Fortinet

Exam Questions FCSS_NST_SE-7.6

FCSS - Network Security 7.6 Support Engineer

NEW QUESTION 1
Exhibit.

```
# diagnose hardware sysinfo memory
MemTotal:          2055916 kB
MemFree:            708880 kB
Buffers:             22140 kB
Cached:             641364 kB
SwapCached:              0 kB
Active:             726352 kB
Inactive:            98908 kB
```

Refer to the exhibit, which shows a partial output of diagnose hardware aysinfo memory. Which two statements about the output are true? (Choose two.)

A. There are 98908 kB o! memory that will never be used.
B. The user space has 708880 kB of physical memory that is not used by the system.
C. The I/O cache, which has 641364 kB of memory allocated to it.
D. The value indicated next to the inactive heading represents the currently unused cache page.

Answer: AD

NEW QUESTION 2
In which two slates is a given session categorized as ephemeral? (Choose two.)

A. A UDP session with only one packet received
B. A UOP session with packets sent and received
C. A TCP session waiting for the SYN ACK
D. A TCP session waiting for FIN ACK

Answer: AC

NEW QUESTION 3
Refer to the exhibits.

```
FGT-B # get router info routing-table all
Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 192.168.1.1, port1, [1/0]
C       10.23.23.0/24 is directly connected, port4
```

```
FGT-B # get router info ospf database brief
...
                AS External Link States

Link ID         ADV Router      Age  Seq#       CkSum Flag Route              Tag
8.8.8.8         0.0.0.112       1464 80000002 3106  0002 E2 8.8.8.8/32       0
```

An administrator Is expecting to receive advertised route 8.8.8.8/32 from FGT-A. On FGT-B, they confirm that the route is being advertised and received, however, the route is not being injected into the routing table. What is the most likely cause of this issue?

A. A batter route to the 8.8.8.8/32 network exists in the routing table.
B. FGT-B is configured with a prefix list denying the 8.8.8.8/32 network to be injected into the routing table.
C. The administrator has misconfigured redistribution of routes on FGT-A.
D. FGT-8 is configured with a distribution list denying the 8.8.8.8/32 network to be injected into the routing table.

Answer: B

NEW QUESTION 4
Refer to the exhibit, which shows a truncated output of a real-time LDAP debug.

```
# diagnose debug application fnbamd -1
# diagnose debug enable
   fnbamd_fsm.c[1274] handle_req-Rcvd auth req 8781845 for jsmith in Lab opt=27 prot=0
   fnbamd_ldap.c[637] resolve_ldap_FQDN-Resolved address 10.10.181.10, result 10.10.181.10
   fnbamd_ldap.c[232] start_search_dn-base:'DC=TAC,DC=ottawa,DC=fortinet,DC=com' filter:sAMAccountName=jsmith
   fnbamd_ldap.c[1351] fnbamd_ldap_get_result-Going to SEARCH state
   fnbamd_fsm.c[1833] poll_ldap_servers-Continue pending for req 8781845
   fnbamd_ldap.c[266] get_all_dn-Found DN 1:CN=John Smith,CN=Users,DC=TAC,DC=ottawa,DC=fortinet,DC=com
```

What two conclusions can you draw from the output? (Choose two.)

A. The name of the configured LDAP server is Lab.
B. The user is authenticating using CN=John Smith.
C. FortiOS is able to locate the user in step 3 (Bind Request) of the LDAP authentication process.
D. FortiOS is performing the second step (Search Request) in the LDAP authentication process.

Answer: BD

NEW QUESTION 5
Exhibit 1.

```
config system global
   set snat-route-change disable
end
-----------------
config router static
   edit 1
      set gateway 10.200.1.254
      set priority 5
      set device "port1"
   next
   edit 2
      set gateway 10.200.2.254
      set priority 10
      set device "port2"
   next
end
```

Exhibit 2.

```
FGT # diagnose sys session list
session info: proto=6 proto_state=01 duration=600 expire=3179 timeout=3600 flags=00000000
sockflag=00000000 sockport= av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan cos=0/255
state=log may_dirty npu f00
statistic (bytes/packets/allow_err): org=3208/25/1 reply=11144/29/1 tuples=2
tx speed (Bps/kbps): 0/0 rx speed (Bps/kbps): 0/0
orgin->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)
src_mac=b4:f7:a1:e9:91:97
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00317c56 tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id = 00000000
dd_type=0 dd_mode=0
npu_state=0x000c00
npu info: flag=0x00/0x00, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0, vlan=0x0000/0x0000
vlifid=0/0, vtag in=0x0000/0x0000 in_npu=0/0, out_npu=0/0, fwd_en=0/0, qid=0/0
no_ofld_reason:
```

Refer to the exhibits, which show the configuration on FortiGate and partial internet session information from a user on the internal network.
An administrator would like to lest session failover between the two service provider connections.
Which two changes must the administrator make to force this existing session to immediately start using the other interface? (Choose two.)

A. Change the priority of the port! static route to 11.
B. Change the priority of the port2 static route to 5.
C. Configure unset snat-route-change to return it to the default setting.
D. Configure set snat-route-change enable.

Answer: AD

NEW QUESTION 6
Refer to the exhibit, which shows a partial output of the real-time LDAP debug.

```
# fnbamd_fsm.c[1274] handle_req-Rcvd auth req 6750221 for jsmith in Lab opt=27 prot=0
fnbamd_ldap.c[637] resolve_ldap_FQDN-Resolved address 10.10.181.10, result 10.10.181.10
fnbamd_ldap.c[232] start_search_dn-base:'DC=fortinet,DC=com' filter:sAMAccountName=jsmith
fnbamd_ldap.c[1351] fnbamd_ldap_get_result-Going to SEARCH state
fnbamd_fsm.c[1833] poll_ldap_servers-Continue pending for req 6750221
fnbamd_ldap.c[275] get_all_dn-Found no DN
fnbamd_ldap.c[298] start_next_dn_bind-No more DN left
fnbamd_ldap.c[1603] fnbamd_ldap_get_result-Auth denied
fnbamd_auth.c[2074] fnbamd_auth_poll_ldap-Result for ldap svr 10.10.181.10 is denied
fnbamd_comm.c[116] fnbamd_comm_send_result-Sending result 1 for req 6750221
```

What two actions can the administrator take to resolve this issue? (Choose two.)

A. Ensure the user logs in using 'John Smith' not 'jsmith'.
B. Ensure the user is providing the correct user credentials.
C. Ensure the user is a member of at least one AD group to ensure step 4 of the LDAP authentication process is successful.
D. Ensure the account is active.

Answer: BD

NEW QUESTION 7
Exhibit.

```
session info: proto=6 proto_state=01 duration=157 expire=3559 timeout=3600 flags=00000000 socktype=0 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
user=User1 state=log may_dirty authed f00 acct-ext
statistic(bytes/packets/allow_err): org=2137/14/1 reply=1663/12/1 tuples=2
tx speed(Bps/kbps): 1/0 rx speed(Bps/kbps): 1/0
orgin->sink: org pre->post, reply pre->post dev=5->3/3->5 gwy=10.1.0.254/10.1.10.1
hook=pre dir=org act=noop 10.1.10.1:34830->35.241.9.150:443(0.0.0.0:0)
hook=post dir=reply act=noop 35.241.9.150:443->10.1.10.1:34830(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 pol_uuid_idx=14735 auth_info=2 chk_client_info=0 vd=0
serial=0000352e tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id=00000000 ngfwid=n/anpu_state=0x000100
no_ofld_reason:  npu-flag-off
```

Refer to the exhibit, which shows the output of a session. Which two statements are true? (Choose Two.)

A. The TCP session has been successfully established.
B. The session was initiated from an authenticated user.
C. The session is being inspected using flow inspection.
D. The session is being offloaded.

Answer: AB

NEW QUESTION 8
Refer to the exhibit, which shows one way communication of the downstream FortiGate with the upstream FortiGate within a Security Fabric.

```
# diagnose sniffer packet any "tcp port 8013 or udp port 8014" 4
Using Original Sniffing Mode
interfaces=[any]
filters=[tcp port 8013 or udp port 8014]
47.220358 port1 in 192.168.1.112.11234 -> 192.168.1.111.8013: syn 1204417526
48.215338 port1 in 192.168.1.112.11234 -> 192.168.1.111.8013: syn 1204417526
50.218552 port1 in 192.168.1.112.11234 -> 192.168.1.111.8013: syn 1204417526
54.222117 port1 in 192.168.1.112.11234 -> 192.168.1.111.8013: syn 1204417526
```

What three actions must you take to ensure successful communication? (Choose three.)
A. You must authorize the downstream FortiGate on the root FortiGate.
B. FortiGate must not be in NAT mode.
C. Ensure TCP port 8013 is not blocked along the way.
D. You must enable Security Fabric/Fortitelemetry on the receiving interface of the upstream FortiGate.
E. Ensure the port for Neighbor Discovery has been changed.

A.

Answer: ACD

NEW QUESTION 9
Refer to the exhibit, which shows a session entry.

```
session_info: proto=1 proto_state=00 duration=1 expire=59 timeout=0 flags=00000000
sockflag=00000000 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log may_dirty none
statistic (bytes/packets/allow_err): org=168/2/1 reply=168/2/1 tuples=2
tx speed (Bps/kbps) : 97/0 rx speed (Bps/kbps) : 97/0
orgin->sink: org pre->post, reply pre->post dev=9->3/3->9 gwy=10.200.1.254/10.1.0.1
hook=post dir=org act=snat 10.1.10.10:40602->10.200.5.1:8 (10.200.1.1:60430)
hook=pre dir=reply act=dnat 10.200.5.1:60430->10.200.1.1:0(10.1.10.10:40602)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=0002a5c9 tos=ff/ff app_list=0 app=0 url_cat=0
dd_type=0 dd_mode=0
```

Which statement about this session is true?

A. Return traffic to the initiator is sent to 10.1.0.1.
B. Return traffic to the initiator is sent lo 10.200.1.254.
C. It is an ICMP session from 10.1.10.10 to 10.200.1.1.
D. It is an ICMP session from 10.1.10.1 to 10.200.5.1.

Answer: B

Explanation:
The session output reveals a session with proto=1 (ICMP) and the origin and reply directions show address and NAT translations. Specifically, thehook=post dir=org act=snatshows that source NAT is performed for outgoing packets, where the source 10.1.10.10:40602 is translated to 10.200.5.1:8 (likely ICMP id 8, not a TCP/UDP port). The reply direction,hook=pre dir=reply act=dnat, indicates destination NAT for incoming packets: packets incoming for 10.200.5.1:60430 are destination-NATed to 10.1.10.10:40602. The gateway (gwy) is listed as 10.200.1.254/10.1.0.1, which for outgoing traffic means that return traffic is directed to the gateway (10.200.1.254), per the NAT policy. This is confirmed by the FortiOS Session Table Guide, which explains that the returned ICMP reply will be routed out to this NAT gateway. The session statistics and logical flow (SNAT out, matching DNAT in) reinforce that reply traffic to the initiator traverses via 10.200.1.254.
FortiOS Administration Guide: Session Table, NAT, and Route Interaction
Fortinet Technical Note: Diagnose sys session list, Direction and NAT Analysis

NEW QUESTION 10
Refer to the exhibit, which shows the partial output of a diagnose command.

```
# diagnose sys session list expectation
session info: proto=6 proto_state=00 duration=6 expire=23 timeout=3600 refresh_dir=both flags=00000000 sockflag=00000000
sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0 policy_dir=1 tunnel=/
state=new npu acct-ext complex
statistic(bytes/packets/allow_err): org=0/0/0 reply=0/0/0 tuples=2
orgin->sink: org pre->post, reply pre->post dev=5->7/7->5 gwy=10.1.1.2/172.17.97.3

hook=pre dir=org act=dnat 93.157.14.94:0->10.200.1.1:60428(10.0.1.10:55402)
hook=pre dir=org act=noop 0.0.0.0:0->0.0.0.0:0(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=25 id_policy_id=0 auth_info=0 chk_client_info=0 vd=0
serial=008423f4 tos=ff/ff ips_view=0 app_list=0 app=0
```

Which two conclusions can you draw from the output shown in the exhibit? (Choose two.)
A. FortiGate will drop the expected traffic if it does not arrive within 23 seconds.
B. Clearing the master session has no impact on the expectation session.
C. This is a pinhole session to allow traffic for a TCP protocol that dynamically assigns TCP ports.
D. The session is checked against firewall policy ID 25.

A.

Answer: AC

NEW QUESTION 10
Refer to the exhibit, which shows the output of a BGP debug command.

```
# get router info bgp summary

VRF 0 BGP router identifier 0.0.0.117, local AS number 65117
BGP table version is 3
3 BGP AS-PATH entries
0 BGP community entries

Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.125.0.60     4      65060    1698    1756      103    0    0 03:02:49        1
10.127.0.75     4      65075    2206    2250      102    0    0 02:45:55        1
100.64.3.1      4      65501    101     115         0    0    0 never       Active

Total number of neighbors 3
```

What can you conclude about the router in this scenario?
A. The router 100.64.3.1 needs to update the local AS number in its BGP configuration in order to bring up the 8GP session with the local router.
B. An inbound route-map on local router is blocking the prefixes from neighbor 100.64.3.1.
C. All of the neighbors displayed are part of a single BGP configuration on the local router with the neighbor-range set to a value of 4.
D. The BGP session with peer 10.127.0.75 is up.

A.

Answer: D

Explanation:
The BGP debug output shows session information for peers, including state details. According to official Fortinet BGP documentation, if the session state with a peer does not show 'Idle,' 'Active,' or 'Connect,' but instead shows 'Established,' 'Up,' or related counters (e.g., messages sent/received or uptime), it indicates the session is operational. In this scenario, the peer 10.127.0.75 is the only one showing a positive indication of a live, established session. Other options like neighbor-range configuration, AS mismatch, or route-maps blocking prefixes are not supported by evidence provided in a simple BGP session state debug, nor does the output show errors relating to local or remote AS issues.
The correct interpretation comes from Fortinet's BGP troubleshooting guide, which outlines how to read session status and neighbor states in debug and summary outputs.
FortiOS BGP Debugging Guide: Session State Interpretation
BGP CLI Reference: Neighbor Status Fields

NEW QUESTION 13
Refer to the exhibit, which shows the port1 interface configuration on FortiGate and partial session information for ICMP traffic.

```
config system interface
    edit "port1"
        set preserve-session-route enable
    next
end

# diagnose sys session list
session info: proto=1 proto_state=00 duration=4 expire=55 timeout=0 refresh_dir=both flags=00000000 socktype=0 sockport=0 av_idx=0 use=3
state=log may_dirty npu f00 route_preserve
orgin->sink: org pre->post, reply pre->post dev=7->19/19->7 gwy=100.64.1.1/10.0.1.101

# diagnose netlink interface list | grep index=19
if=port1 family=00 type=768 index=19 mtu=1420 link=0 master=0
```

What happens to the session information if a routing change occurs that affects this session?
A. Only the interface and gateway information for dev=7 will be removed.
B. The session information will not change unless the current route has been removed from the routing table.
C. The session will be flagged as dirty but no route lookups will be performed.
D. Sessions involving port7 or port19 will not have their routing information flushed.

A.

Answer: B

NEW QUESTION 14
Refer to the exhibit, which shows the modified output of the routing kernel.

Routing information

```
# get router info routing-table database
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
       V - BGP VPNv4
       > - selected route, * - FIB route, p - stale info

Routing table for VRF=0
S     *> 0.0.0.0/0 [10/0] via 10.200.1.254, port1, [1/10]
S        0.0.0.0/0 [20/0] via 10.200.2.254, port2, [5/0]
S        8.8.8.8/32 [10/0] via 172.16.100.254, port8 inactive, [1/0]
O        10.0.1.0/24 [110/1] is directly connected, port3, 00:05:47, [1/0]
C     *> 10.0.1.0/24 is directly connected, port3
O        10.0.2.0/24 [110/1] is directly connected, port4, 00:05:47, [1/0]
C     *> 10.0.2.0/24 is directly connected, port4
B     *> 10.0.3.0/24 [200/10] via 10.0.1.200 (recursive is directly connected, port3), 00:05:40, [1/0]
O     *> 10.0.4.0/24 [110/2] via 10.0.1.200, port3, 00:05:27, [1/0]
B        10.0.4.0/24 [200/10] via 10.0.1.200 (recursive is directly connected, port3), 00:05:40, [1/0]
C     *> 10.200.1.0/24 is directly connected, port1
C     *> 10.200.2.0/24 is directly connected, port2
```

Which statement is true?
A. The egress interface associated with static route 8.8.8.8/32 is administratively up.
B. The default static route through 10.200.1.254 is not in the forwarding information base.
C. The default static route through port2 is in the forwarding information base.
D. The BGP route to 10.0.4.0/24 is not in the forwarding information base.

A.

Answer: D

NEW QUESTION 16
Refer to the exhibit.

```
**** SP Login Dump ****<lasso:Login
xmlns:lasso="http://www.entrouvert.org/namespaces/lasso/0.0"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
LoginDumpVersion="2"><lasso:Request><samlp:AuthnRequest
ID="_EEC718A47FB37B472B205B11153ED409" Version="2.0" IssueInstant="2024-02-
21T00:58:44Z" Destination="https://10.1.10.2/saml-idp/nst/login/"
SignType="0" SignMethod="0" ForceAuthn="false" IsPassive="false"
ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
AssertionConsumerServiceURL="https://10.1.10.254:1003/remote/saml/login/"><sa
ml:Issuer>https://10.1.10.254:1003/remote/saml/metadata/</saml:Issuer><samlp:
NameIDPolicy Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"
AllowCreate="true"/></samlp:AuthnRequest></lasso:Request><lasso:RemoteProvide
rID>http://10.1.10.2/samlidp/nst/metadata/</lasso:RemoteProviderID><lasso:Msg
Url>https://10.1.10.2/saml-
idp/nst/login/?SAMLRequest=jZJfT8IwFMW%2FytL3OW5sAZtBwhhEEtQF0AdfTN0u0GRr22%2
Fnn29vGWIwUeJLk97eX%2B85p01Q1FXDJ63dqxW8tIDWe68rhbw7GJHWKK4FSuRK1IDcFnw9uVnys
Md4Y7TVha7IGXKZEIhgrNSKeItsRJ5ms%4</lasso:HttpRequestMethod><lasso:RequestID>
_EEC718A47FB37B472B205B11153ED409</lasso:RequestID></lasso:Login>
```

The exhibit shows the output from using the command diagnose debug application samld -1 to diagnose a SAML connection.
Based on this output, what can you conclude?
A. Active Directory is used for authentication.
B. The authentication request is for an SSL VPN connection.
C. The IdP IP address is 10.1.10.254.
D. The IdP IP address is 10.1.10.2.

A.

Answer: D

NEW QUESTION 20
Refer to the exhibits.

Exhibit 1

```
FGT-A # get router info bgp summary
...

Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.37.202 4      65110    2500    2552        5    0    0 1d11h33m          0
```

Exhibit 2

```
FGT-B # show router bgp

     config network
         edit 1
             set prefix 172.16.0.0 255.255.0.0
         next
     end
```

Exhibit 3

```
FGT-B # diagnose ip address  list | grep port3
IP=172.16.54.115->172.16.54.202/255.255.255.0 index=5 devname=port3
```

An administrator is attempting to advertise the network configured on port3. However, FGT-A is not receiving the prefix.
Which two actions can the administrator take to fix this problem? (Choose two.)

A. Modify the prefix using the network command from 172.16.0.0/16 to 172.16.54.0/24.
B. Manually add the BGP route on FGT-A.
C. Restart BGP using a soft reset to force both peers to exchange their complete BGP routing tables.
D. Use the set network-import-check disable command.

Answer: AD

NEW QUESTION 23
Refer to the exhibit, which shows the output of get router info bgp summary.

```
get router info bgp summary

VRF 0 BGP router identifier 172.16.1.254, local AS number 65100
BGP table version is 3
2 BGP AS-PATH entries
0 BGP community entries

Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
100.64.1.254    4        100      18      20        3    0    0 00:02:55        1
100.64.2.254    4        100      0        0        0    0    0 never       Active

Total number of neighbors 2
```

Which two statements are true? (Choose two.)

A. The local ForliGate has received one prefix from BGP neighbor 100.64.1.254.
B. The TCP connection with BGP neighbor 100.64.2.254 was successful.
C. The local FortiGate has received 18 packets from a BGP neighbor.
D. The local FortiGate is still calculating the prefixes received from BGP neighbor 100.64.2.264

Answer: AC

Explanation:
The get router info bgp summary output lists BGP neighbor status:
Prefix Reception: The "State/PfxRcd" column shows the number of prefixes received from the neighbor—neighbor 100.64.1.254 has "1", confirming option A.
Received Message Count: Under "MsgRcvd", 18 packets have been received from neighbor 100.64.1.254. This matches option C.
The second neighbor 100.64.2.254 is in "Active" state and has received/sent 0 packets, indicating that its TCP connection is NOT established, disproving option B.
There is no indication anywhere that the router is "still calculating" prefixes; "Active" just means no session is established, so option D is incorrect.
[References:, , FortiOS BGP Command Reference: BGP Neighbor States, PfxRcd, and Counters]

NEW QUESTION 28
In IKEv2, which exchange establishes the first CHILD_SA?

A. IKE_SA_INIT
B. INFORMATIONAL
C. CREATE_CHILD_SA
D. IKE_Auth

Answer: A

Explanation:
According to RFC 7296 (IKEv2) and Fortinet's official documentation, theIKE_SA_INIT exchangeis responsible for negotiating cryptographic parameters, performing the initial Diffie-Hellman exchange, and implementing the cookie challenge mechanism for DoS protection. When the responder suspects a DoS attack (such as mass requests by the same source), it includes a cookie in the IKE_SA_INIT response. The initiator must return the cookie in its next request to prove that it truly exists at the IP address it claims, thereby mitigating resource exhaustion attacks.
This two-step exchange ensures the responder only allocates resources after successful proof of address, aligning with best security practices. Fortinet documentation confirms that this process occurs strictly in the IKE_SA_INIT phase, not in subsequent IKE_Auth or CHILD_SA exchanges.
[References:, RFC 7296: IKEv2, Section 2.6, ??Denial of Service Protection??, Fortinet FortiOS VPN Handbook: IKEv2 Exchange Process and DoS Protection Mechanism, , ,]

NEW QUESTION 29
Refer to the exhibit, which contains partial output from an IKE real-time debug.

Debug output

```
ike 0:624000:98: responder: main mode get 1st message...
ike 0:624000:98: VID DPD AFCAD71368A1F1C96B8696FC77570100
ike 0:624000:98: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3
ike 0:624000:98: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3C0000000
ike 0:624000:98: VID FORTIGATE 8299031757A36082C6A621DE00000000
ike 0:624000:98: incoming proposal:
ike 0:624000:98: proposal id = 0:
ike 0:624000:98:    protocol id = ISAKMP:
ike 0:624000:98:         trans_id = KEY_IKE.
ike 0:624000:98:         encapsulation = IKE/none
ike 0:624000:98:              type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=256
ike 0:624000:98:              type OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:624000:98:              type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:624000:98:              type=OAKLEY_GROUP, val=MODP2048.
ike 0:624000:98: ISAKMP SA lifetime=86400
ike 0:624000:98: proposal id = 0:
ike 0:624000:98:    protocol id = ISAKMP:
ike 0:624000:98:         trans_id = KEY_IKE.
ike 0:624000:98:         encapsulation = IKE/none
ike 0:624000:98:              type OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=256
ike 0:624000:98:              type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:624000:98:              type-AUTH_METHOD, val=PRESHARED_KEY.
ike 0:624000:98:              type=OAKLEY_GROUP, val=MODP1536.
ike 0:624000:98: ISAKMP SA lifetime=86400
ike 0:624000:98: my proposal, gw Remotesite:
ike 0:624000:98: proposal id = 1:
ike 0:624000:98:    protocol id - ISAKMP:
ike 0:624000:98:         trans_id = KEY_IKE.
ike 0:624000:98:         encapsulation = IKE/none
ike 0:620000:98:              type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=128
ike 0:624000:98:              type=OAKLEY_HASH_ALG, val=SHA.
ike 0:624000:98:              type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:624000:98:              type=OAKLEY_GROUP, val=MODP2048.
ike 0:624000:98: ISAKMP SA lifetime=86400
ike 0:624000:98: proposal id = 1:
ike 0:624000:98:    protocol id = ISAKMP:
ike 0:624000:98:         trans_id = KEY_IKE.
ike 0:624000:98:         encapsulation = IKE/none
ike 0:624000:98:              type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=128
ike 0:624000:98:              type=OAKLEY_HASH_ALG, val=SHA.
ike 0:624000:98:              type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:624000:98:              type=OAKLEY_GROUP, val=MODP1536.
ike 0:624000:98: ISAKMP SA lifetime=86400
ike 0:624000:98: negotiation failure
ike Negot:: 624ea7b1bba276fb/0000000000000000:98: no SA proposal chosen
```

The administrator does not have access to the remote gateway.
Based on the debug output, which configuration change the administrator make to the local gateway to resolve the phase 1 negotiation error?

A. In the phase 1 proposal configuration, add AES256-SHA256 to the list of encryption algorithms.
B. In the phase 1 proposal configuration, add AESCBC-SHA2 to the list of encryption algorithms.
C. In the phase 1 network configuration, set the IKE version to 2.
D. In the phase 1 proposal configuration, add AES128-SHA128 to the list of encryption algorithms.

Answer: A

NEW QUESTION 31
Refer to the exhibit, which shows the output of the command get router info ospf neighbor.

```
# get router info ospf neighbor

OSPF process 0, VRF 0:
Neighbor ID     Pri   State           Dead Time   Address         Interface
0.0.0.12          1   Full/DROther    02:14:39    10.10.2.1       wan1
0.0.0.15          1   Full/BDR        04:26:37    10.10.3.2       wan2
0.0.0.18         c1   Full/ -         05:04:36    172.16.1.2      ToHub
```

To what extent does FortiGate operate when looking at its OSPF neighbors? (Choose two.)

A. The local FortiGate has at least one interface that participates in a broadcast network.
B. The local FortiGate has at least one interface that participates in a point-to-point network.
C. The local FortiGate is the DR.
D. Neighbor 0.0.0.18 is the designated router (DR).

Answer: AB

Explanation:
The command on this slide shows a summary of the statuses of all the OSPF neighbors. For each neighbor, it displays the adjacency state and if it is a DR, a BDR, or neither (DROther) Pagina 362 Enterprise_Firewall_7.2_Study. - Point-to-point networks contain only two peers, one at each end of a point-to-point link - Broadcast networks (multi-access) support more than two attached routers. They also support sending messages to multiple recipients (broadcasting). Pagina 365 Enterprise_Firewall_7.2_Study. In any multi-access network there is one DR and one BDR. Pagina 439 Network_Security_Support_Engineer_7.4_Study FULL/- This represents a point-to-point network

NEW QUESTION 34
Which statement about IKEv2 is true?

A. Both IKEv1 and IKEv2 share the feature of asymmetric authentication.
B. IKEv1 and IKEv2 have enough of the header format in common that both versions can run over the same UDP port.
C. IKEv1 and IKEv2 use same TCP port but run on different UDP ports.
D. IKEv1 and IKEv2 share the concept of phase1 and phase2.

Answer: B

NEW QUESTION 36
Refer to the exhibit, which shows the partial output of FortiOS kernel slabs.

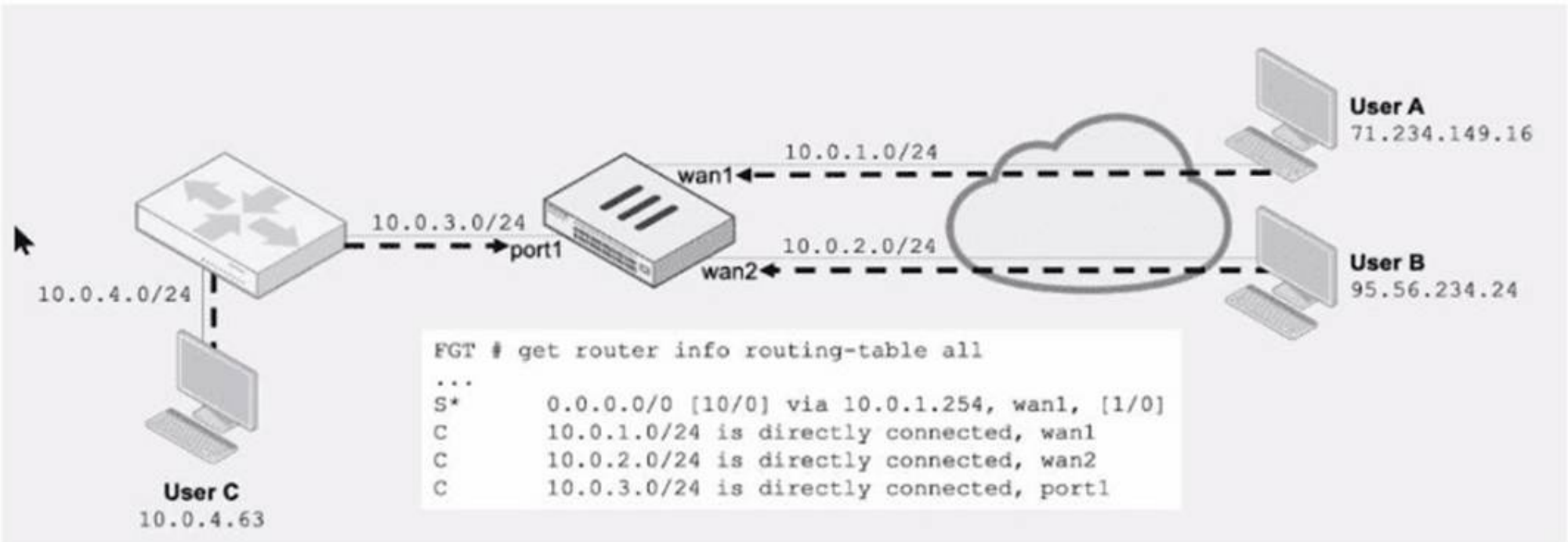
```
...
packet_de_duplication    0    0    128    30    1 : tunables  252  126    0 : slabdata    0    0    0
ip6_nat_record           0    0    128    30    1 : tunables  252  126    0 : slabdata    0    0    0
tcp6_session             0    0   1536     5    2 : tunables   60   30    0 : slabdata    0    0    0
ip6_session              0    0   1300     3    1 : tunables   60   30    0 : slabdata    0    0    0
ip_nat_record            0    0     64    59    1 : tunables  252  126    0 : slabdata    0    0    0
sctp_session             0    0   1600     5    2 : tunables   60   30    0 : slabdata    0    0    0
tcp_session              3    5   1500     5    2 : tunables   60   30    0 : slabdata    1    1    0
ip_session               1    3   1200     3    1 : tunables   60   30    0 : slabdata    1    1    0
...
```

Which statement is true?

A. The total slab size of the sctp_session slab is 0 kB and is associated with the user space.
B. The total slab size of the ip_session slab is 3600 kB and is associated with the user space.
C. The total slab size of the ip6_session slab is 1300 kB and is associated with the kernel.
D. The total slab size of the tcp_session slab is 7500 kB and is associated with the kernel.

Answer: D

NEW QUESTION 40
Refer to the exhibit.



Assuming a default configuration, which three statements are true? (Choose three.)

A. Strict RPF is enabled by default.
B. User B: Fai
C. There is no route to 95.56.234.24 using wan2 in the routing table.
D. User A: Pas
E. The default static route through wan1 passes the RPF check regardless of the source IP address.
F. User B: Pas
G. FortiGate will use asymmetric routing using wan1 to reply to traffic for 95.56.234.24.
H. User C: Fai
I. There is no route to 10.0.4.63 using port1 in the touting table.

Answer: BDE

NEW QUESTION 44
Refer to the exhibit, which shows the output o! the BGP database.

```
router info bgp network
0 BGP table version is 3, local router ID is 1.1.1.1
tus codes: s suppressed, d damped, h history, * valid, > best, i - internal,
           S Stale
gin codes: i - IGP, e - EGP, ? - incomplete

Network          Next Hop            Metric     LocPrf Weight RouteTag Path
.0.0.0/0         100.64.2.254    0              100      0         0 ? <-/->
                 100.64.2.1                          32768         0 ? <-/1>
.2.2.1/32        100.64.2.1                          32768         0 ? <-/1>
.8.8.8/32        100.64.2.254    0              100      0         0 ? <-/1>
0.20.30.0/24     172.16.54.115   0              100      0         0 i <-/1>

l number of prefixes 4
```

Which two statements are correct? (Choose two.)

A. The advertised prefix of 10.20.30.0'24 was configured using the network command.
B. The first four prefixes are being advertised using a legacy route advertisement.
C. The advertised prefix of 10.20.30.0'24 is being advertised through the redistribution of another routing protocol.
D. The output shows all prefixes advertised by all neighbors as well as the local router.

Answer: AD

NEW QUESTION 47
Refer to the exhibit, which shows partial outputs from two routing debug commands.

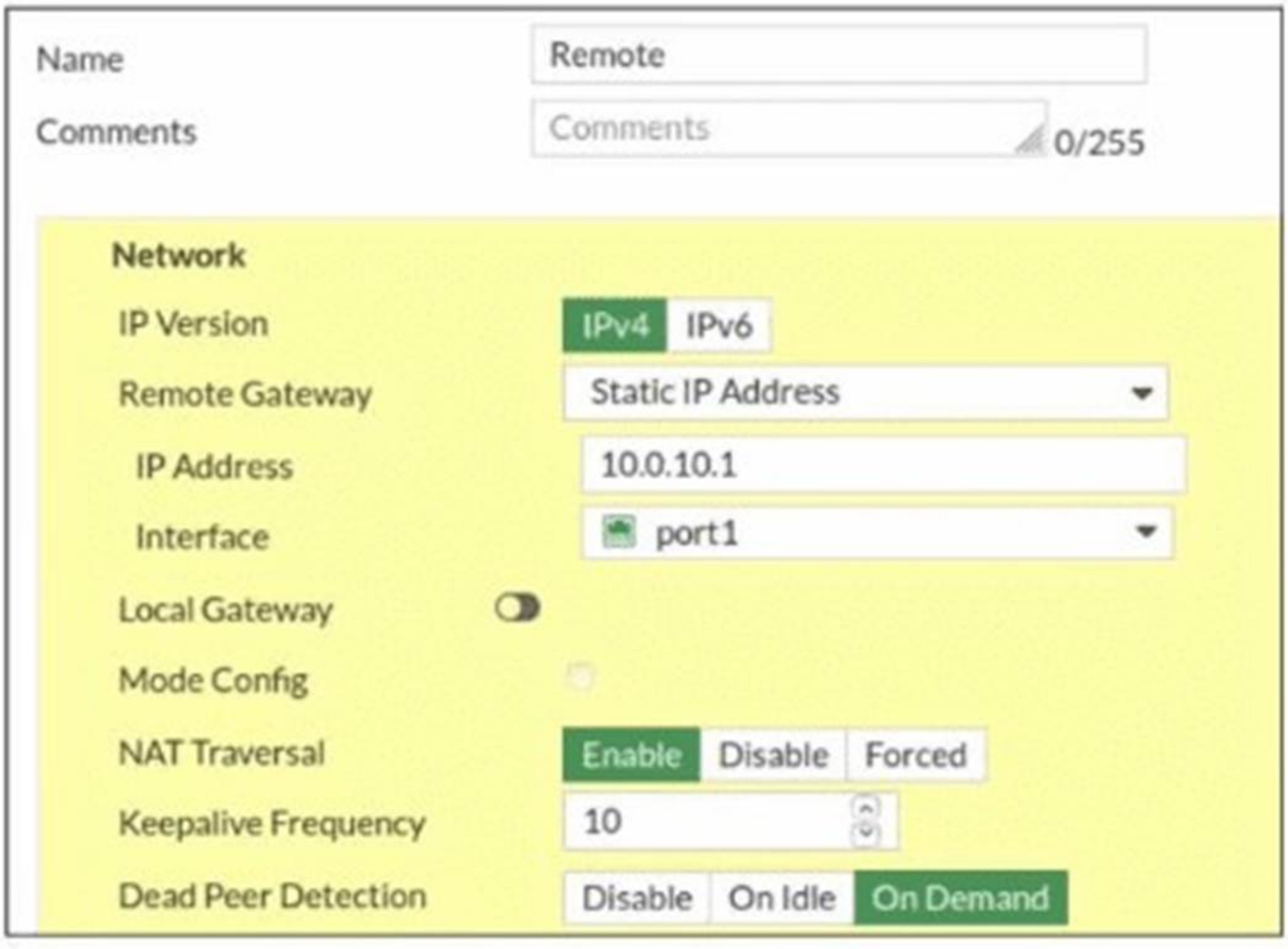
```
FortiGate # get router info kernel
tab=254 vf=0 scope=0 type=1 proto=11 prio=0 0.0.0.0/0.0.0.0/0->0.0.0.0/0 pref=0.0.0.0 qwy=100.64.1.254 dev=3 (port1)
tab=254 vf=0 scope=0 type=1 proto=11 prio=10 0.0.0.0/0.0.0.0/0->0.0.0.0/0 pref=0.0.0.0 gwy=100.64.2.254 dev=6 (port2)
tab=254 vf=0 scope=253 type=1 proto=2 prio=0 0.0.0.0/0.0.0.0/0->10.1.0.0/24 pref=10.1.0.254 gwy=0.0.0.0 dev=9 (port3)

FortiGate # get router info routing-table all

Routing table for VRF=0
S*          0.0.0.0/0 [10/0] via 100.64.1.254, port1
                             [10/0] via 100.64.2.254, port2, [10/0]
C           10.1.0.0/24 is directly connected, port3
S           10.1.10.0/24 [10/0] via 10.1.0.1, port3
C           100.64.1.0/24 is directly connected, port1
C           100.64.2.0/24 is directly connected, port2
```

Which change must an administrator make on FortiGate to route web traffic from internal users to the internet, using ECMP?

A. Set snat-route-change to enable.
B. Set the priority of the static default route using port2 to 1.
C. Set preserve-session-route to enable.
D. Set the priority of the static default route using port1 to 10.

Answer: D

NEW QUESTION 49
Exhibit.



Refer to the exhibit, which contains a screenshot of some phase 1 settings.
The VPN is not up. To diagnose the issue, the administrator enters the following CLI commands on an SSH session on FortiGate:

```
diagnose vpn ike log-filter dst-addr4 10.0.10.1
diagnose debug application ike -1
```

However, the IKE real-time debug does not show any output. Why?

A. The administrator must also run the command diagnose debug enable.
B. The debug shows only error message

C. If there is no output, then the phase 1 and phase 2 configurations match.
D. The log-filter setting is incorrec
E. The VPN traffic does not match this filter.
F. Replace diagnose debug application ike -1 with diagnose debug application ipsec -1.

Answer: A

NEW QUESTION 52
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

FCSS_NST_SE-7.6 Practice Exam Features:

* FCSS_NST_SE-7.6 Questions and Answers Updated Frequently

* FCSS_NST_SE-7.6 Practice Questions Verified by Expert Senior Certified Staff

* FCSS_NST_SE-7.6 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* FCSS_NST_SE-7.6 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year