



Fortinet

NSE7_EFW-6.4

Fortinet NSE 7 - Enterprise Firewall 6.4

QUESTION & ANSWERS

QUESTION 1

Which two statements about an auxiliary session are true? (Choose two.)

- A. With the auxiliary session setting enabled, ECMP traffic is accelerated to the NP6 processor.
- B. With the auxiliary session setting enabled, two sessions will be created in case of routing change.
- C. With the auxiliary session setting disabled, for each traffic path, FortiGate will use the same auxiliary session.
- D. With the auxiliary session disabled, only auxiliary sessions will be offloaded.

Correct Answer: C,D

QUESTION 2

An administrator cannot connect to the GIU of a FortiGate unit with the IP address 10.0.1.254. The administrator runs the debug flow while attempting the connection using HTTP. The output of the debug flow is shown in the exhibit:

```
# diagnose debug flow filter port 80
# diagnose debug flow trace start 5
# diagnose debug enable

id=20085 trace_id=5 msg="vd-root received a packet(proto=6,
10.0.1.10:57459->10.0.1.254:80) from port3. flag [S], seq 3190430861, ack
0, win 8192"
id=20085 trace_id=5 msg="allocate a new session-0000008c"
id=20085 trace_id=5 msg="iprope_in_check() check failed on policy 0, drop"
```

Based on the error displayed by the debug flow, which are valid reasons for this problem? (Choose two.)

- A. HTTP administrative access is disabled in the FortiGate interface with the IP address 10.0.1.254.
- B. Redirection of HTTP to HTTPS administrative access is disabled.
- C. HTTP administrative access is configured with a port number different than 80.
- D. The packet is denied because of reverse path forwarding check.

Correct Answer: A,C

QUESTION 3

An administrator has configured the following CLI script on FortiManager, which failed to apply any changes to the managed device after being executed.

```
# conf rout stat
#     edit 0
#         set gateway 10.20.121.2
#         set priority 20
#         set device "wan1"
#     next
# end
```

Why didn't the script make any changes to the managed device?

- A. Commands that start with the # sign are not executed.
- B. CLI scripts will add objects only if they are referenced by policies.
- C. Incomplete commands are ignored in CLI scripts.
- D. Static routes can only be added using TCL scripts.

Correct Answer: A

Explanation/Reference:

https://help.fortinet.com/fmgr/50hlp/56/5-6-2/FortiManager_Admin_Guide/1000_Device_Manager/2400_Scripts/1000_Script_samples/0200_CLI_scripts+.htm#Error_Messages

A sequence of FortiGate CLI commands, as you would type them at the command line. A comment line starts with the number sign (#). A comment line will not be executed.

QUESTION 4

View the IPS exit log, and then answer the question below.

```
# diagnose test application ipsmonitor3
ipsengine exit log"
pid = 93 (cfg), duration = 5605322 (s) at Wed Apr 19 09:57:26 2017
code = 11, reason: manual
```

What is the status of IPS on this FortiGate?

- A. IPS engine memory consumption has exceeded the model-specific predefined value.
- B. IPS daemon experienced a crash.
- C. There are communication problems between the IPS engine and the management database.
- D. All IPS-related features have been disabled in FortiGate's configuration.

Correct Answer: D

Explanation/Reference:

The command `diagnose test application ipsmonitor` includes many options that are useful for troubleshooting purposes. Option 3 displays the log entries generated every time an IPS engine process stopped. There are various reasons why these logs are generated: Manual: Because of the configuration, IPS no longer needs to run (that is, all IPS-related features have been disabled)

QUESTION 5

Examine the output of the `'diagnose sys session list expectation'` command shown in the exhibit; then answer the question below.

```
#diagnose sys session list expectation

session info: proto= proto_state=0 0 duration=3 expire=26 timeout=3600
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 complex
statistic (bytes/packets/allow_err): org=0/0/0 reply=0/0/0 tuples=2
origin-> sink: org pre-> post, reply pre->post dev=2->4/4->2
gwy=10.0.1.10/10.200.1.254
hook=pre dir=org act=dnat 10.171.121.38:0-> 10.200.1.1: 60426
(10.0.1.10: 50365)
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=1.auth_info=0.chk_client_info=0.vd=0
serial1=000000e9.tos=ff/ff.ips_view=0 app_list=0.app=0
dd type=0.dd_mode=0
```

Which statement is true regarding the session in the exhibit?

- A. It was created by the FortiGate kernel to allow push updates from FortiGuard.
- B. It is for management traffic terminating at the FortiGate.
- C. It is for traffic originated from the FortiGate.
- D. It was created by a session helper or ALG.

Correct Answer: D

QUESTION 6

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: C,D,E

Explanation/Reference:

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 7

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: A,B

Explanation/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 8

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

Name

Comments

Network

IP Version IPv4 IPv6

Remote Gateway

IP Address

Interface

Mode Config

NAT Traversal

Keepalive Frequency

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: B

QUESTION 9

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

QUESTION 10

Four FortiGate devices configured for OSPF connected to the same broadcast domain. The first unit is elected as the designated router The second unit is elected as the backup designated router Under normal operation, how many OSPF full adjacencies are formed to each of the other two units?

- A. 1
- B. 2
- C. 3
- D. 4

Correct Answer: B

QUESTION 11

What events are recorded in the crashlogs of a FortiGate device? (Choose two.)

- A. A process crash.
- B. Configuration changes.
- C. Changes in the status of any of the FortiGuard licenses.
- D. System entering to and leaving from the proxy conserve mode.

Correct Answer: A,D

Explanation/Reference:

diagnose debug crashlog read

```
275: 2014-08-05 13:03:53 proxy=acceptor service=imap session fail mode=activated 276: 2014-08-05 13:03:53 proxy=acceptor service=ftp session fail mode=activated 277: 2014-08-05 13:03:53 proxy=acceptor service=nntp session fail mode=activated 278: 2014-08-06 11:05:47 service=kernel conserve=on free="45034 pages" red="45874 pages" msg="Kernel 279: 2014-08-06 11:05:47 enters conserve mode" 280: 2014-08-06 13:07:16 service=kernel conserve=exit free="86704 pages" green="68811 pages" 281: 2014-08-06 13:07:16 msg="Kernel leaves conserve mode" 282: 2014-08-06 13:07:16 proxy=imd sysconserve=exited total=1008 free=349 marginenter=201 283: 2014-08-06 13:07:16 marginexit=302
```

Correct Answer: B

[Certspilot now are offering 100% pass ensure dumps!](#)

Practice Exam Features:

- Questions and Answers Updated Frequently
- Practice Questions Verified by Expert Senior Certified Staff
- Most Realistic Questions that Guarantee you a Pass on Your First Try
- Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

[100% Actual & Verified — Instant Download, Please Click](#)

[Unlock The latest Dumps Here](#)

