

FCNSP.V5^{Q&As}

Fortinet Certified Network Security Professional (FCNSP.v5)

Pass Fortinet FCNSP.V5 Exam with 100% Guarantee

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

<https://www.leadspass.com/fcnsp-v5.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

Review the IPsec diagnostics output of the command `diag vpn tunnel list` shown in the Exhibit.

```
STUDENT # diagnose vpn tunnel list
list all ipsec tunnel in vd 0
-----
name=Remote_1 ver=1 serial=1 10.200.1.1:0->10.200.3.1:0 lgwy=static tun=intf mode=auto bound_if=2
proxyid_num=1 child_num=0 refcnt=6 ilast=2 olast=2
stat: rxp=8 txp=8 rxb=960 txb=480
dpd: mode=active on=1 idle=5000ms retry=3 count=0 seqno=128
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=P2_Remote_1 proto=0 sa=1 ref=2 auto_negotiate=0 serial=1
src: 0:0.0.0.0/0.0.0.0:0
dst: 0:0.0.0.0/0.0.0.0:0
SA: ref=3 options=0000000f type=00 soft=0 mtu=1412 expire=1486 replaywin=1024 seqno=1
life: type=01 bytes=0/0 timeout=1753/1800
dec: spi=b95a77fe esp=aes key=32 84ed410c1bb9f61e635a49563c4e7646e9e110628b79b0ac03482d05e3b6a0e6
ah=sha1 key=20 6bddbfad7161237daa46c19725dd0292b062dda5
enc: spi=9293e7d4 esp=aes key=32 951befd87860cdb59b98b170a17dcb75f77bd541bdc3a1847e54c78c0d43aa13
ah=sha1 key=20 8a5bedd6a0ce0f8daf7593601acfe2c618a0d4e2
-----
name=Remote_2 ver=1 serial=2 10.200.2.1:0->10.200.4.1:0 lgwy=static tun=intf mode=auto bound_if=3
proxyid_num=1 child_num=0 refcnt=6 ilast=0 olast=0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=active on=1 idle=5000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=P2_Remote_2 proto=0 sa=1 ref=2 auto_negotiate=0 serial=1
src: 0:0.0.0.0/0.0.0.0:0
dst: 0:0.0.0.0/0.0.0.0:0
SA: ref=3 options=0000000f type=00 soft=0 mtu=1280 expire=1732 replaywin=1024 seqno=1
life: type=01 bytes=0/0 timeout=1749/1800
dec: spi=b95a77ff esp=aes key=32 582af59d71635b835c9208878e0e3f3fe31baldfd88ff83ca9babied66ac325e
ah=sha1 key=20 0d951e62a1bcb63232df6d0fb86df49ab714f53b
enc: spi=9293e7d5 esp=aes key=32 eeeecacf3a58161f3390fa612b794c776654c86aef51fbc7542906223d56ebb3
ah=sha1 key=20 09eaa3085bc30a59091f182eb3d11550385b8304
```

Which of the following statements is correct regarding this output? (Select one answer).

- A. One tunnel is rekeying
- B. Two tunnels are rekeying
- C. Two tunnels are up
- D. One tunnel is up

Correct Answer: C

QUESTION 2

A static route is configured for a FortiGate unit from the CLI using the following commands:

```
config router static edit 1 set device "wan1" set distance 20 set gateway 192.168.100.1 next end
```

Which of the following conditions is NOT required for this static default route to be displayed in the FortiGate unit's routing table?

- A. The Administrative Status of the wan1 interface is displayed as Up.
- B. The Link Status of the wan1 interface is displayed as Up.
- C. All other default routes should have an equal or higher distance.
- D. You must disable DHCP client on that interface.

Correct Answer: D

QUESTION 3

Examine the following log message for IPS and identify the valid responses below. (Select all that apply.)

```
2012-07-01 09:54:28 oid=2 log_id=18433 type=ips subtype=anomaly pri=alert vd=root severity="critical"
src="192.168.3.168" dst="192.168.3.170" src_int="port2" serial=0 status="detected" proto=1 service="icmp" count=1
attack_name="icmp_flood" icmp_id="0xa8a4" icmp_type="0x08" icmp_code="0x00" attack_id=16777316 sensor="1"
ref="http://www.fortinet.com/ids/VID16777316" msg="anomaly: icmp_flood, 51 > threshold 50"
```

- A. The target is 192.168.3.168.
- B. The target is 192.168.3.170.
- C. The attack was detected and blocked.
- D. The attack was detected only.
- E. The attack was TCP based.

Correct Answer: BD

QUESTION 4

Which of the following is an advantage of using SNMP v3 instead of SNMP v1/v2 when querying the FortiGate unit?

- A. Packet encryption
- B. MIB-based report uploads
- C. SNMP access limits through access lists
- D. Running SNMP service on a non-standard port is possible

Correct Answer: A

QUESTION 5

Which of the following cannot be used in conjunction with the endpoint compliance check?

- A. HTTP Challenge Redirect to a Secure Channel (HTTPS) in the Authentication Settings.

B. Any form of firewall policy authentication.

C. WAN optimization.

D. Traffic shaping.

Correct Answer: A

[FCNSP.V5 Practice Test](#)

[FCNSP.V5 Exam Questions](#)

[FCNSP.V5 Braindumps](#)