NSE4-5.4 Q&As

Fortinet Network Security Expert 4 Written Exam - FortiOS 5.4

Pass Fortinet NSE4-5.4 Exam with 100% Guarantee

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

https://www.pass2lead.com/nse4-5-4.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 are the advantages of FSSO DC mode over polling mode?

A. Redundancy in the collector agent.

B. Allows transparent authentication.

C. DC agents are not required in the AD domain controllers.

D. Scalability

Correct Answer: C

QUESTION 2

Examine the routing database.

```
S     *> 0.0.0.0/0 [10/0] via 172.20.121.2, port1, [20/0]
      *>           [10/0] via 10.0.0.2, port2, [30/0]
S        0.0.0.0/0 [20/0] via 192.168.15.2, port3, [10/0]
C     *> 10.0.0.0/24 is directly connected, port2
S        172.13.24.0/24 [10/0] is directly connected, port4
C     *> 172.20.121.0/24 is directly connected, port1
S     *> 192.167.1.0/24 [10/0] via 10.0.0.2, port2
C     *> 192.168.15.0/24 is directly connected, port3
```

Which of the following statements are correct? (Choose two.)

A. The port3 default route has the lowest metric, making it the best route.

B. There will be eight routes active in the routing table.

C. The port3 default has a higher distance than the port1 and port2 default routes.

D. Both port1 and port2 default routers are active in the routing table.

Correct Answer: CD

QUESTION 3

Which statement about the FortiGuard services for the FortiGate is true?

A. Antivirus signatures are downloaded locally on the FortiGate.

B. FortiGate downloads IPS updates using UDP port 53 or 8888.

C. FortiAnalyzer can be configured as a local FDN to provide antivirus and IPS updates.

D. The web filtering database is downloaded locally on the FortiGate.

Correct Answer: A

QUESTION 4

Which of the following components are contained in all FortiGate units from the FG50 models and up? (Select all that apply.)

A. FortiASIC content processor.

B. Hard Drive.

C. Gigabit network interfaces.

D. Serial console port.

Correct Answer: AD

QUESTION 5

How do you configure inline SSL inspection on a firewall policy? (Choose two.)

A. Enable one or more flow-based security profiles on the firewall policy.

B. Enable the SSL/SSH Inspection profile on the firewall policy.

C. Execute the inline ssl inspection CLI command.

D. Enable one or more proxy-based security profiles on the firewall policy.

Correct Answer: AB

QUESTION 6

Which of the following statements is correct regarding URL Filtering on the FortiGate unit?

A. The FortiGate unit can filter URLs based on patterns using text and regular expressions.

B. The available actions for URL Filtering are Allow and Block.

C. Multiple URL Filter lists can be added to a single Web filter profile.

D. A FortiGuard Web Filtering Override match will override a block action in the URL filter list.

Correct Answer: A

QUESTION 7

When browsing to an internal web server using a web-mode SSL VPN bookmark, which IP address is used as the source of the HTTP request?

A. The FortiGate unit\\'s public IP address

B. The FortiGate unit\\'s internal IP address

C. The remote user\\'s virtual IP address

D. The remote user\\'s public IP address

Correct Answer: B

QUESTION 8

Which of the following combinations of two FortiGate device configurations (side A and side B), can be used to successfully establish an IPsec VPN between them? (choose two)

A. Side A:main mode, remote gateway as static IP address, policy based VPN. Side B: aggressive mode, remote Gateway as static IP address policy-based VPN.

B. Side A:main mode, remote gateway as static IP address, policy based VPN. Side B: main mode, remote gateway as static IP address, route-based VPN

C. Side A:main mode, remote gateway as static IP address, policy based VPN. Side B: main mode, remote gateway as dialup, route-based VPN.

D. Side A: main mode, remote gateway as dialup policy based VPN, Side B: main mode, remote gateway as dialup, policy based VPN.

Correct Answer: BC

QUESTION 9

Which of the following authentication methods are supported in an IPsec phase 1? (Choose two.)

A. Asymmetric Keys

B. CA root digital certificates

C. RSA signature

D. Pre-shared keys

Correct Answer: CD

QUESTION 10

How is the FortiGate password recovery process?

A. Interrupt boot sequence, modify the boot registry and reboot. After changing the password, reset the boot registry.

B. Log in through the console port using the "maintainer" account within several seconds of physically power cycling the FortiGate.

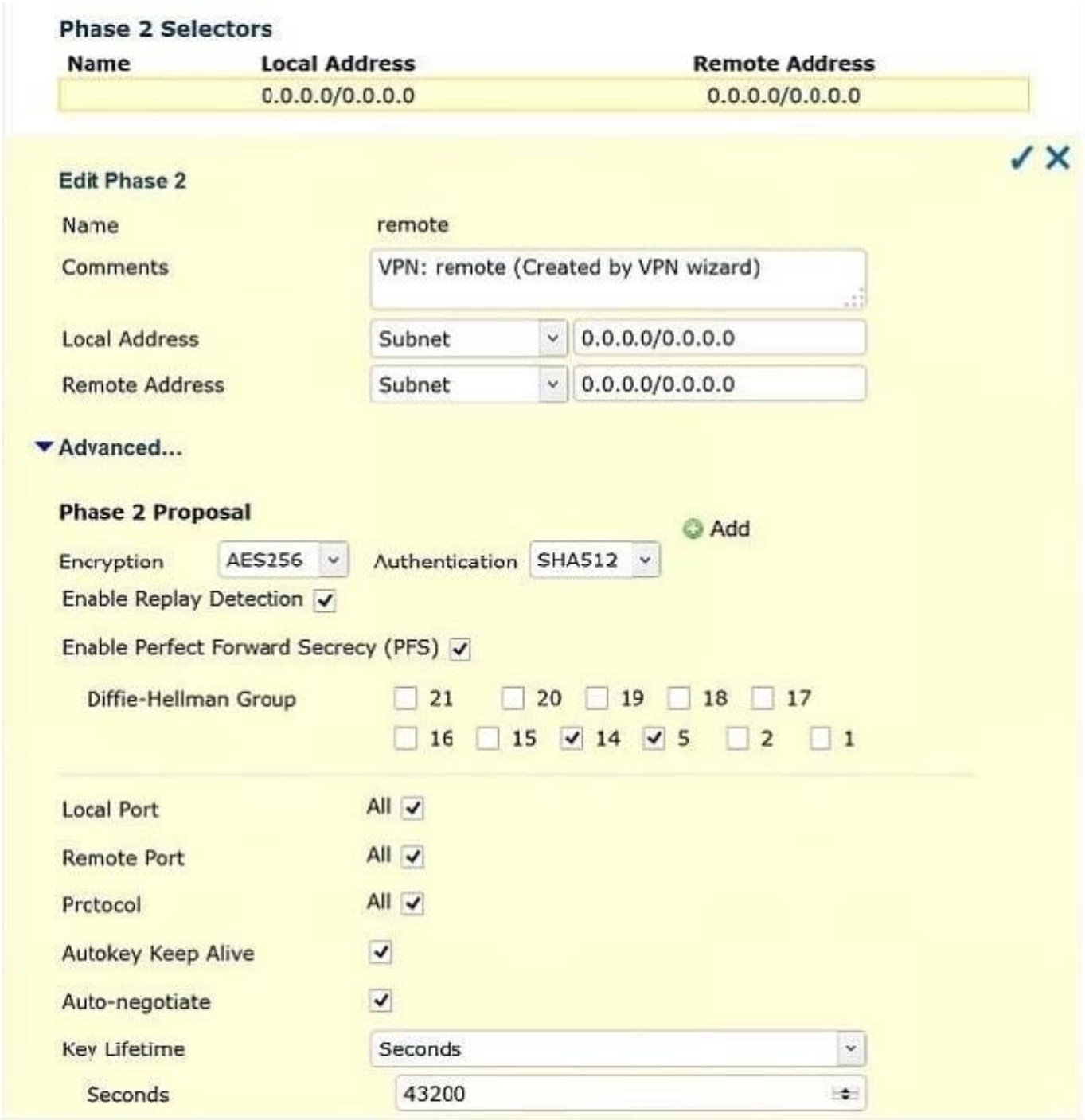
C. Hold down the CTRL + Esc (Escape) keys during reboot, then reset the admin password.

D. Interrupt the boot sequence and restore a configuration file for which the password has been modified.

Correct Answer: B

QUESTION 11

Review the IPsec phase 2 configuration shown in the exhibit; then answer the question below.



Which statements are correct regarding this configuration? (Choose two.).

A. The Phase 2 will re-key even if there is no traffic.

B. There will be a DH exchange for each re-key.

C. The sequence number of ESP packets received from the peer will not be checked.

D. Quick mode selectors will default to those used in the firewall policy.

Correct Answer: AB

QUESTION 12

Review the IPsec diagnostics output of the command diagnose 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 582af59d71635b835c9208878e0e3f3fe31ba1dfd88ff83ca9bab1ed66ac325e
       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 13

An administrator observes that the port1 interface cannot be configured with an IP address. What can be the reasons for that? (Choose three.)

A. The interface has been configured for one-arm sniffer.

B. The interface is a member of a virtual wire pair.

C. The operation mode is transparent.

D. The interface is a member of a zone.

E. Captive portal is enabled in the interface.

Correct Answer: ABC

QUESTION 14

Which statement is an advantage of using a hub and spoke IPsec VPN configuration instead of a fully-meshed set of IPsec tunnels?

A. Using a hub and spoke topology provides full redundancy.

B. Using a hub and spoke topology requires fewer tunnels.

C. Using a hub and spoke topology uses stronger encryption protocols.

D. Using a hub and spoke topology requires more routes.

Correct Answer: B

QUESTION 15

A client can create a secure connection to a FortiGate device using SSL VPN in web-only mode. Which one of the following statements is correct regarding the use of web-only mode SSL VPN?

A. Web-only mode supports SSL version 3 only.

B. A Fortinet-supplied plug-in is required on the web client to use web-only mode SSL VPN.

C. Web-only mode requires the user to have a web browser that supports 64-bit cipher length.

D. The JAVA run-time environment must be installed on the client to be able to connect to a web- only mode SSL VPN.

Correct Answer: C