http://www.ipass4sure.com

NSE4

Fortinet

Fortinet Network Security Expert 4 Written Exam (400)

The NSE4 practice exam is written and formatted by Certified Senior IT Professionals working in today's prospering companies and data centers all over the world! The NSE4 Practice Test covers all the exam topics and objectives and will prepare you for success quickly and efficiently. The NSE4 exam is very challenging, but with our NSE4 questions and answers practice exam, you can feel confident in obtaining your success on the NSE4 exam on your FIRST TRY!

Fortinet NSE4 Exam Features

- **Detailed questions and answers for NSE4 exam**
- **Try a demo before buying any Fortinet exam**
- **NSE4 questions and answers, updated regularly**
- **Verified NSE4 answers by Experts and bear almost 100% accuracy**
- **NSE4 tested and verified before publishing**
- **NSE4 exam questions with exhibits**
- **NSE4 same questions as real exam with multiple choice options**

Acquiring Fortinet certifications are becoming a huge task in the field of I.T. More over these exams like NSE4 exam are now continuously updating and accepting this challenge is itself a task. This NSE4 test is an important part of Fortinet certifications. We have the resources to prepare you for this. The NSE4 exam is essential and core part of Fortinet certifications and once you clear the exam you will be able to solve the real life problems yourself.Want to take advantage of the Real NSE4 Test and save time and money while developing your skills to pass your Fortinet NSE4 Exam? Let us help you climb that ladder of success and pass your NSE4 now!

QUESTION: 1
Review the output of the command get router info routing-table all shown in the Exhibit below; then answer the question following it.

```
STUDENT # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

S*      0.0.0.0/0 [10/0] via 10.200.1.254, port1
                 [10/0] via 10.200.2.254, port2, [5/0]
C       10.0.1.0/24 is directly connected, port3
O       10.0.2.0/24 [110/101] via 172.16.2.1, Remote_1, 00:00:21
                    [110/101] via 172.16.2.2, Remote_2, 00:00:21
C       10.200.1.0/24 is directly connected, port1
C       10.200.2.0/24 is directly connected, port2
C       172.16.1.1/32 is directly connected, Remote_1
C       172.16.1.2/32 is directly connected, Remote_2
C       172.16.2.1/32 is directly connected, Remote_1
C       172.16.2.2/32 is directly connected, Remote_2
```

Which one of the following statements correctly describes this output?

A. The two routes to the 10.0.2.0/24 subnet are ECMP routes and traffic will be load balanced based on the configured ECMP settings.
B. The route to the 10.0.2.0/24 subnet via interface Remote_1 is the active and the route via Remote_2 is the backup.
C. OSPF does not support ECMP therefore only the first route to subnet 10.0.1.0/24 is used.
D. 172.16.2.1 is the preferred gateway for subnet 10.0.2.0/24.

Answer: A

QUESTION: 2
Identify the correct properties of a partial mesh VPN deployment:

A. VPN tunnels interconnect between every single location.
B. VPN tunnels are not configured between every single location.
C. Some locations are reached via a hub location.
D. There are no hub locations in a partial mesh.

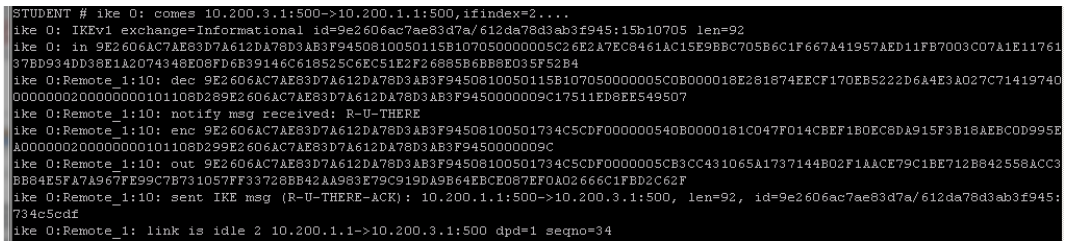
Answer: B, C

QUESTION: 3
Data Leak Prevention archiving gives the ability to store files and message data onto a FortiAnalyzer unit for which of the following types of network traffic? (Select all that apply.)

A. SNMP
B. IPSec
C. SMTP
D. POP3
E. HTTP

Answer: C, D, E

QUESTION: 4
Review the IKE debug output for IPsec shown in the Exhibit below.



Which one of the following statements is correct regarding this output?

A. The output is a Phase 1 negotiation.
B. The output is a Phase 2 negotiation.
C. The output captures the Dead Peer Detection messages.
D. The output captures the Dead Gateway Detection packets.

Answer: C

QUESTION: 5
Two FortiGate devices fail to form an HA cluster, the device hostnames are STUDENT and REMOTE. Exhibit A shows the command output of 'show system ha' for the STUDENT device. Exhibit B shows the command output of 'show system ha' for the REMOTE device.

Exhibit A:

```
Max number of virtual domains: 10
Virtual domains status: 1 in NAT mode, 0 in TP mode
Virtual domain configuration: disable
FIPS-CC mode: disable
Current HA mode: a-p, master
Branch point: 128
Release Version Information: GA
System time: Thu Jan 24 08:34:19 2013

STUDENT #
STUDENT #
STUDENT #
STUDENT #
STUDENT #
STUDENT # show system ha
config system ha
    set mode a-p
    set password ENC 9FHCYwOJXK9z8w6QkUnUsREWBruVcMJ5NUVE3oV5otyn+4dsgx4CnV1GRJ8
McEECpiT3Z/3dCmIuYIDgW2sE+lAlkHfADOV/r5DkaqGnbj15XV/a
    set hbdev "port2" 50
    set override disable
    set priority 200
end

STUDENT # _
```

Exhibit B

```
global: ses_limit=0 ses6_limit=0 rt_limit=0 rt6_limit=0

REMOTE # diagnose sys session stat
misc info:       session_count=11 setup_rate=0 exp_count=0 clash=4
        memory_tension_drop=0 ephemeral=0/57344 removeable=0  ha_scan=0
delete=0, flush=0, dev_down=0/0
TCP sessions:
         2 in ESTABLISHED state
         1 in SYN_SENT state
firewall error stat:
error1=00000000
error2=00000000
error3=00000000
error4=00000000
tt=00000000
cont=00000000
ids_recv=00000000
url_recv=00000000
av_recv=00000000
fqdn_count=00000000
tcp reset stat:
        syncqf=0 acceptqf=0 no-listener=7 data=0 ses=0 ips=0
global: ses_limit=0 ses6_limit=0 rt_limit=0 rt6_limit=0

REMOTE # _
```

Which one of the following is the most likely reason that the cluster fails to form?

A. Password
B. HA mode
C. Hearbeat
D. Override

Answer: B

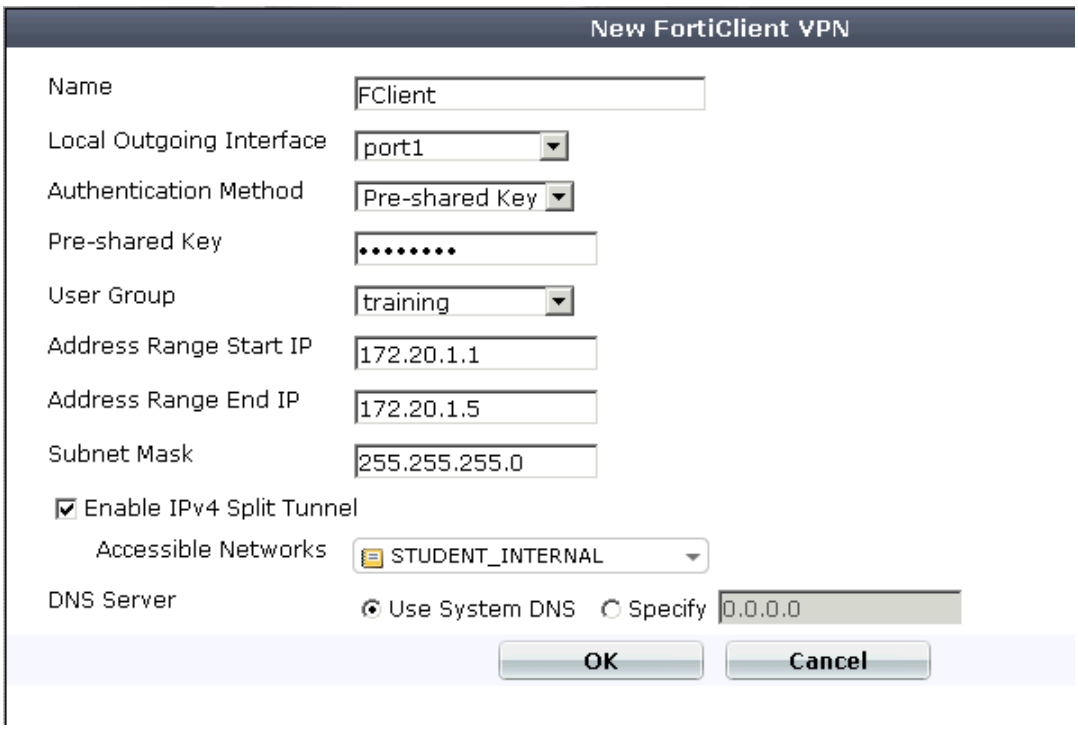
QUESTION: 6
Examine the Exhibit shown below; then answer the question following it.

The Vancouver FortiGate unit initially had the following information in its routing table: S 172.20.0.0/16 [10/0] via 172.21.1.2, port2
C 172.21.0.0/16 is directly connected, port2 C 172.11.11.0/24 is directly connected, port1
Afterwards, the following static route was added:
config router static edit 6
set dst 172.20.1.0 255.255.255.0
set pririoty 0
set device port1
set gateway 172.11.12.1 next
end
Since this change, the new static route is NOT showing up in the routing table. Given the information provided, which of the following describes the cause of this problem?

A. The subnet 172.20.1.0/24 is overlapped with the subnet of one static route that is already in the routing table (172.20.0.0/16), so, we need to enable allow-subnet-overlap first.
B. The 'gateway' IP address is NOT in the same subnet as the IP address of port1.
C. The priority is 0, which means that the route will remain inactive.
D. The static route configuration is missing the distance setting.

Answer: B

QUESTION: 7
Review the configuration for FortiClient IPsec shown in the Exhibit below.



Which of the following statements is correct regarding this configuration?

A. The connecting VPN client will install a route to a destination corresponding to the STUDENT_INTERNAL address object
B. The connecting VPN client will install a default route
C. The connecting VPN client will install a route to the 172.20.1.[1-5] address range
D. The connecting VPN client will connect in web portal mode and no route will be installed

Answer: A

QUESTION: 8
What advantages are there in using a hub-and-spoke IPSec VPN configuration instead of a fully-meshed set of IPSec tunnels? (Select all that apply.)

A. Using a hub and spoke topology is required to achieve full redundancy.
B. Using a hub and spoke topology simplifies configuration because fewer tunnels are required.
C. Using a hub and spoke topology provides stronger encryption.
D. The routing at a spoke is simpler, compared to a meshed node.

Answer: B, D

QUESTION: 9
In the case of TCP traffic, which of the following correctly describes the routing table lookups

performed by a FortiGate unit when searching for a suitable gateway?

A. A look-up is done only when the first packet coming from the client (SYN) arrives.
B. A look-up is done when the first packet coming from the client (SYN) arrives, and a second is performed when the first packet coming from the server (SYNC/ACK) arrives.
C. A look-up is done only during the TCP 3-way handshake (SYNC, SYNC/ACK, ACK).
D. A look-up is always done each time a packet arrives, from either the server or the client side.

Answer: B

QUESTION: 10
Which of the following represents the correct order of criteria used for the selection of a Master unit within a FortiGate High Availability (HA) cluster when master override is disabled?

A. 1. port monitor, 2. unit priority, 3. up time, 4. serial number
B. 1. port monitor, 2. up time, 3. unit priority, 4. serial number
C. 1. unit priority, 2. up time, 3. port monitor, 4. serial number
D. 1. up time, 2. unit priority, 3. port monitor, 4. serial number

Answer: B

QUESTION: 11
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 8a5bedd6a0ce0f8daf759360lacfe2c618a0d4e2
------------------------------------------------------
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

Answer: C

QUESTION: 12
Review the output of the command config router ospf shown in the Exhibit below; then answer the question following it.

```
STUDENT (ospf) # show
config router ospf
        config area
            edit 0.0.0.0
            next
        end
        config network
            edit 1
                set prefix 10.0.1.0 255.255.255.0
            next
            edit 2
                set prefix 172.16.0.0 255.240.0.0
            next
        end
        config ospf-interface
            edit "R1_OSPF"
                set interface "Remote_1"
                set ip 172.16.1.1
                set mtu 1436
                set network-type point-to-point
            next
            edit "R2_OSPF"
                set cost 20
                set interface "Remote_2"
                set ip 172.16.1.2
                set mtu 1436
                set network-type point-to-point
            next
        end
        config redistribute "connected"
        end
        config redistribute "static"
        end
        config redistribute "rip"
        end
        config redistribute "bgp"
        end
        config redistribute "isis"
        end
    set router-id 0.0.0.1
end
```

Which one of the following statements is correct regarding this output?

A. OSPF Hello packets will only be sent on interfaces configured with the IP addresses 172.16.1.1 and 172.16.1.2.
B. OSPF Hello packets will be sent on all interfaces of the FortiGate device.
C. OSPF Hello packets will be sent on all interfaces configured with an address matching the 10.0.1.0/24 and 172.16.0.0/12 networks.
D. OSPF Hello packets are not sent on point-to-point networks.

Answer: C

**** END OF DEMO ****

Pass4sure Certification Exam Features;

- Pass4sure offers over **4500** Certification exams for professionals.
- More than **98,800** Satisfied Customers Worldwide.
- Average **99.8%** Success Rate.
- Over **150** Global Certification Vendors Covered.
- Services of Professional & Certified Experts available via support.
- Free 90 days updates to match real exam scenarios.
- Instant Download Access! No Setup required.
- Price as low as $19, which is 80% more cost effective than others.
- Verified answers researched by industry experts.
- Study Material **updated** on regular basis.
- Questions / Answers are downloadable in **PDF** format.
- Mobile Device Supported (Android, iPhone, iPod, iPad)
- **No authorization** code required to open exam.
- **Portable** anywhere.
- ***Guaranteed Success***.
- **Fast**, helpful support 24x7.

View list of All certification exams offered;
http://www.ipass4sure.com/allexams.asp

View list of All Study Guides (SG);
http://www.ipass4sure.com/study-guides.asp

View list of All Audio Exams (AE);
http://www.ipass4sure.com/audio-exams.asp

Download Any Certication Exam DEMO.
http://www.ipass4sure.com/samples.asp

To purchase Full version of exam click below;
http://www.ipass4sure.com/allexams.asp

3COM	CompTIA	Filemaker	IBM	LPI	OMG	Sun
ADOBE	ComputerAssociates	Fortinet	IISFA	McAfee	Oracle	Sybase
APC	CWNP	Foundry	Intel	McData	PMI	Symantec
Apple	DELL	Fujitsu	ISACA	Microsoft	Polycom	TeraData
BEA	ECCouncil	GuidanceSoftware	ISC2	Mile2	RedHat	TIA
BICSI	EMC	HDI	ISEB	NetworkAppliance	Sair	Tibco
CheckPoint	Enterasys	Hitachi	ISM	Network-General	SASInstitute	TruSecure
Cisco	ExamExpress	HP	Juniper	Nokia	SCP	Veritas
Citrix	Exin	Huawei	Legato	Nortel	See-Beyond	Vmware
CIW	ExtremeNetworks	Hyperion	Lotus	Novell	Google	

and many others.. See complete list Here