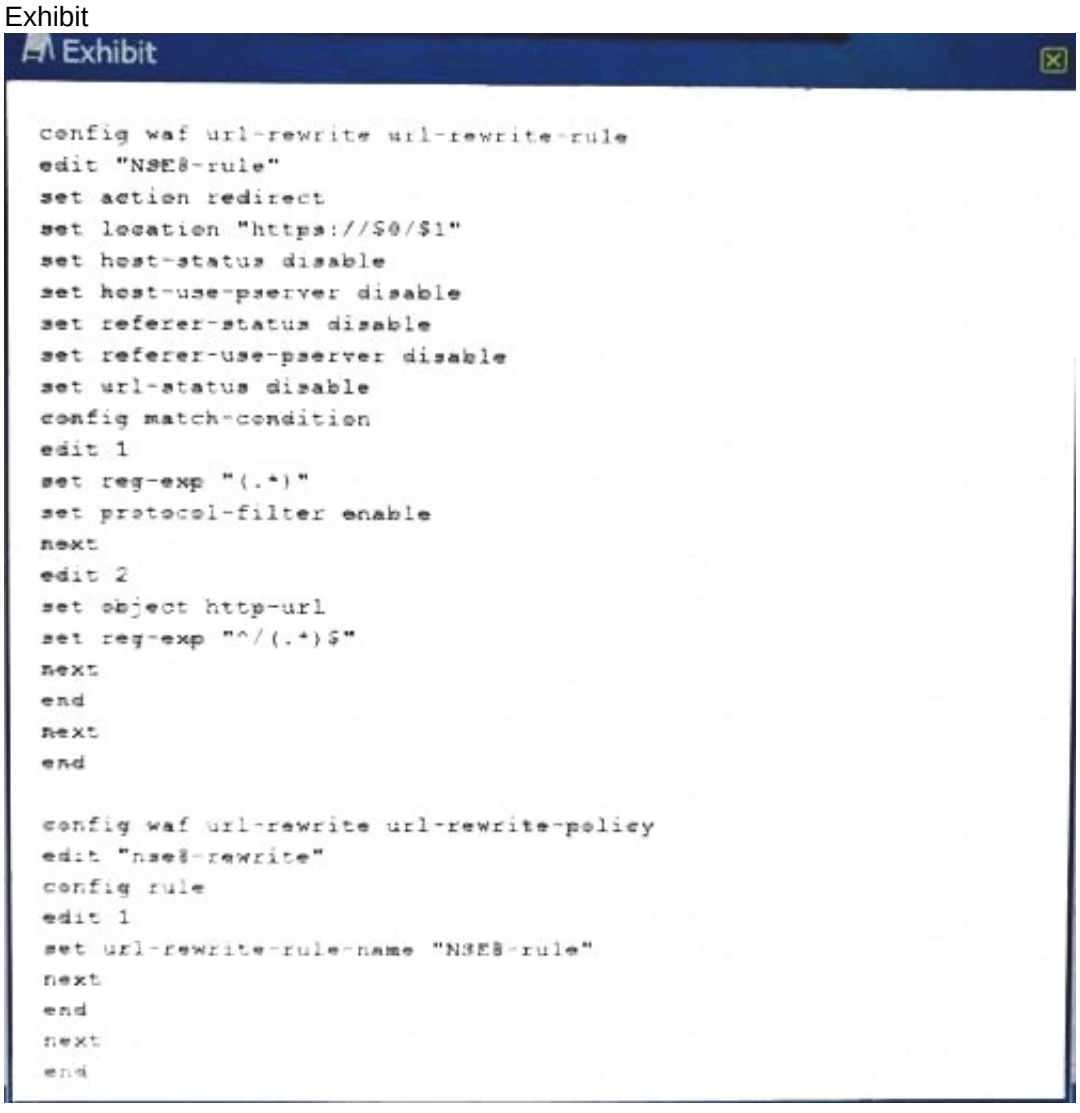
Answer: D

NEW QUESTION 3
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 ip arp list
B. diag aniffer packet wan1 'arp and host 10.10.1O.1'
C. diagnose hardware deviceinfo nice wan1
D. diagnose debug flow filter addt 10.10.10.1
E. diagnose debug flow trace trace 10

Answer: AD

NEW QUESTION 4
Exhibit



The exhibit shows the steps for creating a URL rewrite policy on a FortWet-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 HTTP

Answer: A

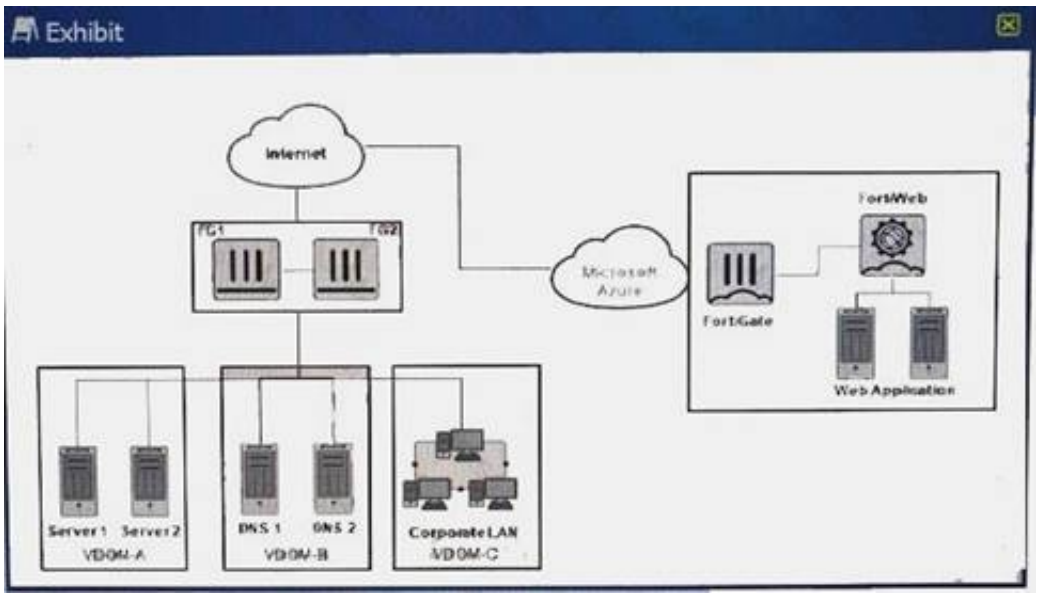
NEW QUESTION 5
Your customer is using dynamic routing to exchange the default route between two FortiGate using OSPFv2. The output of the get router info ospf neighbor command shows that the neighbor is up, but the default does not appears in the routing neighbor shows below.

According to the exhibit, what is causing the problem?

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 are

Answer: A

NEW QUESTION 6
Exhibit

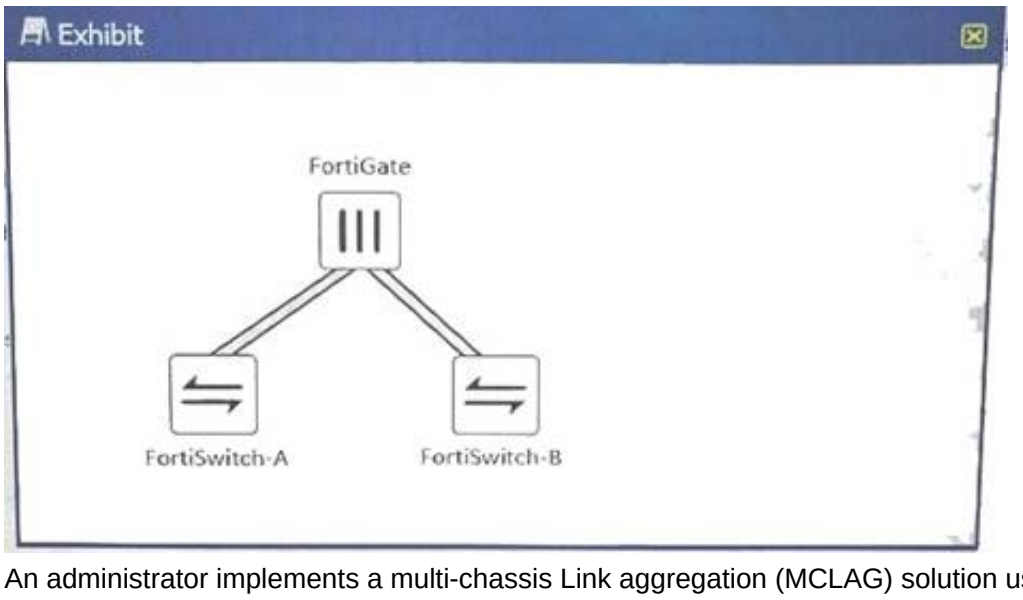


A customer gas just finished their Azure deployment to ensure a Web application behind a FortiWeb. Now they want to add components to protect against advance threats (zero day attacks), centrally the entire environment, and centrally monitor Fortinet and non-Fortinet products.
Which Fortinet will standby 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.

Answer: A

NEW QUESTION 7
Exhibit



An administrator implements a multi-chassis Link aggregation (MCLAG) solution using two FortiSwitch 448Ds and one FortiGate 3700D.
As described in the topology shown in the exhibit. two Inks are connected to each FortiSwitch. what is required to implement this solution? (Choose two)

A. a FortiGate with a hardware or a software switch
B. an ICL link between both FortiSwitches
C. a disabled FortiLink, split interface
D. two Link aggregated (LAG) interfaces on the FortiGate side

Answer: AD

NEW QUESTION 8
Central NAT was configured on a FortiGate firewall a Sniffer ICMP packets out to a host the internet egresses with the port IP address instead of the virtual IP (VP) that was configured.
Referring to the exhibit, which configuration change ensure that ICMP traffic is also translated?
A)

```
config firewall ippool
    edit "secondary_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
```

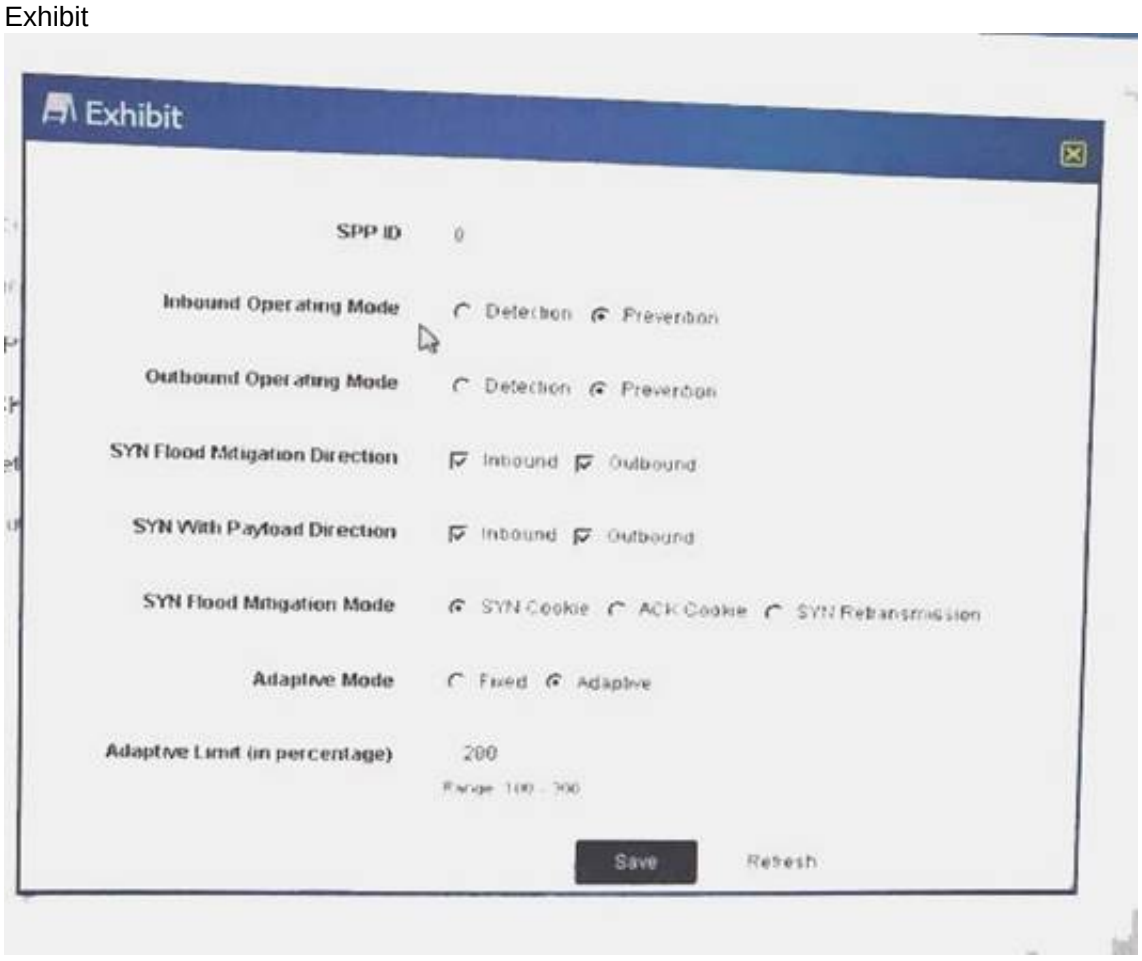
D)

```
config firewall central-snat-map
    edit 1
        set orig-addr "all"
    next
```

A. Option A
B. Option B
C. Option C
D. Option D

Answer: C

NEW QUESTION 9
Exhibit

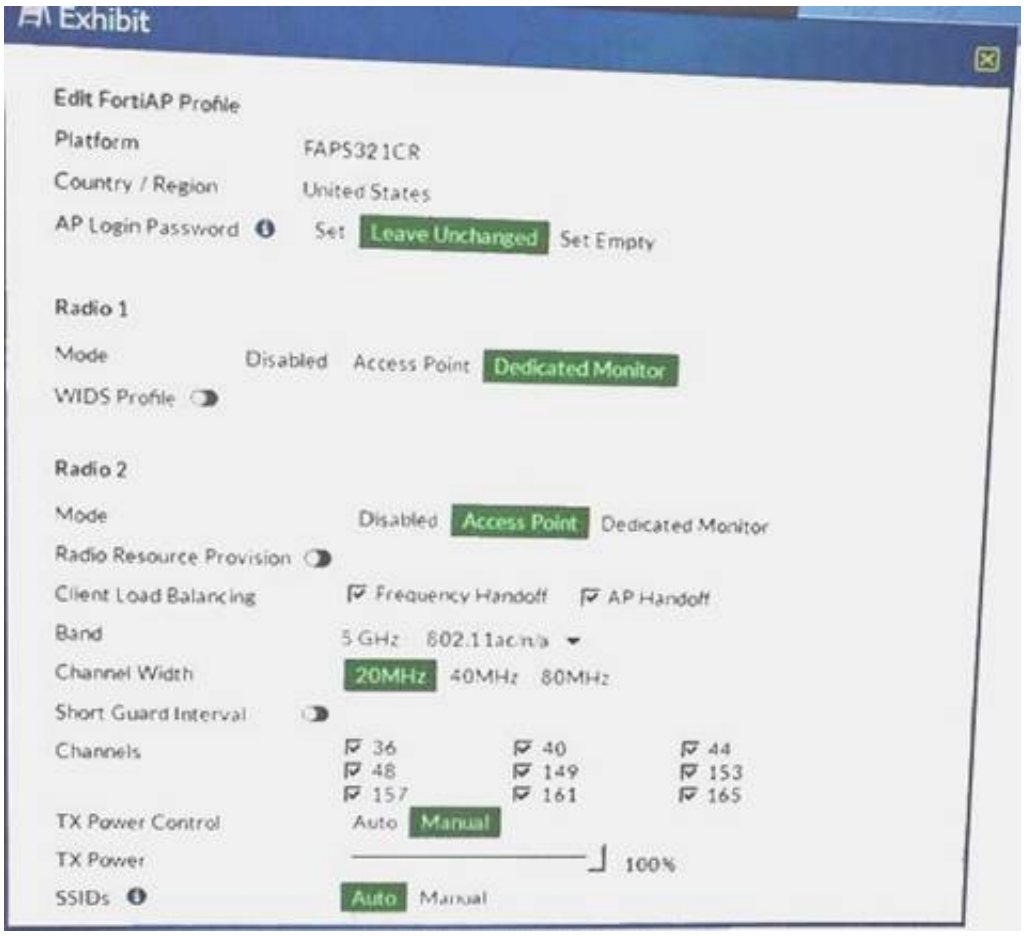


The exhibit shows the configuration of a service protection profile (SPP) in a FortiDDoS device. Which two statements are true about the traffic matching being inspection by this SPP? (Choose two.)

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 droope

Answer: AB

NEW QUESTION 10
Exhibit



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

A. All FortiAPs using thre profile will nave Radio 1 scan rogue access points.
B. Map this profile to SSIDs that you want to be available on the FortiAPs using this profile.
C. All FortiAPs using this profile will have Radio 1 monitor wireless clients.
D. Interference will be prevented between FortiAPs using this profile.

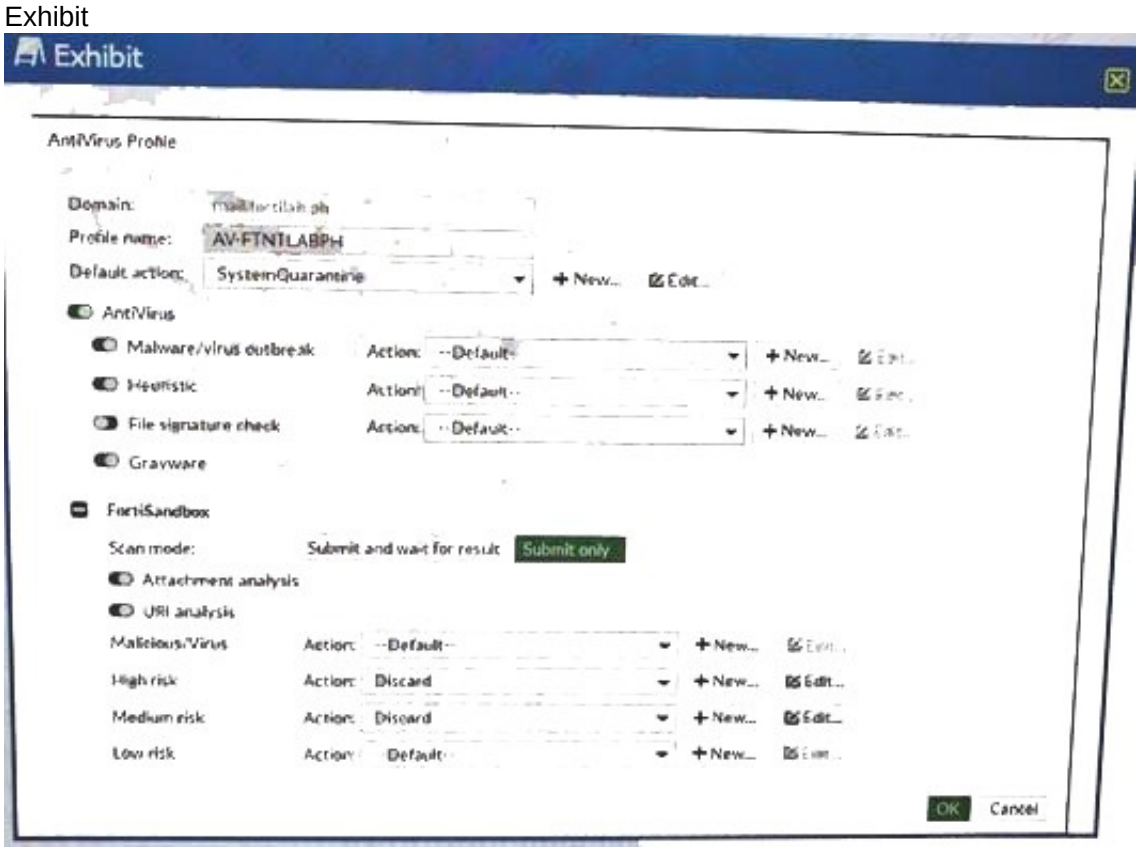
Answer: BC

NEW QUESTION 10
You ate asked lo 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

Answer: A

NEW QUESTION 14
Exhibit



Referring to the exhibit, what will happen if FortiSandbox categorizes an e-mail attachment submitted by FortiMarf as a high risk?

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 protectio

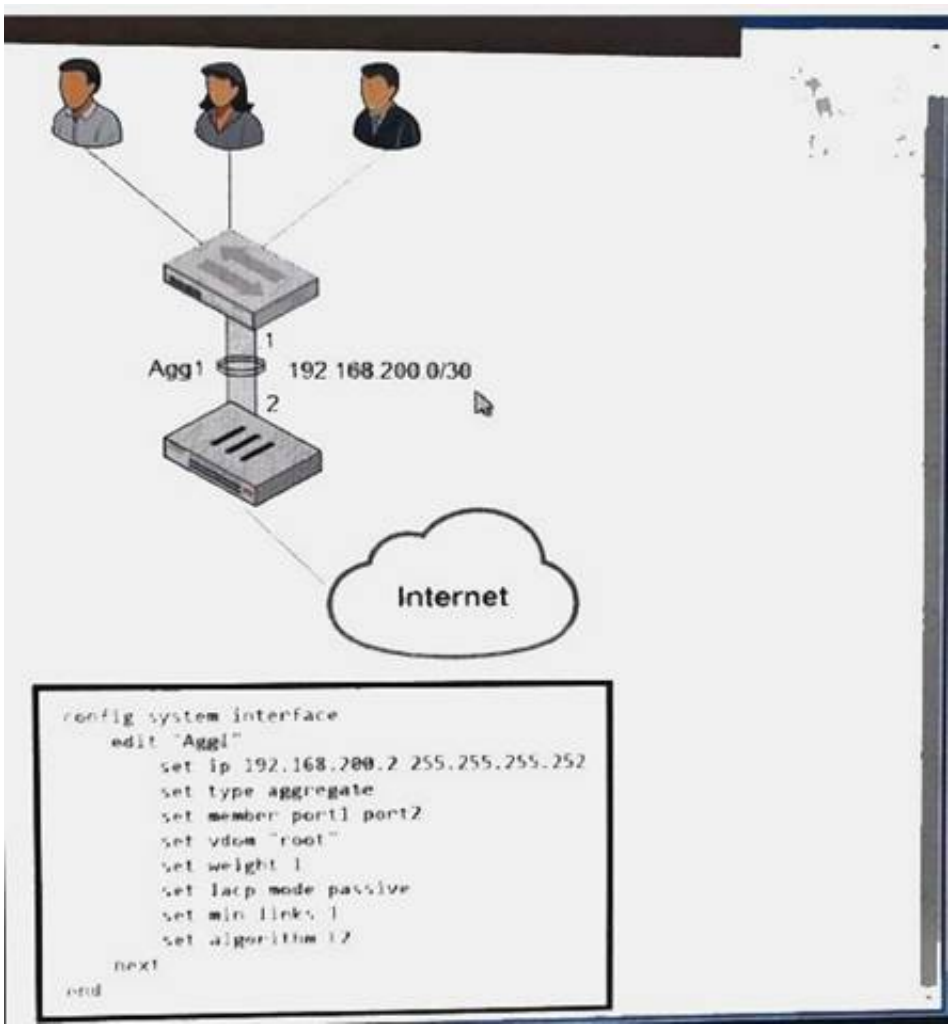
Answer: C

NEW QUESTION 18
You have deployed a FortiGate In NAT/Route mode as a secure as a web gateway with a few P-base authentication firewall policies. Your customer reports that some users now have different browsing permission =s from what is expected. All these users are browsing using internet Explorer through Desktop Connection to a Terminal Server. When you took at the Fortigate logs the username for the Terminal Server IP is not consistent.
Which action will correct this problem?

A. Make sure Terminal Service is using the correct DNS ever.
B. Configure FSSO Advanced with LDAP integration
C. Change the FSSO polling mode to windows NetAPI
D. Install the TSCitrix on the terminal server

Answer: C

NEW QUESTION 20
Exhibit



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

```
config system interface
 edit Aggl
  set min-links 2
end
```

B)

```
config system interface
 edit Aggl
  set weight 2
end
```

C)

```
config system interface
 edit Aggl
  set algorithm L4
end
```

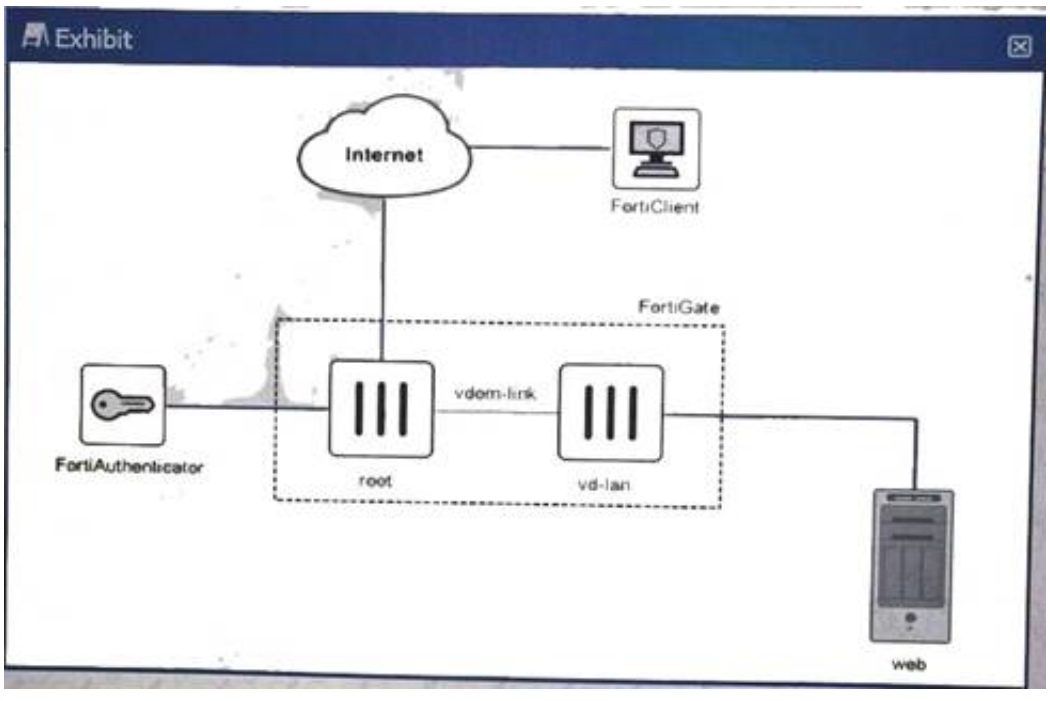
D)

```
config system interface
 edit Aggl
  set lacp mode active
end
```

A. Option A
B. Option B
C. Option C
D. Option D

Answer: A

NEW QUESTION 25
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 FortiAuthenticato

Answer: AC

NEW QUESTION 28
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

Answer: A

NEW QUESTION 31
You are asked implement a single FortiGate 5000 chassis using Session-aware Load Balance Cluster (SLBC) with Active-passive for Controllers have the configuration shown below, with the rest of the configuration set to the default values.

```
config system ha
    set mode dual
    set password fortinet123
    set group-id 5
    set chassis-id 1
    set minimize-chassis-failover enable
        set hbdev "b1"
end
```

Both FotiController 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.

Answer: A

NEW QUESTION 35
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual NSE8_810 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the NSE8_810 Product From:

https://www.2passeasy.com/dumps/NSE8_810/

Money Back Guarantee

NSE8_810 Practice Exam Features:

* NSE8_810 Questions and Answers Updated Frequently

* NSE8_810 Practice Questions Verified by Expert Senior Certified Staff

* NSE8_810 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* NSE8_810 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year