NSE7_EFW-7.0 Q&As

Fortinet NSE 7 - Enterprise Firewall 7.0

Pass Fortinet NSE7_EFW-7.0 Exam with 100% Guarantee

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

https://www.certbus.com/nse7_efw-7-0.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 is configured as an explicit web proxy. Clients using this web proxy are reposting DNS errors when accessing any website. The administrator executes the following debug commands and observes that the n-dns-timeout counter is increasing:

```
#diagnose test application wad 2200
#diagnose test application wad 104
DNS Stats:
n_dns_reqs=878  n_dns_fails= 2  n_dns_timeout=875
n_dns_success=0

n_snd_retries=0  n_snd_fails=0 n_snd_success=0 n_dns_overflow=0
n_build_fails=0
```

What should the administrator check to fix the problem?

A. The connectivity between the FortiGate unit and the DNS server.

B. The connectivity between the client workstations and the DNS server.

C. That DNS traffic from client workstations is allowed by the explicit web proxy policies.

D. That DNS service is enabled in the explicit web proxy interface.

Correct Answer: A

QUESTION 2

Refer to the exhibit, which shows the output of diagnose sys session list.

```
# diagnose sys session list
session info: proto=6 proto_state=01 duration=73 expire=3597 timeout=3600
flags=00000000 sockflag=00000000 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
state=may_dirty synced none app_ntf
statistic(bytes/packets/allow_err): org=822/11/1 reply=9037/15/1 tuples=2
orgin->sink: org pre->post, reply pre->post dev=4->2/2->4
gwy=100.64.1.254/10.0.1.10
hook=post dir=org act=snat 10.0.1.10:65464->54.192.15.182:80(100.64.1.1:65464)
hook=pre dir=reply act=dnat 54.192.15.182:80->100.64.1.1:65464(10.0.1.10:65464)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00000098 tos=ff/ff ips_view=0 app_list=0 app=0
dd_type=0 dd_mode=0
```

If the HA ID for the primary device is 0, what will happen if the primary fails and the secondary becomes the primary?

A. Traffic for this session continues to be permitted on the new primary device after failover, without requiring the client to restart the session with the server.

B. The secondary device has this session synchronized; however, because application control is applied, the session will be marked dirty and have to be re-evaluated after failover.

C. The session state will be preserved but the kernel will need to re-evaluate the session due to NAT being applied.

D. The session will be removed from the session table of the secondary device due to the presence of allowed error packets, which will force the client to restart the session with the server.

Correct Answer: A

Explanation: https://community.fortinet.com/t5/FortiGate/Technical-Note-How-to-see-if-a- session-is-synced-in-HA/ta-p/194185

QUESTION 3

View the exhibit, which contains the output of a BGP debug command, and then answer the question below.

```
FGT # get router info bgp summary
BGP router identifier 0.0.0.117, local AS number 65117
BGP table version is 104
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
```

Which of the following statements about the exhibit are true? (Choose two.)

A. The local router\\'s BGP state is Established with the 10.125.0.60 peer.

B. Since the counters were last reset; the 10.200.3.1 peer has never been down.

C. The local router has received a total of three BGP prefixes from all peers.

D. The local router has not established a TCP session with 100.64.3.1.

Correct Answer: AD

QUESTION 4

Refer to the exhibit, which shows a FortiGate configuration.

```
config system fortiguard
    set protocol udp
    set port 8888
    set load-balance-servers 1
    set auto-join-forticloud enable
    set update-server-location any
    set sandbox-region ''
    set fortiguard-anycast disable
    set antispam-force-off disable
    set antispam-cache enable
    set antispam-cache-ttl 1800
    set antispam-cache-mpercent 2
    set antispam-timeout 7
    set webfilter-force-off enable
    set webfilter-cache enable
    set webfilter-cache-ttl 3600
    set webfilter-timeout 15
    set sdns-server-ip "208.91.112.220"
    set sdns-server-port 53
    unset sdns-options
    set source-ip 0.0.0.0
    set source-ip6 ::
    set proxy-server-ip 0.0.0.0
    set proxy-server-port 0
    set proxy-username ''
    set ddns-server-ip 0.0.0.0
    set ddns-server-port 443
end
```

An administrator is troubleshooting a web filter issue on FortiGate. The administrator has configured a web filter profile and applied it to a policy; however, the web filter is not inspecting any traffic that is passing through the policy. What

must the administrator change to fix the issue?

A. Increase webfilter-timeout.

B. Change protocol to TCP.

C. Enable fortiguard-anycast.

D. Disable webfilter-force-off.

Correct Answer: D

Reference: https://docs.fortinet.com/document/fortigate/6.4.5/cli-reference/109620/config- system-fortiguard

QUESTION 5

The logs in a FSSO collector agent (CA) are showing the following error:

failed to connect to registry: PIKA1026 (192.168.12.232)

What can be the reason for this error?

A. The CA cannot resolve the name of the workstation.

B. The FortiGate cannot resolve the name of the workstation.

C. The remote registry service is not running in the workstation 192.168.12.232.

D. The CA cannot reach the FortiGate with the IP address 192.168.12.232.

Correct Answer: C

https://kb.fortinet.com/kb/documentLink.do?externalID=FD30548

QUESTION 6

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

```
Student# get router info bgp summary
BGP router indentifier 10.200.1.1, local AS number 65500
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries

Neighbor   V     AS   MsgRcvd MsgSent   TblVer  InQ  OutQ  Up/Down  State/PfxRcd
10.200.3.1 4  65501        92     112        0    0     0  never    Connect

Total number of neighbors 1
```

Which statement can explain why the state of the remote BGP peer 10.200.3.1 is Connect?

A. The local peer is receiving the BGP keepalives from the remote peer but it has not received any BGP prefix yet.

B. The TCP session for the BGP connection to 10.200.3.1 is down.

C. The local peer has received the BGP prefixed from the remote peer.

D. The local peer is receiving the BGP keepalives from the remote peer but it has not received the OpenConfirm yet.

Correct Answer: B

http://www.ciscopress.com/articles/article.asp?p=2756480andseqNum=4

QUESTION 7

Refer to the exhibits, which show the configuration on FortiGate and partial internet session information from a user on the internal network.

Configuration Session

```
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
```

Configuration Session

```
FGT # diagnose sys session list
session info: proto=6 proto_state=01 duration=600 expire=3179 timeout=3600 flags=00000000
sockflag=00000000 sockport=0 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=00317c5b 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:
```

An administrator would like to test session failover between the two service provider connections.

What changes must the administrator make to force this existing session to immediately start using the other interface? (Choose two.)

A. Configure set snat-route-change enable.

B. Change the priority of the port2 static route to 5.

C. Change the priority of the port1 static route to 11.

D. unset snat-route-change to return it to the default setting.

Correct Answer: AC

Explanation: Enterprise_Firewall_7.0_Study_Guide-Online.pdf p 148-149

QUESTION 8

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

The synced sessions have the `synced\\' flag. The command `diag sys session list\\' can be used to see the sessions on the member, with the associated flags.

QUESTION 9

View the exhibit, which contains an entry in the session table, and then answer the question below.

```
session info: proto=6 proto_state=11 duration=53 expire=265 timeout=300 flags=00000000
sockflag=00000000
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
user=AALI state=redir log local may_dirty npu nlb none acct-ext
statistic (bytes/packets/allow_err): org=2651/17/1 reply=19130/28/1 tuples=3
tx speed (Bps/kbps): 75/0 rx speed (Bps/kbps): 542/4
orgin->sink: org pre->post, reply pre->post dev=7->6/6->7 gwy=172.20.121.2/10.0.0.2
hook=post dir=org act=snat 192.167.1.100:49545->216.58.216.238:443(172.20.121.96:49545)
hook=pre dir=reply act=dnat 216.58.216.238:443->172.20.121.96:49545 (192.167.1.100:49545)
hook=post dir=reply act=noop 216.58.216.238:443->192.167.1.100:49545 (0.0.0.0:0)
pos/(before, after) 0/(0,0), 0/(0,0)
src_mac=08:5b:0e:6c:7b:7a
misc=0 policy_id=21 auth_info=0 chk_client_info=0 vd=0
serial=007f2948 tos=ff/ff app_list=0 app=0 url_cat=41
dd_type=0 dd_mode=0
npu_state=00000000
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
```

Which one of the following statements is true regarding FortiGate\\'s inspection of this session?

A. FortiGate applied proxy-based inspection.

B. FortiGate forwarded this session without any inspection.

C. FortiGate applied flow-based inspection.

D. FortiGate applied explicit proxy-based inspection.

Correct Answer: A

https://kb.fortinet.com/kb/viewContent.do?externalId=FD30042

QUESTION 10

Examine the partial output from the IKE real time debug shown in the exhibit; then answer the question below. Why didn\\'t the tunnel come up?

A. IKE mode configuration is not enabled in the remote IPsec gateway.

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. One IPsec gateway is using main mode, while the other IPsec gateway is using aggressive mode.

Correct Answer: C

QUESTION 11

Which two statements about OCVPN are true? (Choose two.)

A. Only root vdom supports OCVPN.

B. OCVPN supports static and dynamic IPs in WAN interface.

C. OCVPN offers only Hub-Spoke VPNs.

D. FortiGate devices under different FortiCare accounts can be used to form OCVPN.

Correct Answer: AB

Reference: https://docs.fortinet.com/document/fortigate/6.0.0/cookbook/977344/one-click-vpn-ocvpn
https://docs.fortinet.com/document/fortigate/6.2.9/cookbook/496884/overlay-controller-vpn- ocvpn

QUESTION 12

Which of the following conditions must be met for a static route to be active in the routing table? (Choose three.)

A. The next-hop IP address is up.

B. There is no other route, to the same destination, with a higher distance.

C. The link health monitor (if configured) is up.

D. The next-hop IP address belongs to one of the outgoing interface subnets.

E. The outgoing interface is up.

Correct Answer: CDE

A configured static route only goes to routing table from routing database when all the following are met : The outgoing interface is up There is no other matching route with a lower distance The link health monitor (if configured) is successful The next-hop IP address belongs to one of the outgoing interface subnets

QUESTION 13

Refer to the exhibit, which shows the output of a debug command.

```
FGT # get router info ospf neighbor

OSPF process 0:
Neighbor ID     Pri   State           Dead Time     Address         Interface
0.0.0.69          1   Full/DR         00:00:32      10.126.0.69     wan1
0.0.0.117         1   Full/DROther    00:00:34      10.126.0.117    wan2
0.0.0.2           1   Full/ -         00:00:38      172.16.1.2      ToRemote
```

What can be concluded from the debug command output?

A. The OSPF router with the ID 0.0.0.69 has its OSPF priority set to 0.

B. The local FortiGate has a different MTU value from the OSPF router with ID 0.0.0.2, based on the state information.

C. There are more than two OSPF routers on the wan2 network.

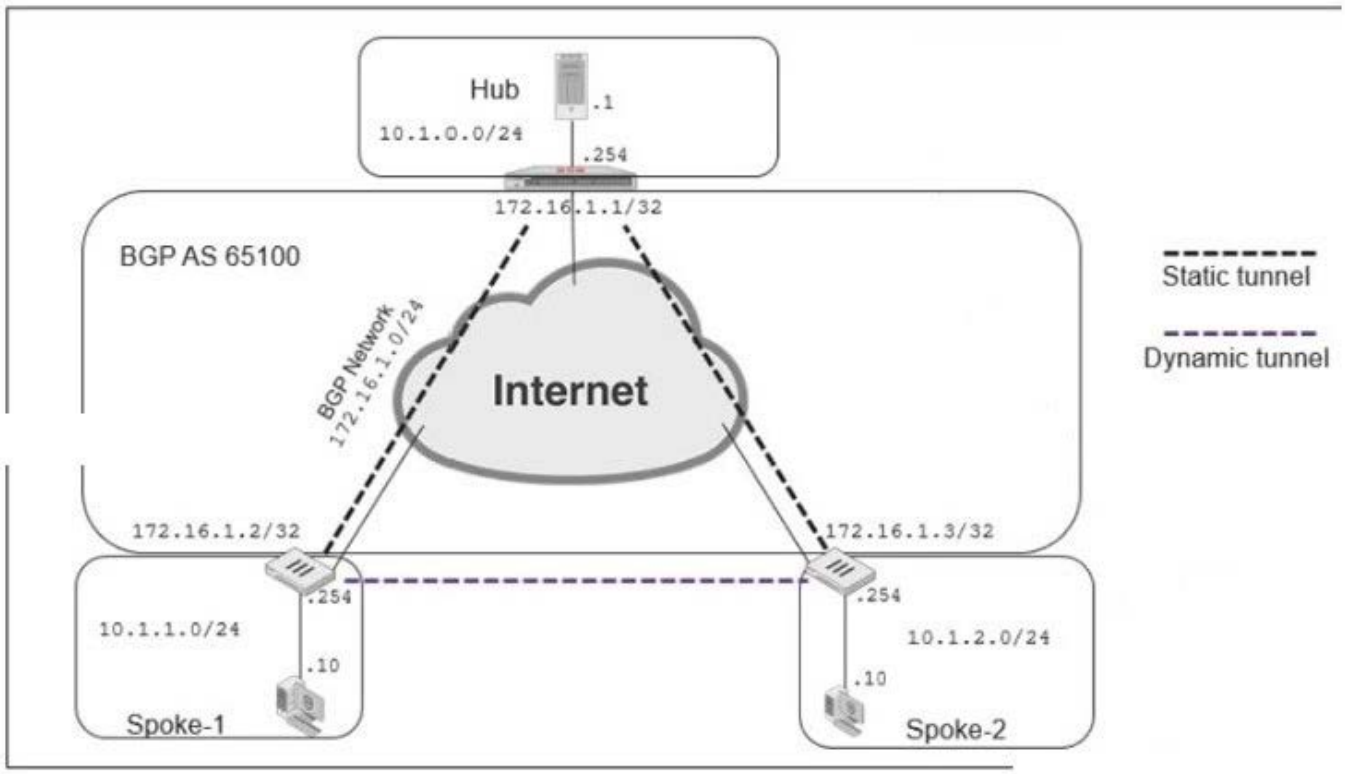
D. The interface ToRemote is a broadcast OSPF network.

Correct Answer: C

Explanation: Enterprise_Firewall_7.0_Study_Guide-Online.pdf p 296

QUESTION 14

Exhibits:




```
how router bgp
router bgp
 as 65100
 router-id 172.16.1.1
fig neighbor-group
 edit "advpn"
     set remote-as 65100

     set route-reflector-client disable
 next

fig neighbor-range
 edit 1
     set prefix 172.16.1.0 255.255.255.0
     set neighbor-group "advpn"
 next
```

Refer to the exhibits, which contain the network topology and BGP configuration for a hub.

An administrator is trying to configure ADVPN with a hub-spoke VPN setup using iBGP. All the VPNs are up and connected to the hub. The hub is receiving route information from both spokes over iBGP; however, the spokes are not receiving

route information from each other.

What change must the administrator make to the hub BGP configuration so that the routes learned by one spoke are forwarded to the other spokes?

A. Configure an individual neighbor and remove neighbor-range configuration.

B. Configure the hub as a route reflector client.

C. Change the router id to 10.1.0.254.

D. Make the configuration of remote-as different from the configuration of local-as.

Correct Answer: B

Explanation: Source: https://community.fortinet.com/t5/FortiGate/Technical-Tip- Configuring-BGP-route-reflector/ta-p/191503 Source 2: RFC 4456

QUESTION 15

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: B