



NSE4^{Q&As}

Fortinet Network Security Expert 4 Written Exam (400)

Pass Fortinet NSE4 Exam with 100% Guarantee

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

<https://www.geekcert.com/nse4.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

What is the maximum number of FortiAnalyzer/FortiManager devices a FortiGate unit can be configured to send logs to?

- A. 1
- B. 2
- C. 3
- D. 4

Correct Answer: C

QUESTION 2

What log type would indicate whether a VPN is going up or down?

- A. Event log
- B. Security log
- C. Forward log
- D. Syslog

Correct Answer: A

QUESTION 3

Which of the following statements are correct regarding SSL VPN Web-only mode? (Choose two.)

- A. It can only be used to connect to web services.
- B. IP traffic is encapsulated over HTTPS.
- C. Access to internal network resources is possible from the SSL VPN portal.
- D. The standalone FortiClient SSL VPN client CANNOT be used to establish a Web-only SSL VPN.
- E. It is not possible to connect to SSH servers through the VPN.

Correct Answer: BC

QUESTION 4

Which statements are true regarding IPv6 anycast addresses? (Choose two.)



- A. Multiple interfaces can share the same anycast address.
- B. They are allocated from the multicast address space.
- C. Different nodes cannot share the same anycast address.
- D. An anycast packet is routed to the nearest interface.

Correct Answer: AD

QUESTION 5

The exhibit shows a part output of the diagnostic command `\\diagnose debug application ike 255\\`, taken during establishment of a VPN. Which of the following statement are correct concerning this output? (choose two)

```
Ike 0:Remote:7:22: responder received first quick-mode message
ike 0:Remote:7:22: peer proposal is: peer:0:0.0.0.0-255.255.255.255:0, me:0:0.0.0.0-255.255.255.255:0
ike 0:Remote:7: sent IKE msg (quick_risend): 172.20.186.222:500->172.20.187.114:500, len=356
ike 0: comes 172.20.187.114:500->172.20.186.222:500,ifindex=2....
ike 0:Remote:7:P2:22: replay protection enabled
ike 0:Remote:7:P2:22: SA life soft seconds=1750.
ike 0:Remote:7:P2:22: SA life hard seconds=1800.
ike 0:Remote:7:P2:22: IPsec SA selectors #src=1 #dst=1
ike 0:Remote:7:P2:22: src 0 7 0:0.0.0.0-255.255.255.255:0
ike 0:Remote:7:P2:22: dst 0 7 0:0.0.0.0-255.255.255.255:0
ike 0:Remote:7:P2:22: add IPsec SA: SPIs=6e13ca19/8f1ce9ae
ike 0:Remote:7:P2:22: added IPsec SA: SPIs=6e13ca19/8f1ce9ae
ike 0:Remote:7:P2:22: sending SNMP tunnel UP trap
```

- A. The quick mode selectors negotiated between both IPsec VPN peers is 0.0.0.0/32 for both source and destination addresses.
- B. The output corresponds to a phase 2 negotiation
- C. NAT-T enabled and there is third device in the path performing NAT of the traffic between both IPsec VPN peers.
- D. The IP address of the remote IPsec VPN peer is 172.20.187.114

Correct Answer: BD

[Latest NSE4 Dumps](#)

[NSE4 VCE Dumps](#)

[NSE4 Brindumps](#)