

NSE8_810^{Q&As}

Fortinet Network Security Expert 8 Written Exam (810)

Pass Fortinet NSE8_810 Exam with 100% Guarantee

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

https://www.pass2lead.com/nse8_810.html

100% Passing Guarantee
100% Money Back Assurance

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

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



QUESTION 1

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
```

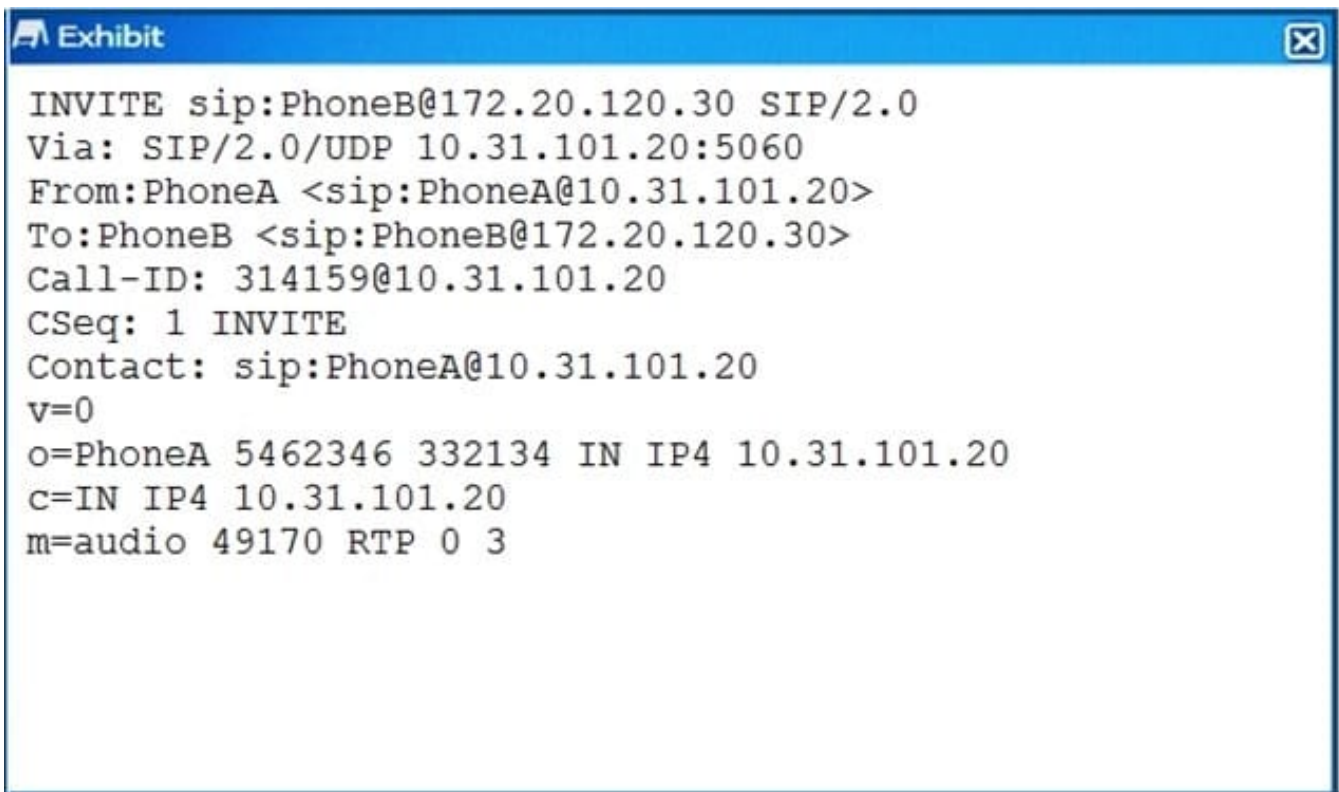
```
FGR # show firewall policy
config firewall policy
edit 1
set name "Internet"
set srcintf "port2"
set dstintf "port1"
set srcaddr "all"
set dstaddr "all"
set action accept
set schedule "always"
set service "ALL"
set utm-status enable
set logtraffic all
set fssso disable
set users "nse8user"
  set 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: AD

QUESTION 2



```
Exhibit
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.

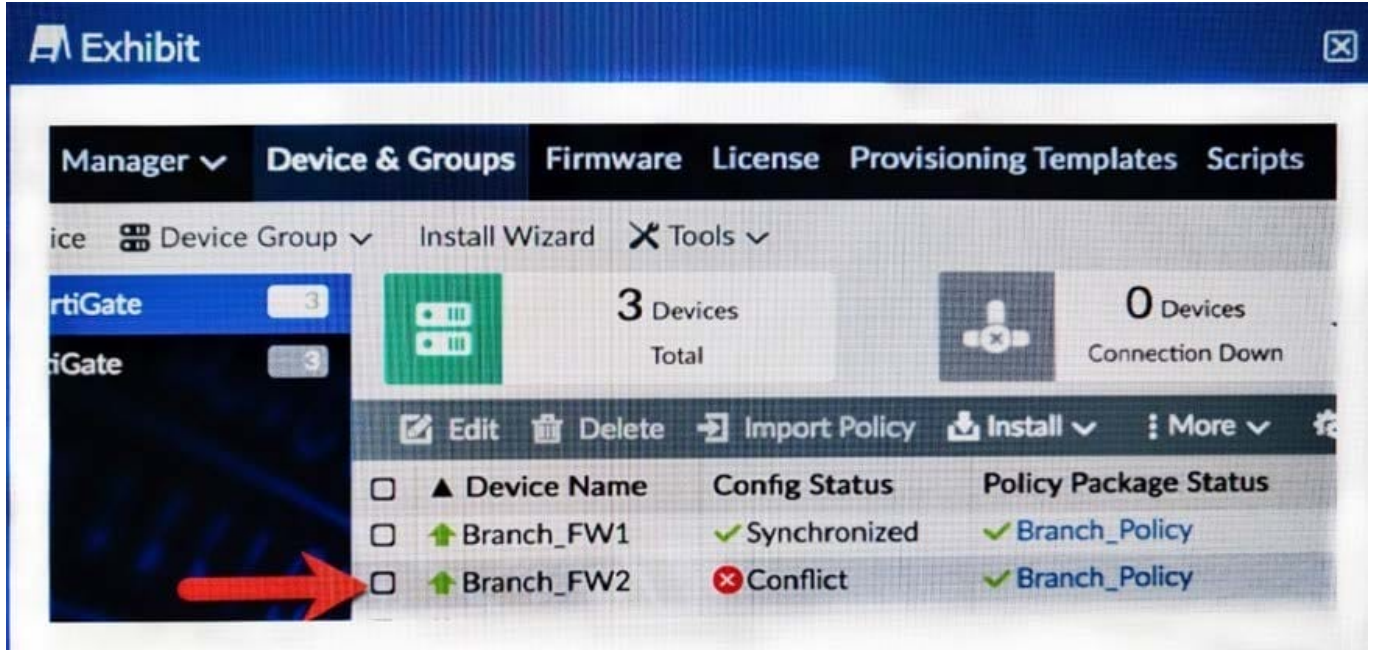
A FortiGate with the default configuration is deployed between two IP phones. FortiGate receives the INVITE request shown in the exhibit from Phone A (internal) to Phone B (external). Which two actions are taken by the FortiGate after the packet is received? (Choose two.)

- 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 49170 and 49171.
- C. The phone A IP address will be translated to 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: BD

QUESTION 3

Click the Exhibit button.



You log into FortiManager, look at the Device Manager window and notice that one of your managed devices is not in normal status.

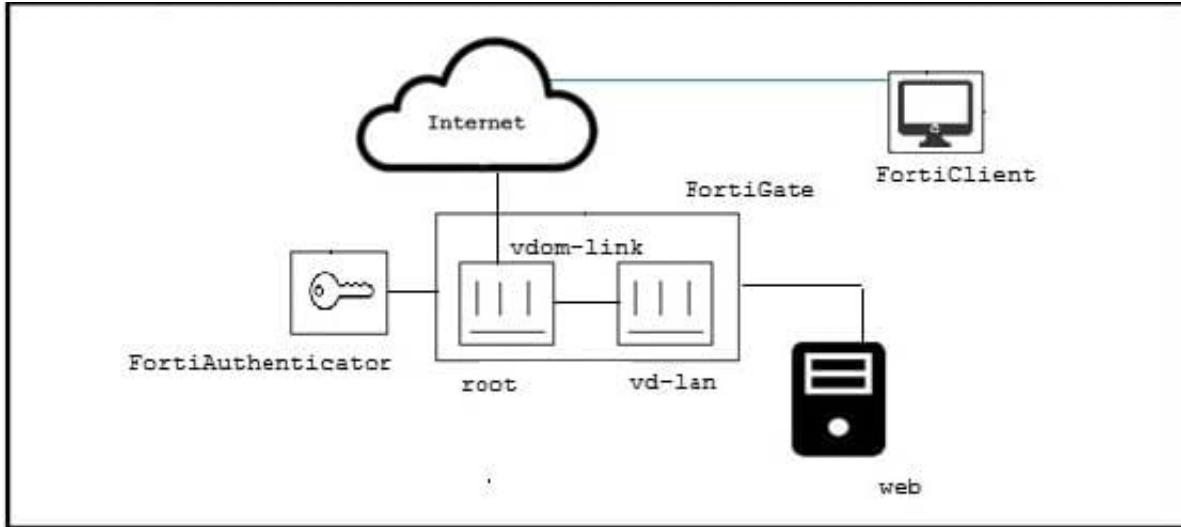
Referring to the exhibit, which two statements correctly describe the affected device's status and result? (Choose two.)

- 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 from 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

QUESTION 4

The exhibit shows a topology where a FortiGate is two VDOMS, root and vd-vlan. The root VDCM provides SSL-VPN access, where the users are authenticated by a FortiAuthenticator. The vd-lan VDOM provides 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

QUESTION 5

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
```

Click the Exhibit button.

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 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 enable.

Correct Answer: C

[NSE8_810 PDF Dumps](#)

[NSE8_810 VCE Dumps](#)

[NSE8_810 Study Guide](#)