

Latest Version: 7.0

Question: 1

Which components make up the secure SD-WAN solution?

- A. Application, antivirus, and URL, and SSL inspection
- B. Datacenter, branch offices, and public cloud
- C. FortiGate, FortiManager, FortiAnalyzer, and FortiDeploy
- D. Telephone, ISDN, and telecom network.

Answer: C

Question: 2

Refer to the exhibit.

```
config system virtual-wan-link
  set status enable
  set load-balance-mode source-ip-based
  config members
    edit 1
      set interface "port1"
      set gateway 100.64.1.254
      set source 100.64.1.1
      set cost 15
    next
    edit 2
      set interface "port2"
      set gateway 100.64.2.254
      set priority 10
    next
  end
end
```

Based on the output shown in the exhibit, which two criteria on the SD-WAN member configuration can be used to select an outgoing interface in an SD-WAN rule? (Choose two.)

- A. Set priority 10.
- B. Set cost 15.
- C. Set load-balance-mode source-ip-ip-based.

D. Set source 100.64.1.1.

Answer: D

Question: 3

What are two reasons why FortiGate would be unable to complete the zero-touch provisioning process? (Choose two.)

- A. The FortiGate cloud key has not been added to the FortiGate cloud portal.
- B. FortiDeploy has connected with FortiGate and provided the initial configuration to contact FortiManager
- C. The zero-touch provisioning process has completed internally, behind FortiGate.
- D. FortiGate has obtained a configuration from the platform template in FortiGate cloud.
- E. A factory reset performed on FortiGate.

Answer: AC

Question: 4

Which two statements describe how IPsec phase 1 main mode is different from aggressive mode when performing IKE negotiation? (Choose two)

- A. A peer ID is included in the first packet from the initiator, along with suggested security policies.
- B. XAuth is enabled as an additional level of authentication, which requires a username and password.
- C. A total of six packets are exchanged between an initiator and a responder instead of three packets.
- D. The use of Diffie Hellman keys is limited by the responder and needs initiator acceptance.

Answer: BC

Question: 5

Refer to the exhibit.

```
FortiGate # diagnose sys session list
session info: proto=1 proto_state=00 duration=25 expire=34 timeout=0 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
state=dirty may_dirty
statistic(bytes/packets/allow_err): org=84/1/1 reply=84/1/1 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
origin->sink: org pre->post, reply pre->post dev=5->4/4->5 gwy=192.168.73.2/10.0.1.10
hook=post dir-org act=snat 10.0.1.10:2246->8.8.8.8(192.168.73.132:62662)
hook=pre dir-reply act=dnat 8.8.8.8:62662->192.168.73.132:0(10.0.1.10:2246)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00000a2c tos=ff/ff app_list=0 app=0 url_cat=0
rpd_b_link_id= 80000000 rpd_b_svc_id=0 ngfwid=n/a
npu_state=0x040000
total session 1
```

Based on the exhibit, which statement about FortiGate re-evaluating traffic is true?

- A. The type of traffic defined and allowed on firewall policy ID 1 is UDP.
- B. FortiGate has terminated the session after a change on policy ID 1.
- C. Changes have been made on firewall policy ID 1 on FortiGate.
- D. Firewall policy ID 1 has source NAT disabled.

Answer: C