



Fortinet

Exam Questions FCSS_NST_SE-7.6

FCSS - Network Security 7.6 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!

Exhibit.

Refer to the exhibit, which shows a partial web fillet 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 2

Exhibit.

```
config system fortiguard
  set protocol udp
  set port 8888
  set load-balance-servers1
  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-mpercent2
  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-id6 ::
  set proxv-server-ip 0.0.0.0
  set proxy-server-port 0
  set proxy-username
  set ddns-server-ip 0.0.0.0
  set dns-server-port 443
end
```

Refer to the exhibit, which shows a FortiGate configuration.

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 do to fix the issue?

- A. Disable webfilter-force-off.
- B. Increase webfilter-timeout.
- C. Enable fortiguard-anycast.
- D. Change protocol to TCP.

Answer: A

NEW QUESTION 3

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

Diagnose output

```
# 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
origin->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/if 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 happens if the primary fails and the secondary becomes the primary?

- A. The secondary device has this session synchronized; however, because application control is applied, the session is marked dirty and has to be re-evaluated after failover.
- B. 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.
- C. The session will be removed from the session table of the secondary device because of the presence of allowed error packets, which will force the client to restart the session with the server.
- D. The session state is preserved but the kernel will need to re-evaluate the session because NAT was applied.

Answer: B

NEW QUESTION 4

Refer to the exhibit, which shows the partial output of a real-time OSPF debug.

Real-time OSPF debug output

```
OSPF: RECV[Hello]: From 0.0.0.112 via port2:192.168.37.114 {192.168.37.115 -> 224.0.0.5}
OSPF: -----
OSPF: Header
OSPF:   Version 2
OSPF:   Type 1 (Hello)
OSPF:   Packet Len 48
OSPF:   Router ID 0.0.0.112
OSPF:   Area ID 0.0.0.0
OSPF:   Checksum 0x2f85
OSPF:   AuType 0
OSPF: Hello
OSPF:   NetworkMask 255.255.255.0
OSPF:   HelloInterval 10
OSPF:   Options 0x2 (*| |-|-|-|E|-)
OSPF:   RtrPriority 1
OSPF:   RtrDeadInterval 40
OSPF:   DRouter 192.168.37.114
OSPF:   BDRouter 192.168.37.115
OSPF:   # Neighbors 1
OSPF:     Neighbor 0.0.0.111
OSPF: -----
OSPF: RECV[Hello]: From 0.0.0.112 via port2:192.168.37.114: Authentication type mismatch
```

Why are the two FortiGate devices unable to form an adjacency?

- A. The Hello packet is being sent from an OSPF router with ID 0.0.0.112.
- B. The two FortiGate devices attempting adjacency are in area 0.0.0.0.
- C. One FortiGate device is configured to require authentication, while the other is not.
- D. The passwords on the FortiGate devices do not match.

Answer: C

NEW QUESTION 5

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. An SD-WAN rule

Answer: A

NEW QUESTION 6

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 7

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.

A.

Answer: CD

Explanation:

FortiTelemetry is a critical part of Security Fabric communications and requires explicit configuration for each participating FortiGate interface. The administrative access setting 'fabric' (corresponding to FortiTelemetry) must be manually enabled per interface on both upstream and downstream devices. This is performed in the GUI under Administrative Access or via the CLI using the commandset allowaccess fabricfor the relevant network interface. Without this step, FortiTelemetry communications will not occur on that interface.

Additionally, the default communication between downstream and upstream FortiGate units in the Security Fabric is over TCP port 8013. This port is well-documented as the standard for Security Fabric and FortiTelemetry connections, and must be open and permitted across the network path for connectivity and status enforcement between units. The downstream FortiGate initiates the connection to the upstream via this port unless otherwise configured. This has also been documented as a PCI-relevant port, showing its default usage.

Other options:

Neighbor Discovery in FortiOS uses IPv6 ND protocol, not TCP.

FortiTelemetry port (8013) can be modified, but the interface Administrative Access for the Security Fabric must be manually enabled; Neighbor Discovery port modification is not documented as a supported change for FortiGate.

FortiGate/FortiOS Administration Guide: Enabling FortiTelemetry (fabric) on interfaces

Fortinet Technical Tip: FortiTelemetry uses TCP port 8013 by default

PCI compliance documentation on port 8013 usage for Security Fabric

Fortinet Security Fabric setup procedures and interface options

NEW QUESTION 8

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, [1/0]
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 9

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 10

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 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_uuid_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 11

Refer to the exhibit, which shows the output of the BGP database.

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

Network          Next Hop          Metric      LocPrf  Weight  RouteTag  Path
0.0.0.0/0         100.64.2.254      0           100      0        0 ? <-/->
                  100.64.2.1        32768        0 ? <-/1>
1.2.2.1/32        100.64.2.1        32768        0 ? <-/1>
8.8.8.8/32        100.64.2.254      0           100      0        0 ? <-/1>
10.20.30.0/24     172.16.54.115     0           100      0        0 i <-/1>

Total 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 13

Refer to the exhibit, which shows the output of get router info ospf neighbor.

```
Spoke1 # get router info ospf neighbor

OSPF process 0, VRF 0:
Neighbor ID      Pri   State           Dead Time   Address      Interface
0.0.0.1          1     Full/DR          00:00:39    10.10.2.1    wan1
0.0.0.3          1     Full/DROther     00:00:37    10.10.3.2    wan2
0.0.0.10         c1    Full/-           00:00:36    172.16.1.2   ToHub
```

What can you conclude from the command output?

- A. The network type connecting the local Fortigate and OSPF neighbor 0.0.0.10 is point-to-point.
- B. All neighbors are in area 0.0.0.0.
- C. The local FortiGate is the BDR.
- D. The local FortiGate is not a DROther.

Answer: A

NEW QUESTION 18

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 21

.....

Relate Links

100% Pass Your FCSS_NST_SE-7.6 Exam with ExamBible Prep Materials

https://www.exambible.com/FCSS_NST_SE-7.6-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/>