NSE8_811^{Q&As}

Fortinet NSE 8 Written Exam (NSE8_811)

Pass Fortinet NSE8_811 Exam with 100% Guarantee

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

https://www.pass2lead.com/nse8_811.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

Refer to the exhibit.

```
ike 0:Dial-Up_0:30:Dial-Up:5: IPsec SA selectors #src=1 #dst=1
ike 0:Dial-Up_0:30:Dial-Up:5: src 0 7 0:0.0.0.0-255.255.255.255:0
ike 0:Dial-Up_0:30:Dial-Up:5: dst 0 7 0:10.10.10.0-10.10.10.255:0
ike 0:Dial-Up_0:30:Dial-Up:5: add dynamic IPsec SA selectors
ike 0:Dial-Up_1:2: moving route 10.10.10.0/255.255.255.0 oif Dial-Up_1(23) metric 15 priority 0 to 0:DialUp_0:5
ike 0:Dial-Up_1:2: del route 10.10.10.0/255.255.255.0 oif Dial-Up_1(23) metric 15 priority 0
ike 0:Dial-Up_1: deleting
ike 0:Dial-Up_1: flushing
ike 0:Dial-Up_1: deleting IPsec SA with SPI fa6915c1
ike 0:Dial-Up_1:Dial-Up: deleted IPsec SA with SPI fa6915c1, SA count: 0
ike 0:Dial-Up_1: sending SNMP tunnel DOWN trap for Dial-Up
ike 0:Dial-Up_1:Dial-Up: delete
```

A FortiGate is configured for a dial-up IPsec VPN to allow multiple remote FortiGate devices to connect to it. However, FortiGate A and B have problems connecting to the VPN. Only one of them can be connected at a time. If site B tries to connect while site A is connected, site A is disconnected. The IKE real-time debug shows the output in the exhibit when site A is disconnected.

Referring to the exhibit, which configuration setting should be executed in the dial-up configuration to allow both VPNs to be connected at the same time?

A. set route-overlap allow

B. set single-source disable

C. set enforce-unique-id disable

D. set add-route enable

Correct Answer: A

QUESTION 2

A legacy router has been replaced by a FortiGate device. The FortiGate has inherited the management IP address of the router and now the network administrator needs to remove the router from the FortiSIEM configuration.

Which two statements about this operation are true? (Choose two.)

A. FortiSIEM will move the router device into the Decommission folder.

B. The router will be completely deleted from the FortiSIEM database.

C. By default, FortiSIEM can only parser event logs for FortiGate devices.

D. FortiSIEM will discover a new device for the FortiGate with the same IP.

Correct Answer: AD

QUESTION 3

![Pass2Lead](https://Pass2Lead.com)
A customer wants to use a central RADIUS server for management authentication when connecting to the FortiGate GUI and to provide different levels of access for different types of employees.

Which three actions are required to provide the requested functionality? (Choose three.)

A. Create a wildcard administrator on the FortiGate.

B. Enable radius-vdom-override in the CLI.

C. Create multiple administrator profiles with matching RADIUS VSAs.

D. Enable accprofile-override in the CLI.

E. Set the RADIUS authentication type to MS-CHAPv2.

Correct Answer: ACD

QUESTION 4

Refer to the 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=20000ms 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 7eda44316eced542e4eb10b9961c0e0ff1a94ef3759998621d4721e2f1f8ca17
    enc: spi=a4867d12 esp=aes key=16 25161f51a29777bbf6232c9865d83afc
        ah=sha256 key=32 5d7b23e771575a947bd01d49c05efed79674a41a650ea9f6207413441d62f277
    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. Outgoing traffic is offloaded; you cannot determine if incoming traffic is offloaded at this time.

B. Outgoing traffic is offloaded; incoming traffic not offloaded.

C. Incoming and outgoing traffic is offloaded.

D. Traffic is not offloaded.

![Pass2Lead logo](https://Pass2Lead.com)
Correct Answer: B

QUESTION 5

Refer to the exhibit.

SPP ID	0
Inbound Operating Mode	○ Detection ● Prevention
Outbound Operating Mode	○ Detection ● Prevention
SYN Flood Mitigation Direction	☑ Inbound ☑ Outbound
SYN With Payload Direction	☑ Inbound ☑ Outbound
SYN Flood Mitigation Mode	● SYN Cookie ○ ACK Cookie ○ SYN Retransmission
Adaptive Mode	○ Fixed ● Adaptive
Adaptive Limit (in percentage)	200 Range: 100 - 300

Save   Refresh

The exhibit shows the configuration of a service protection profile (SPP) in a FortiDDoS device. Which two statements are true about the traffic matching being inspected by this SPP? (Choose two.)

A. Traffic that does not match any SPP policy will be inspected by this SPP.

B. FortiDDoS will not send a SYN/ACK if a SYN packet is coming from an IP address that is not in the legitimate IP (LIP) address table.

C. FortiDDoS will start dropping packets as soon as the traffic exceeds the configured minimum threshold.

D. SYN packets with payloads will be dropped.

Correct Answer: AD

[Latest NSE8_811 Dumps](https://www.pass2lead.com)   [NSE8_811 VCE Dumps](https://www.pass2lead.com)   [NSE8_811 Exam Questions](https://www.pass2lead.com)