

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.leads4pass.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

Exhibit

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

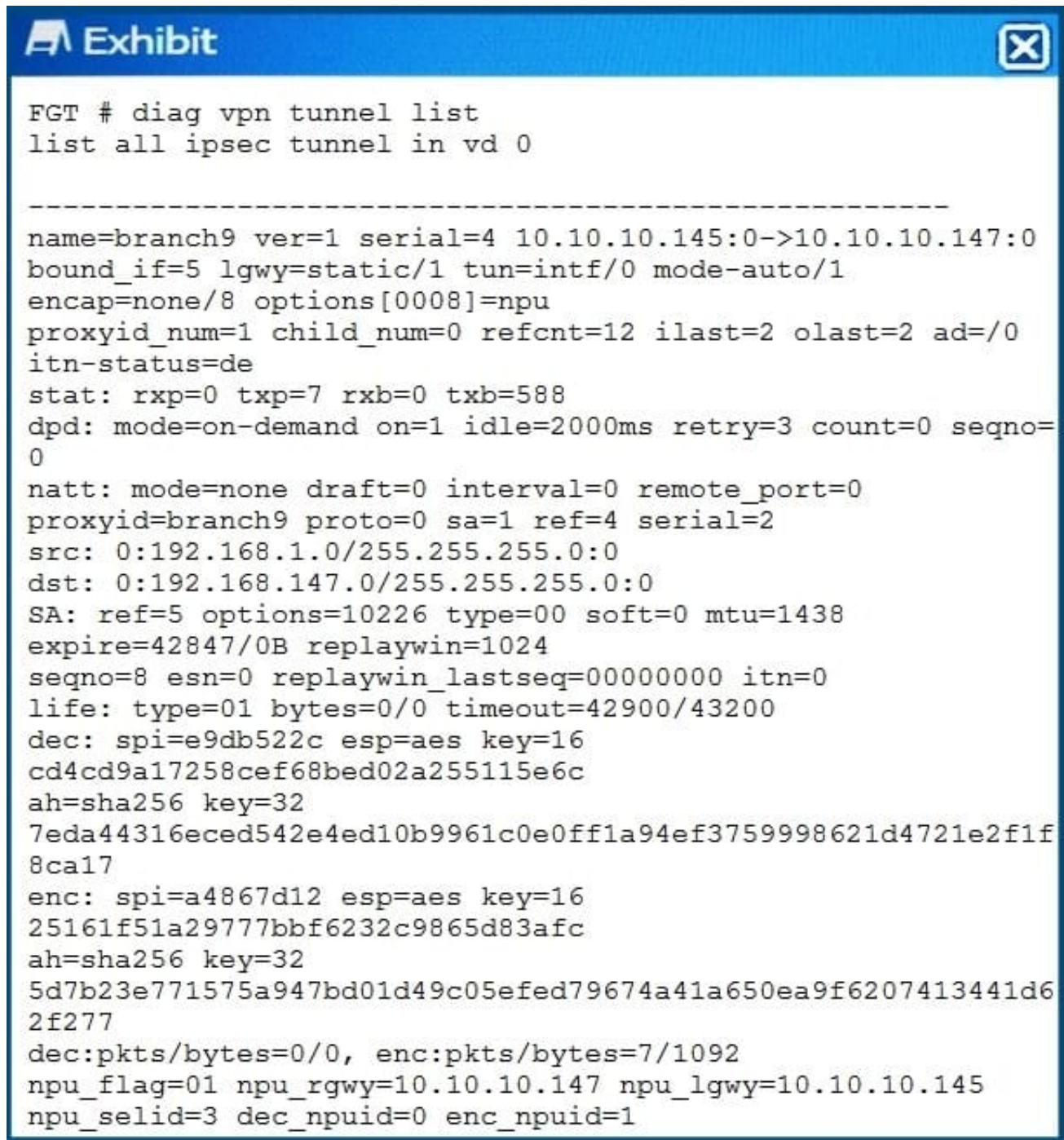
Profile Name	Default				
AntiVirus	Sanbox	Web Filter	Firewall	VPN	Vulnerability Scan
Sandbox Detection <input checked="" type="radio"/>					
Server					
IP Address/Hostname		<input type="text" value="172.16.1.12"/>			
<input checked="" type="radio"/> Wait for FortiSandbox Results before Allowing File Access					
<input checked="" type="radio"/> Deny Access to File If FortiSandbox Is Unreachable					
Timecut		<input type="text" value="60 seconds"/>			
Access will be allowed if results are not received when then timeout expires. Set to -1 to infinitely restrict access.					
Submission					
<input checked="" type="radio"/> All Files Executed from Removable Media					
<input type="radio"/> All Files Executed from Mapped Network Drives					
<input checked="" type="radio"/> All Web Downloads					
<input checked="" type="radio"/> All Email Downloads					

- A. Files executed from a mapped network drive will not be inspected by the FortiClient endpoint Antivirus engine.
- B. The user will not be able to access a Web downloaded file for at least 60 seconds when the FortiSandbox is reachable.
- C. The user will not be able to access a Web downloaded file for a maximum of 60 seconds if it is not a virus and the FortiSandbox is reachable.
- D. The user will not be able to access a Web downloaded file when the FortiSandbox is unreachable.

Correct Answer: AC

QUESTION 2

Click the Exhibit button.



```
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=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?

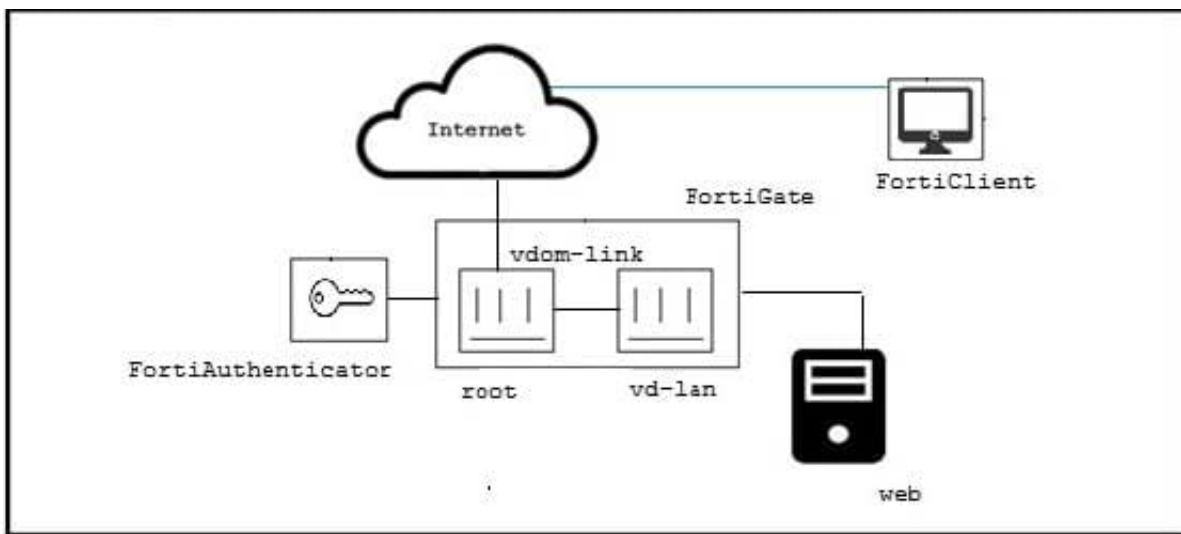
- A. Incoming and outgoing traffic is offloaded
- B. Outgoing traffic is offloaded, you cannot determine if incoming traffic is offloaded at this time.
- C. Traffic is not offloaded.

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

Correct Answer: D

QUESTION 3

Exhibit 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 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 4

Exhibit

The screenshot shows the 'Service Deployments' section in NSX Manager. At the top, there are navigation tabs: 'Installation', 'Management Host Preparation', 'Logical Network Preparation', and 'Service Deployments'. Below the tabs, the 'NSX Manager' IP is set to '10.10.50.3'. The main heading is 'Network & Security Service Deployments', with a sub-heading stating: 'Network & security service are deployed on a set of clusters. Manage service deployments here by adding new services or deleting existing ones.' There are '+', 'x', and 'Actions' icons, and a 'Filter' dropdown. A table lists the service deployment details:

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

At the bottom right of the table area, it says '1 items'.

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 vCenter was not able to locate the FortiGate-VMX's OVF file.
- B. The vCenter could not connect to the FortiGate Service Manager
- C. The NSX Manager was not able to connect on the FortiGate Service Manager's RestAPI service.
- D. The FortiGate Service Manager did not have the proper permission to register the FortiGate-VMX Service.

Correct Answer: D

QUESTION 5

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.)

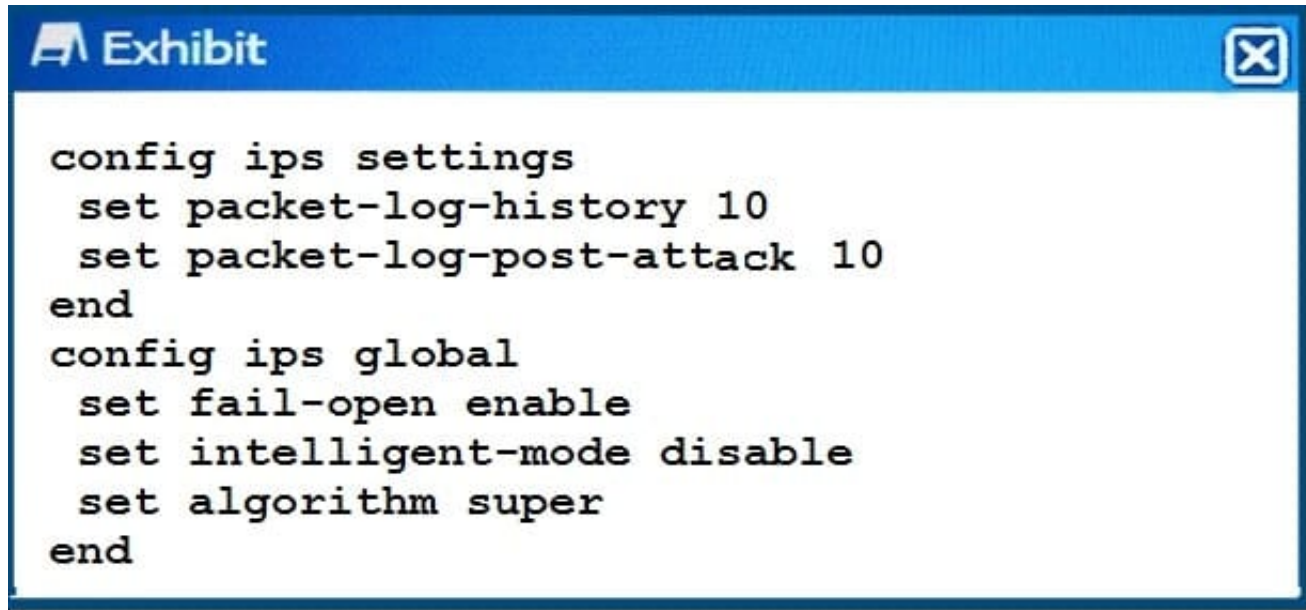
```
config vpn certificate setting
  set oosp-status enable
  set-oosp-default-server "FAC"
  set strict-oosp-check enable
end
config user peer
edit _any_
  set ca CA_Cert
  set ldap-server Training-Lab
  set ldap-mode principal-name
next
end
config user group
  edit "SSLVPN_Users"
  set member "_any_"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

QUESTION 6

Exhibit 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.)

An exhibit window with a blue header containing the word "Exhibit" and a close button. The window contains a text area with the following configuration commands:

```
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
```

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

Correct Answer: CD

QUESTION 7

You have a customer with a SCADA environmental control devices that is triggered a false- positive OPS alert whenever the device's Web GUI is accessed. You cannot seem to create a functional custom IPS filter expert this behavior, and it appears that the device is so old that it does HTTPS support. You need to prevent the false posited IPS alert occurring.

In this scenario, which two actions would accomplish this task? (Choose two.)

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

Correct Answer: AD

QUESTION 8

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:

Profile name:

Default action: + New Edit

AntiVirus

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

FortiSandbox

Scan mode:

- Attachment analysis
- URI analysis

Malicious/Virus	Action:	<input type="text" value="--Default--"/>	+ New	Edit
High risk	Action:	<input type="text" value="--Default--"/>	+ New	Edit
Medium risk	Action:	<input type="text" value="--Default--"/>	+ New	Edit
Low risk	Action:	<input type="text" value="--Default--"/>	+ New	Edit

- 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

QUESTION 9

Exhibit 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?


```
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
```

- 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 `^(.*)$` string to HTTP.
- D. The policy redirects only HTTP URLs containing the `^(.*)$` string to HTTPS.

Correct Answer: A

QUESTION 10

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.

Correct Answer: BC

[NSE8_810 PDF Dumps](#)

[NSE8_810 VCE Dumps](#)

[NSE8_810 Exam Questions](#)