



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

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

```
FGT # 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, VRF 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 6 sent 3
  LS-Req received 2 sent 2, LS-Upd received 7 sent 17
  LS-Ack received 4 sent 3, Discarded 1
```

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

- A. The interface is part of the OSPF backbone area.
- B. There are a total of five OSPF routers attached to the port4 network segment.
- C. One of the neighbors has a router ID of 0.0.0.4.
- D. In the network connected to port4, two OSPF routers are down.

Answer: AD

NEW QUESTION 2

In which two states is a given session categorized as ephemeral? (Choose two.)

- A. A UDP session with only one packet received
- B. A UDP 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

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

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
origin->sink: org pre->post, reply pre->post dev=5->3/3->5 gw=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_uid_idx=14735 auth_info=2 chk_client_info=0 vd=0
serial=0000352e tos=ff/ff app_list=0 app=0 url_cat=0
rpidb_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 5

Exhibit.

Edit Web Filter Profile

☰ **Bandwidth Consuming** 6

| | |
|---|--|
| Freeware and Software Downloads | ✔ Allow |
| File Sharing and Storage | ✘ Block |
| 30% 93 | |

Allow users to override blocked categories

☰ **Static URL Filter**

Block invalid URLs

URL Filter

| + Create New | ✎ Edit | ✖ Delete | Search <input style="width: 80%;" type="text"/> | 🔍 |
|---|--|--|---|--|
| URL | Type | Action | Status | |
| *dropbox.com | Wildcard | ✔ Allow | ✔ Enable | |
| | | | | 1 |

Block malicious URLs discovered by FortiSandbox

Content Filter

| + Create New | ✎ Edit | ✖ Delete | | |
|---|--|--|--|---|
| Pattern Type | Pattern | Language | Action | Status |
| Wildcard | *dropbox* | Western | ⊖ Exempt | ✔ Enable |

Refer to the exhibit, which shows a partial web filter profile configuration.

Which action does FortiGate take if a user attempts to access www.dropbox.com, which is categorized as File Sharing and Storage?

- A. FortiGate allows the connection, based on the URL Filter configuration.
- B. FortiGate blocks the connection as an invalid URL.
- C. FortiGate exempts the connection, based on the Web Content Filter configuration.
- D. FortiGate blocks the connection, based on the FortiGuard category based filter configuration.

Answer: D

NEW QUESTION 6

Which two statements about conserve mode are true? (Choose two.)

- A. FortiGate enters conserve mode when the system memory reaches the configured extreme threshold.
- B. FortiGate starts taking the configured action for new sessions requiring content inspection when the system memory reaches the configured red threshold.
- C. FortiGate exits conserve mode when the system memory goes below the configured green threshold.
- D. FortiGate starts dropping all new sessions when the system memory reaches the configured red threshold.

Answer: BC

NEW QUESTION 7

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 8

Which two statements are true regarding heartbeat messages sent from an FSSO collector agent to FortiGate? (Choose two.)

- A. The heartbeat messages can be seen using the command diagnose debug authd fssolist.
- B. The heartbeat messages can be seen in the collector agent logs.
- C. The heartbeat messages can be seen on FortiGate using the real-time FSSO debug.
- D. The heartbeat messages must be manually enabled on FortiGate.

Answer: BC

NEW QUESTION 9

Refer to the exhibit.

```
# diagnose sys top
Run Time: 0 days, 0 hours and 18 minutes
OU, 0N, 1S, 95I, 0WA, 0HI, 0SI, 0ST; 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 newcli daemon continues to be in the R state, it will need to be manually restarted.

Answer: ABD

NEW QUESTION 10

Refer to the exhibit, which shows the omitted output of a session table entry.

```
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 pol_uid_idx=14720 confiauth_info=0 chk_client_info=0 vd=0
serial=0002932f tos=ff/ff app_list=2000 app=34050 url_cat=0
sdwan_mbr_seq=1 sdwan_service_id=1
rpd_b_link_id=80000000 ngfwid=n/a
npu_state=0x003c94 ips_offload
npu_info: flag=0x81/0x81, offload=8/8, ips_offload=1/1, epid=16/16, ipid=64/88, vlan=0x0000/0x0000
vlifid=64/88, vtag_in=0x0000/0x0000 in_npu=1/1, out_npu=1/1, fwd_en=0/0, qid=0/0
```

Which two statements are true? (Choose two.)

- A. The traffic has been tagged for VLAN 0000.
- B. NP7 is handling offloading of this session.
- C. The traffic matches Policy ID 1.
- D. The session has been offloaded.

Answer: BD

NEW QUESTION 10

Refer to the exhibit, which shows the output of a policy route table entry.

```
id=2113929223 static_route=7 dscp_tag=0xff 0xff flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 sport=0-0 iif=0 dport=1-65535 path(1) oif=3(port1) gwy=192.2.0.2
source wildcard(1): 0.0.0.0/0.0.0.0
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(1): Fortinet-FortiGuard(1245324,0,0,0)
hit_count=0 last_used=2022-02-23 06:39:07
```

Which type of policy route does the output show?

- A. An ISDB route
- B. A regular policy route
- C. A regular policy route, which is associated with an active static route in the FIB
- D. AnSD-WAN rule

Answer: A

NEW QUESTION 11

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 15

What are two reasons you might see iprope_in_check() check failed, drop when using the debug flow? (Choose two.)

- A. Packet was dropped because of policy route misconfiguration.
- B. Packet was dropped because of traffic shaping.
- C. Trusted host list misconfiguration.
- D. VIP or IP pool misconfiguration.

Answer: CD

NEW QUESTION 17

In IKEv2, which exchange establishes the first CHILD_SA?

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

Answer: C

NEW QUESTION 19

.....

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/>