

PassTest

Bessere Qualität , bessere Dienstleistungen!



Q&A

<http://www.passtest.de>

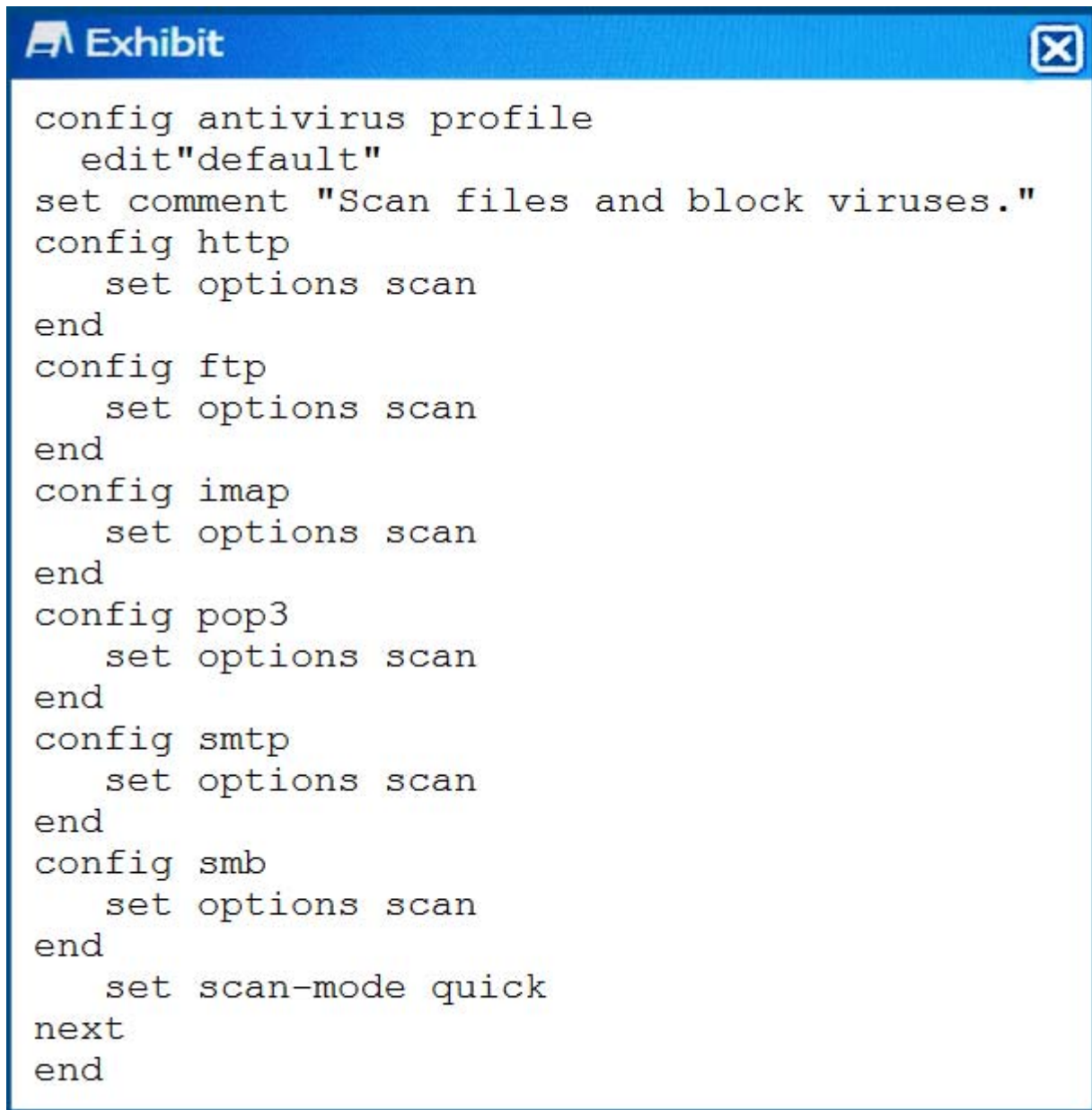
Einjährige kostenlose Aktualisierung

Exam : NSE8_810

**Title : Fortinet Network Security
Expert 8 Written Exam
(NSE8 810)**

Version : DEMO

1.Exhibit

A screenshot of a FortiGate configuration window titled "Exhibit" with a close button in the top right corner. The window contains a text area with the following configuration code:

```
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.

Answer: C

2.Click the Exhibit button.

 Exhibit

```
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
```

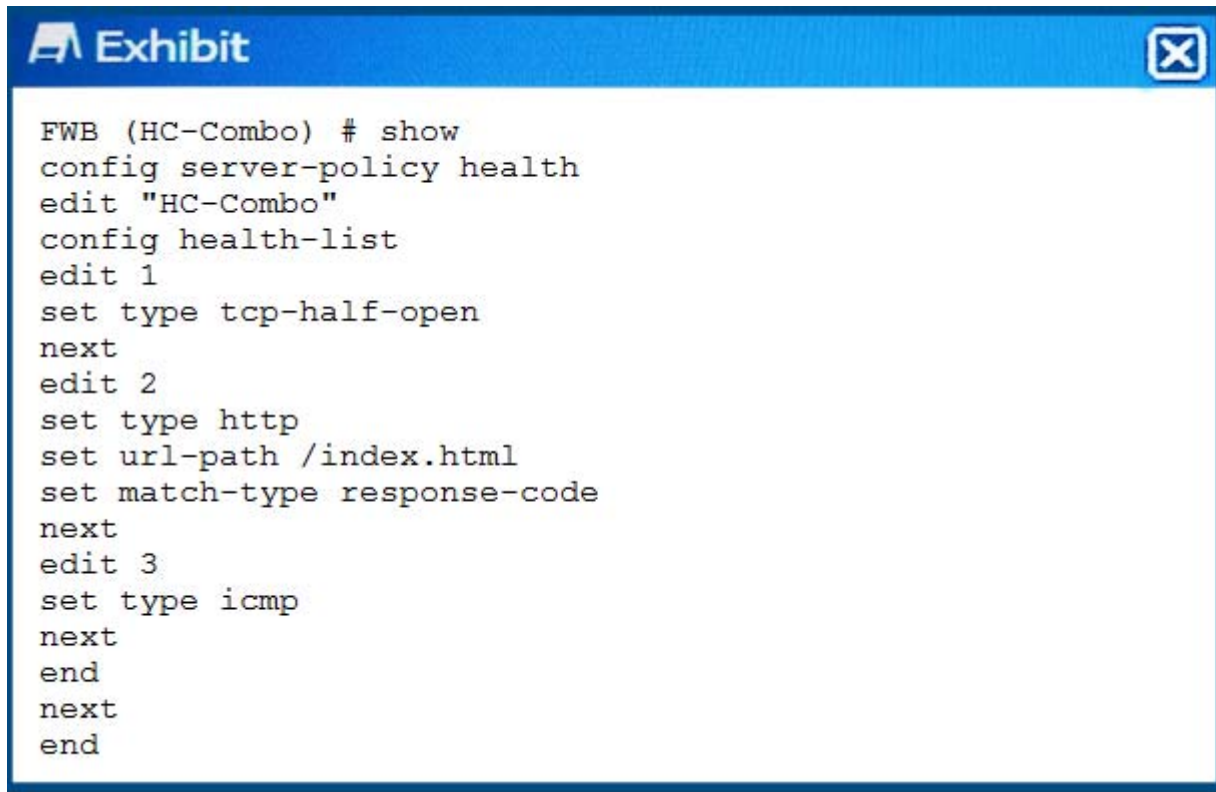
```
FortiGate-A # show switch-controller managed-switch
config switch-controller managed-switch
edit FS448D-A
config ports
edit "LAG-3"
set type trunk
set mode lacp-active
set mclag enable
set members "port15"
next
end
next
edit FS448D-B
config ports
edit "LAG-3"
set type trunk
set mode lacp-active
set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

Answer: BC

3.Exhibit

The exhibit is a screenshot of a FortiWeb configuration window titled "Exhibit" with a close button in the top right corner. The window contains a terminal-like interface showing the configuration of a health-check policy named "HC-Combo". The configuration steps are as follows: entering the configuration mode for "server-policy health", editing the policy "HC-Combo", entering the configuration mode for "health-list", editing list item "1", setting the type to "tcp-half-open", moving to the next item, editing list item "2", setting the type to "http", setting the URL path to "/index.html", setting the match type to "response-code", moving to the next item, editing list item "3", setting the type to "icmp", and finally exiting the list configuration and the policy configuration.

```
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.

Answer: B

4.A company has just deployed a new FortiMail in gateway mode. The administrator is asked to strengthen e-mail protection by applying the policies shown below.

- E-mails can only be accepted if a valid e-mail account exists.
- Only authenticated users can send e-mails out

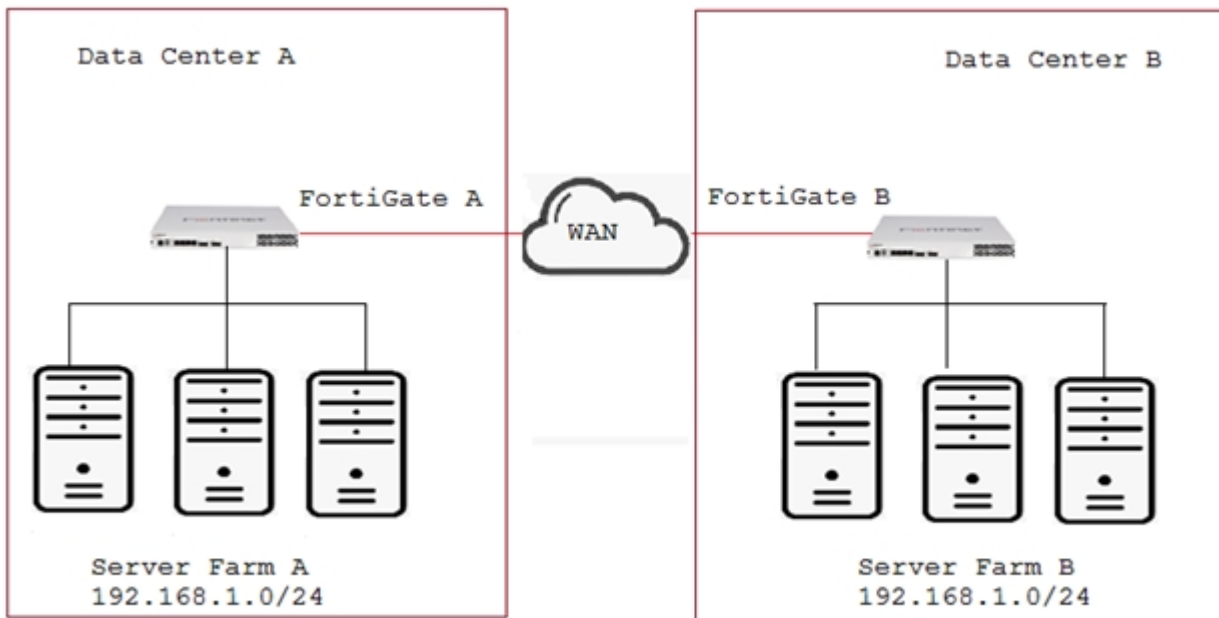
Which two actions will satisfy the requirements? (Choose two.)

- A. Configure recipient address verification.
- B. Configure inbound recipient policies.

- C. Configure outbound recipient policies.
- D. Configure access control rules.

Answer: AD

5. Click the Exhibit button.



Your company has two data centers (DC) connected using a Layer 3 network. Servers in farm A need to connect to servers in farm B as though they all were in the same Layer 2 segment.

What would be configured on the FortiGates on each DC to allow such connectivity?

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

Answer: C