



Fortinet

Exam Questions FCSS_NST_SE-7.4

FCSS - Network Security 7.4 Support Engineer

About ExamBible

[Your Partner of IT Exam](#)

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1

Exhibit.

```
# diagnose automation test HAFailOver
automation test failed(1). stitch:HAFailOver
```

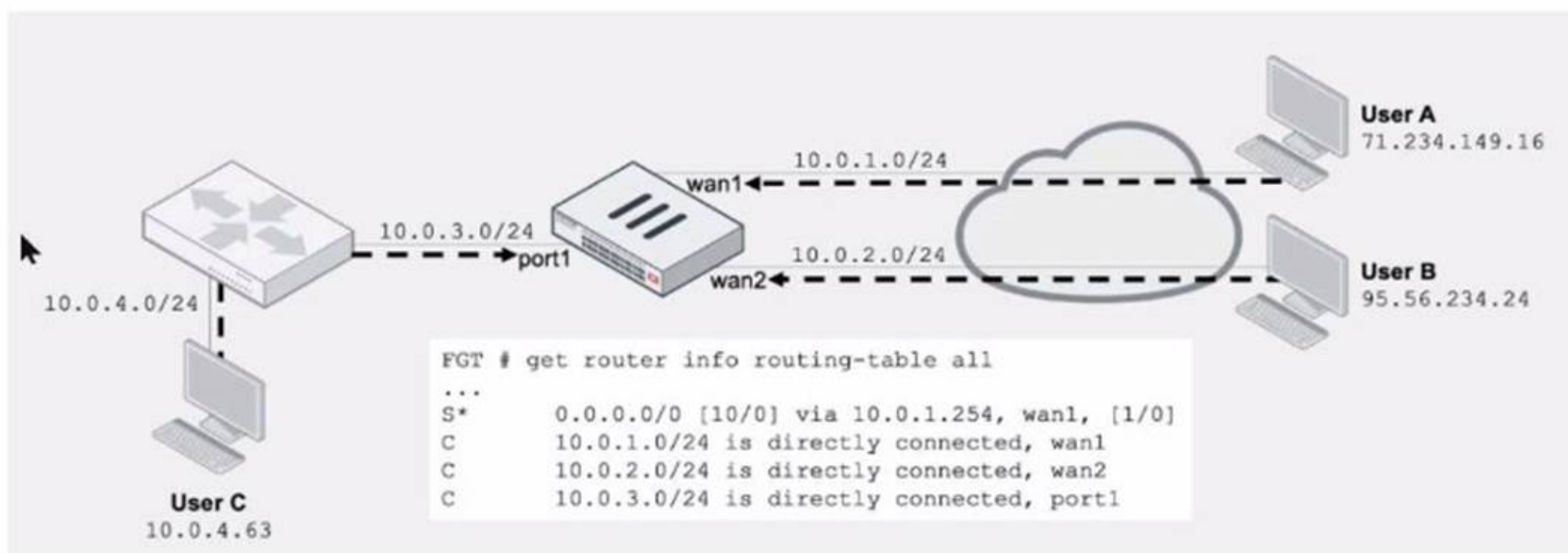
Refer to the exhibit, which shows the output of diagnose automation test. What can you observe from the output? (Choose two.)

- A. The automation stitch test is not being logged.
- B. The automation stitch test failed but the HA failover was successful.
- C. An HA failover occurred.
- D. The test was unsuccessful.

Answer: AD

NEW QUESTION 2

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 routing table.

Answer: BDE

NEW QUESTION 3

An administrator wants to capture encrypted phase 2 traffic between two FortiGate devices using the built-in sniffer.

If the administrator knows that there is no NAT device located between both FortiGate devices, which command should the administrator run?

- A. diagnose sniffer packet any 'udp port 500'
- B. diagnose sniffer packet any 'ip proto 50'
- C. diagnose sniffer packet any 'udp port 4500'
- D. diagnose sniffer packet any 'ah'

Answer: B

NEW QUESTION 4

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

```
# diagnose debug application fnbamd -l
# 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

Consider the scenario where the server name indication (SNI) does not match either the common name (CN) or any of the subject alternative names (SAN) in the server certificate.

Which action will FortiGate take when using the default settings for SSL certificate inspection?

- A. FortiGate uses the SNI from the user's web browser.
- B. FortiGate closes the connection because this represents an invalid SSL/TLS configuration.
- C. FortiGate uses the first entry listed in the SAN field in the server certificate.
- D. FortiGate uses the ZN information from the Subject field in the server certificate.

Answer: C

NEW QUESTION 6

Refer to the exhibit.

```
# diagnose sys top
Run Time: 0 days, 0 hours and 18 minutes
OU, ON, 1S, 95I, OWA, OHI, OSI, OST; 16063, 12523F
      pyfcgid      248      S      2.9      3.8      9
      newcli       251      R      0.1      1.0      5
merged_daemons   185      S      0.1      0.7      6
      miglogd      177      S      0.0      6.8      0
      pyfcgid      249      S      0.0      3.0      2
      pyfcgid      246      S      0.0      2.8      5
      reportd      197      S      0.0      2.7      2
      cmdbsvr      113      S      0.0      2.4      7
```

Which three pieces of information does the diagnose sys top command provide? (Choose three.)

- A. The miglogd daemon is running on CPU core ID 0.
- B. The diagnose sys top command has been running for 18 minutes.
- C. The miglogd daemon would be on top of the list, if the administrator pressed m on the keyboard.
- D. The cmdbsvr process is occupying 2.4% of the total user memory space.
- E. If the neweli daemon continues to be in the R state, it will need to be manually restarted.

Answer: ABD

NEW QUESTION 7

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 gwy=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 8

Which two statements about Security Fabric communications are true? (Choose two.)

- A. FortiTelemetry and Neighbor Discovery both operate using TCP.
- B. The default port for Neighbor Discovery can be modified.
- C. FortiTelemetry must be manually enabled on the FortiGate interface.
- D. By default, the downstream FortiGate establishes a connection with the upstream FortiGate using TCP port 8013.

Answer: CD

NEW QUESTION 10

.....

Relate Links

100% Pass Your FCSS_NST_SE-7.4 Exam with Examible Prep Materials

https://www.exambible.com/FCSS_NST_SE-7.4-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>