NSE7^{Q&As}

Fortinet Troubleshooting Professional

Pass Fortinet NSE7 Exam with 100% Guarantee

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

https://www.leads4pass.com/nse7.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

A FortiGate has two default routes: All Internet traffic is currently using port1. The exhibit shows partial information for one sample session of Internet traffic from an internal user:

```
config router static
    edit 1
        set gateway 10.200.1.254
        set priority 5
        set device "port1"
    next
    edit2
        set gateway 10.200.2.254
        set priority 10
        set device "port2"
    next
end
```

```
# diagnose sys session list
Session info: proto=6 proto_state=01 duration =17 expire=7 timeout=3600
flags= 00000000 sockflag=00000000 sockport=0 av idx=0 use=3
ha_id=0 policy_dir=0 tunnel=/
state=may_dirty none app_ntf
statistic (bytes/packets/allow_err): org=575/7/1 reply=23367/19/1 tuples=2
origin->sink: org pre->post, reply pre->post dev=4->2/2->4
gwy=10.200.1.254/10.0.1.10
hook=post dir=org act=snat 10.0.1.10:64907-
>54.239.158.170:80(10.200.1.1:64907)
hook=pre ·dir=reply act=dnat 54.239.158.170:80-
>10.200.1.1:64907(10.0.1.10:64907)
pos/(before, after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00000294 tos=ff/ff ips_view=0 app_list=0 app=0
dd_type=0 dd_mode=0
```

What would happen with the traffic matching the above session if the priority on the first default route (IDd1) were changed from 5 to 20?

A. Session would remain in the session table and its traffic would keep using port1 as the outgoing interface.

B. Session would remain in the session table and its traffic would start using port2 as the outgoing interface.

C. Session would be deleted, so the client would need to start a new session.

D. Session would remain in the session table and its traffic would be shared between port1 and port2.

Correct Answer: A

QUESTION 2

Examine the IPsec configuration shown in the exhibit; then answer the question below.

Name	Remote
Comments	Comments

Network

IP Version	⦿ IPv4	◯ IPv6
Remote Gateway	Static IP Address ⬇	
IP Address	10.0.10.1	
Interface	port1 ⬇	
Mode Config	☐	
NAT Traversal	☑	
Keepalive Frequency	10	
Dead Peer Detection	☑	

An administrator wants to monitor the VPN by enabling the IKE real time debug using these commands: diagnose vpn ike log-filter src-addr4 10.0.10.1 diagnose debug application ike -1 diagnose debug enable The VPN is currently up, there is no traffic crossing the tunnel and DPD packets are being interchanged

between both IPsec gateways. However, the IKE real time debug does NOT show any output. Why isn\'t there any output?

A. The IKE real time shows the phases 1 and 2 negotiations only. It does not show any more output once the tunnel is up.

B. The log-filter setting is set incorrectly. The VPN\\'s traffic does not match this filter.

C. The IKE real time debug shows the phase 1 negotiation only. For information after that, the administrator must use the IPsec real time debug instead: diagnose debug application ipsec -1.

D. The IKE real time debug shows error messages only. If it does not provide any output, it indicates that the tunnel is operating normally.

Correct Answer: A

QUESTION 3

When using the SSL certificate inspection method for HTTPS traffic, how does FortiGate filter web requests when the browser client does not provide the server name indication (SNI)?

A. FortiGate uses the Issued To: field in the server\\'s certificate.

B. FortiGate switches to the full SSL inspection method to decrypt the data.

C. FortiGate blocks the request without any further inspection.

D. FortiGate uses the requested URL from the user\\'s web browser.

Correct Answer: D

QUESTION 4

What conditions are required for two FortiGate devices to form an OSPF adjacency? (Choose three.)

A. IP addresses are in the same subnet.

B. Hello and dead intervals match.

C. OSPF IP MTUs match.

D. OSPF peer IDs match.

E. OSPF costs match.

Correct Answer: ABD

QUESTION 5

View the exhibit, which contains the partial output of an IKE real-time debug, and then answer the question below.

```
ike 0:c49e59846861b0f6/000000000000000:278: responder: main mode get 1st message…
ike 0:c49e59846861b0f6/000000000000000:278: incoming proposal:
ike 0:c49e59846861b0f6/000000000000000:278: proposal id = 0:
ike 0:c49e59846861b0f6/000000000000000:278:   protocol id = ISAKMP:
ike 0:c49e59846861b0f6/000000000000000:278:     trans_id = KEY_IKE.
ike 0:c49e59846861b0f6/000000000000000:278:     encapsulation = IKE/none
ike 0:c49e59846861b0f6/000000000000000:278:       type=OAKLEY_ENCRYPT_ALG, val=3DES_CBC.
ike 0:c49e59846861b0f6/000000000000000:278:       type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:c49e59846861b0f6/000000000000000:278:       type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:c49e59846861b0f6/000000000000000:278:       type=OAKLEY_GROUP, val=MODP2048.
ike 0:c49e59846861b0f6/000000000000000:278: ISAKMP SA lifetime=86400
...
ike 0:c49e59846861b0f6/000000000000000:278: my proposal, gw VPN:
ike 0:c49e59846861b0f6/000000000000000:278: proposal id = 1:
ike 0:c49e59846861b0f6/000000000000000:278:   protocol id = ISAKMP:
ike 0:c49e59846861b0f6/000000000000000:278:     trans_id = KEY_IKE.
ike 0:c49e59846861b0f6/000000000000000:278:     encapsulation = IKE/none
ike 0:c49e59846861b0f6/000000000000000:278:       type=OAKLEY_ENCRYPT_ALG, val=AES_CBC,
key-len=256
ike 0:c49e59846861b0f6/000000000000000:278:       type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:c49e59846861b0f6/000000000000000:278:       type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:c49e59846861b0f6/000000000000000:278:       type=OAKLEY_GROUP, val=MODP2048.
ike 0:c49e59846861b0f6/000000000000000:278: ISAKMP SA lifetime=86400
...
ike 0:c49e59846861b0f6/000000000000000:278: negotiation failure
ike Negotiate ISAKMP SA Error: ike 0:c49e59846861b0f6/000000000000000:278:
proposal chosen
...
```

Why didn\'t the tunnel come up?

A. The pre-shared keys do not match.

B. The remote gateway\'s phase 2 configuration does not match the local gateway\'s phase 2 configuration.

C. The remote gateway\'s phase 1 configuration does not match the local gateway\'s phase 1 configuration.

D. The remote gateway is using aggressive mode and the local gateway is configured to use man mode.

Correct Answer: C

QUESTION 6

An administrator has enabled HA session synchronization in a HA cluster with two members. Which flag is added to a primary unit\'s session to indicate that it has been synchronized to the secondary unit?

A. redir.

B. dirty.

C. synced

D. nds.

Correct Answer: C

QUESTION 7

Examine the output of the `get router info ospf interface\\' command shown in the exhibit; then answer the question below.

```
# get router info ospf interface port4
port4 is up, line protocol is up
    Internet Address 172.20.121.236/24, Area 0.0.0.0, MTU 1500
    Process ID 0, Router ID 0.0.0.4, Network Type BROADCAST, Cost: 1
    Transmit Delay is 1 sec, State DROther, Priority 1
    Designated Router (ID) 172.20.140.2, Interface Address 172.20.121.2
Backup Designated Router (ID) 0.0.0.1, Interface Address
172.20.121.239
Timer intervals configured, Hello 10.000, Dead 40, Wait 40, Retransmit
5
    Hello due in 00:00:05
    Neighbor Count is 4, Adjacent neighbor count is 2
    Crypt Sequence Number is 411
    Hello received 106, sent 27, DD received 7 sent 9
    LS-Req received 2 sent 2, LS-Upd received 7 sent 5
    LS-Ack received 4 sent 3, Discarded 1
```

Which statements are true regarding the above output? (Choose two.)

A. The port4 interface is connected to the OSPF backbone area.

B. The local FortiGate has been elected as the OSPF backup designated router.

C. There are at least 5 OSPF routers connected to the port4 network.

D. Two OSPF routers are down in the port4 network.

Correct Answer: AD

QUESTION 8

Which statements about bulk configuration changes using FortiManager CLI scripts are correct? (Choose two.)

A. When executed on the Policy Package, ADOM database, changes are applied directly to the managed FortiGate.

B. When executed on the Device Database, you must use the installation wizard to apply the changes to the managed FortiGate.

C. When executed on the All FortiGate in ADOM, changes are automatically installed without creating a new revision history.

D. When executed on the Remote FortiGate directly, administrators do not have the option to review the changes prior to installation.

Correct Answer: AD

QUESTION 9

An administrator has configured a dial-up IPsec VPN with one phase 2, extended authentication (XAuth)

and IKE mode configuration. The administrator has also enabled the IKE real time debug:

diagnose debug application ike-1

diagnose debug enable

In which order is each step and phase displayed in the debug output each time a new dial- up user is

connecting to the VPN?

A. Phase1; IKE mode configuration; XAuth; phase 2.

B. Phase1; XAuth; IKE mode configuration; phase2.

C. Phase1; XAuth; phase 2; IKE mode configuration.

D. Phase1; IKE mode configuration; phase 2; XAuth.

Correct Answer: D

QUESTION 10

View the exhibit, which contains the output of diagnose sys session stat, and then answer the question

below.

```
NGFW-1 # diagnose sys session stat
misc info:      session_count=591  setup_rate=0  exp_count=0
clash=162  memory_tension_drop=0  ephemeral=0/65536
removeable=0
delete=0, flush-0, dev_down=0/0
TCP sessions:
        166 in NONE state
        1 in ESTABLISHED state
        3 in SYN_SENT state
        2 in TIME_WAIT 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=00000006
global: ses_limit=0  ses6_limit=0  rt_limit=0  rt6_limit=0
```

Which statements are correct regarding the output shown? (Choose two.)

A. There are 0 ephemeral sessions.

B. All the sessions in the session table are TCP sessions.

C. No sessions have been deleted because of memory pages exhaustion.

D. There are 166 TCP sessions waiting to complete the three-way handshake.

Correct Answer: AD

QUESTION 11

View the exhibit, which contains a partial output of an IKE real-time debug, and then answer the question below.

```
ike 0:H2S_0_1: shortcut 10.200.5.1.:0   10.1.2.254->10.1.1.254
…
ike 0:H2S_0_1:15:  sent IKE msg (SHORTCUT-OFFER):  10.200.1.1:500->10.200.5.1:500,
len=164, id=4134df8580d5cdd/ce54851612c7432f:a21f14fe
ike 0: comes 10.200.5.1:500->10.200.1.1:500,ifindex=3….
ike 0: IKEv1 exchange=Informational id=4134df8580d5bcdd/ce54851612c7432f:6266ee8c
len=196

ike 0:H2S_0_1:15: notify msg received: SHORTCUR-QUERY
ike 0:H2S_0_1: recv shortcut-query 16462343159772385317

ike 0:H2S_0_0:16:  senr IKE msg (SHORTCUT-QUERY): 10.200.1.1:500->10.200.3.1:500,
len=196, id=7c6b6cca6700a935/dba061eaf51b89f7:b326df2a
ike 0: comes 10.200.3.1:500->10.200.1.1:500,ifindex=3….
ike 0: IKEv1 exchange=Informational id=7c6b6cca6700a935/dba061eaf51b89f7:1c1dbf39
len=188

ike 0:H2S_0_0:16: notify msg received: SHORTCUT-REPLY
ike 0:H2S_0_0: recv shortcut-reply 16462343159772385317
f97a7565a441e2aa/667d3e2e3442211e 10.200.3.1 to 10.1.2.254 psk 64
ike 0:H2S_0_0: shortcut-reply route to 10.1.2.254 via H2S_0_1 29
ike 0:H2S: forward shortcut-reply 16462343159772385317
f97a7565a441e2aa/667d3e2e3442211e 10.200.3.1 to 10.1.2.254 psk 64 ttl 31
ike 0:H2S_0_1:15: enc
…
ike 0:H2S_0_1:15: sent IKE msg (SHORTCUT-REPLY): 10.200.1.1:500->10.200.5.1:500,
len=188, id=4134df8580d5bcdd/ce54851612c7432f:70ed6d2c
```

Based on the debug output, which phase-1 setting is enabled in the configuration of this VPN?

A. auto-discovery-sender

B. auto-discovery-forwarder

C. auto-discovery-shortcut

D. auto-discovery-receiver

Correct Answer: C

QUESTION 12

A FortiGate device has the following LDAP configuration:

```
config user ldap
    edit "WindowsLDAP"
        set server "10.0.1.10"
        set cnid "cn"
        set dn "cn=Users, dc=trainingAD, dc=training, dc=lab"
        set type regular
        set username "dc=trainingAD, dc=training, dc=lab"
        set password xxxxxxx
    next
end
```

The administrator executed the `dsquery\\' command in the Windows LDAp server 10.0.1.10, and got the following output:

>dsquery user –samid administrator

"CN=Administrator, CN=Users, DC=trainingAD, DC=training, DC=lab"

Based on the output, what FortiGate LDAP setting is configured incorrectly?

A. cnid.

B. username.

C. password.

D. dn.

Correct Answer: A

QUESTION 13

What configuration changes can reduce the memory utilization in a FortiGate? (Choose two.)

A. Reduce the session time to live.

B. Increase the TCP session timers.

C. Increase the FortiGuard cache time to live.

D. Reduce the maximum file size to inspect.

Correct Answer: AD

QUESTION 14

Examine the following traffic log; then answer the question below.

date-20xx-02-01 time=19:52:01 devname=master device_id="xxxxxxx" log_id=0100020007 type=event subtype=system pri critical vd=root service=kemel status=failure msg="NAT port is exhausted." What does the log mean?

A. There is not enough available memory in the system to create a new entry in the NAT port table.

B. The limit for the maximum number of simultaneous sessions sharing the same NAT port has been reached.

C. FortiGate does not have any available NAT port for a new connection.

D. The limit for the maximum number of entries in the NAT port table has been reached.

Correct Answer: B

QUESTION 15

A FortiGate is rebooting unexpectedly without any apparent reason. What troubleshooting tools could an administrator use to get more information about the problem? (Choose two.)

A. Firewall monitor.

B. Policy monitor.

C. Logs.

D. Crashlogs.

Correct Answer: CD

[NSE7 VCE Dumps](#)   [NSE7 Study Guide](#)   [NSE7 Braindumps](#)