

## NSE7\_SDW-7.0 Dumps

### Fortinet NSE 7 - SD-WAN 7.0

[https://www.certleader.com/NSE7\\_SDW-7.0-dumps.html](https://www.certleader.com/NSE7_SDW-7.0-dumps.html)



**NEW QUESTION 1**

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: AB**

**NEW QUESTION 2**

Refer to the exhibit, which shows the IPsec phase 1 configuration of a spoke.

```
config vpn ipsec phase1-interface
  edit "T_INET_0_0"
    set interface "port1"
    set ike-version 2
    set keylife 28800
    set peertype any
    set net-device disable
    set proposal aes128-sha256 aes256-sha256 aes128gcm-prfsha256 aes256gcm-prfsha384
    chacha20poly1305-prfsha256
    set comments "[created by FMG VPN Manager]"
    set idle-timeout enable
    set idle-timeoutinterval 5
    set auto-discovery-receiver enable
    set remote-gw 100.64.1.1
    set psksecret ENC
    6D5rVsaKlMeAyVYt1z95BS24Psew761wY023hnFVviwb6deIt8c5ltCa+iNYhuJT8gycfD4+Wuszpmlv8rRzrVh
    7DFkHaW2auAAprQ0dHUfaCzjOhME7mPw+8he2xB7Edb9ku/nZEHb0cKLkKYJc/p9J9IMweV21ZUgFjvIpXNxHxpH
    LReOFShoH01SPFKz5IYCVA==
  next
end
```

What must you configure on the IPsec phase 1 configuration for ADVPN to work with SD-WAN?

- A. You must set ike-version to 1.
- B. You must enable net-device.
- C. You must enable auto-discovery-sender.
- D. You must disable idle-timeout.

**Answer: B**

**NEW QUESTION 3**

Which two conclusions for traffic that matches the traffic shaper are true? (Choose two.)

```
# diagnose firewall shaper traffic-shaper list name VoIP_Shaper
name VoIP_Shaper
maximum-bandwidth 6250 KB/sec
guaranteed-bandwidth 2500 KB/sec
current-bandwidth 93 KB/sec
priority 2
overhead 0
tos ff
packets dropped 0
bytes dropped 0
```

- A. The traffic shaper drops packets if the bandwidth is less than 2500 KBps.
- B. The measured bandwidth is less than 100 KBps.

- C. The traffic shaper drops packets if the bandwidth exceeds 6250 KBps.  
D. The traffic shaper limits the bandwidth of each source IP to a maximum of 6250 KBps.

**Answer:** BC

#### NEW QUESTION 4

Refer to the exhibit.

```
config vpn ipsec phase1-interface
  edit "T_INET_0_0"
    set type dynamic
    set interface "port1"
    set keylife 28800
    set peertype any
    set net-device disable
    set proposal aes128-sha256
    set add-route enable
    set psksecret ENC
Zv9n4Urfk0W4jj6vWI+KywxBG42DT7jWHKd8YaL8j4+pRpYOx/N7mSgc7VL0BW22HQUXWJ6zvFxNKktiPYNtA8aP
i6ly7gDx2lP/OiKexTQQJzgCGRYzLM8eFTOnK7K6AuX0bFDCpBBhEidf+03CYBMLwkFZmdU6RsT+qvybblVX+Ioy
HK5EXakpmz5RiltELgZ9Gg==
    next
  end
```

Which configuration change is required if the responder FortiGate uses a dynamic routing protocol to exchange routes over IPsec?

- A. type must be set to static.  
B. mode-cfg must be enabled.  
C. exchange-interface-ip must be enabled.  
D. add-route must be disabled.

**Answer:** D

#### Explanation:

for using "non ike" routes (for example BGP/static and so on) you must do disable the add-route that inject automatically kernel route based on p2 selectors from the remote site from the SD-WAN\_7.2\_Study\_Guide page 236

#### NEW QUESTION 5

Refer to the exhibit.

```
config vpn ipsec phase1-interface
  edit "FIRST_VPN"
    set type dynamic
    set interface "port1"
    set peertype any
    set proposal aes128-sha256 aes256-sha38
    set dhgrp 14 15 19
    set xauthtype auto
    set authusrgrp "first-group"
    set psksecret fortinet1
  next
  edit "SECOND_VPN"
    set type dynamic
    set interface "port1"
    set peertype any
    set proposal aes128-sha256 aes256-sha38
    set dhgrp 14 15 19
    set xauthtype auto
    set authusrgrp "second-group"
    set psksecret fortinet2
  next
edit
```

FortiGate has multiple dial-up VPN interfaces incoming on port1 that match only FIRST\_VPN.

Which two configuration changes must be made to both IPsec VPN interfaces to allow incoming connections to match all possible IPsec dial-up interfaces? (Choose two.)

- A. Specify a unique peer ID for each dial-up VPN interface.  
B. Use different proposals are used between the interfaces.  
C. Configure the IKE mode to be aggressive mode.  
D. Use unique Diffie Hellman groups on each VPN interface.

**Answer:** AC

#### NEW QUESTION 6

Which are two benefits of using CLI templates in FortiManager? (Choose two.)

- A. You can reference meta fields.
- B. You can configure interfaces as SD-WAN members without having to remove references first.
- C. You can configure FortiManager to sync local configuration changes made on the managed device, to the CLI template.
- D. You can configure advanced CLI settings.

**Answer:** AD

## NEW QUESTION 7

Refer to the exhibits.

Exhibit A

Exhibit B -

```
branch1_fgt # diagnose sys sdwan member | grep port
Member(1): interface: port1, flags=0x0 , gateway: 192.2.0.2, priority: 0 1024, weight: 0
Member(2): interface: port2, flags=0x0 , gateway: 192.2.0.10, priority: 0 1024, weight: 0

branch1_fgt # get router info routing-table all | grep port
S* 0.0.0.0/0 [1/0] via 192.2.0.2, port1
   [1/0] via 192.2.0.10, port2
S 8.8.8.8/32 [10/0] via 192.2.0.11, port2
C 10.0.1.0/24 is directly connected, port5
S 172.16.0.0/16 [10/0] via 172.16.0.2, port4
C 172.16.0.0/29 is directly connected, port4
C 192.2.0.0/29 is directly connected, port1
C 192.2.0.8/29 is directly connected, port2
C 192.168.0.0/24 is directly connected, port10

branch1_fgt # diagnose sys sdwan health-check status Level3_DNS
Health Check(Level3_DNS):
Seq(1 port1): state(alive), packet-loss(0.000%) latency(1.919), jitter(0.137), bandwidth-
up(10238), bandwidth-dw(10238), bandwidth-bi(20476) sla_map=0x0
Seq(2 port2): state(alive), packet-loss(0.000%) latency(1.509), jitter(0.101), bandwidth-
up(10238), bandwidth-dw(10238), bandwidth-bi(20476) sla_map=0x0
```

Exhibit A shows the SD-WAN performance SLA and exhibit B shows the SD-WAN member status, the routing table, and the performance SLA status. If port2 is detected dead by FortiGate, what is the expected behavior?

- A. Port2 becomes alive after three successful probes are detected.
- B. FortiGate removes all static routes for port2.
- C. The administrator manually restores the static routes for port2, if port2 becomes alive.
- D. Host 8.8.8.8 is reachable through port1 and port2.

**Answer:** B

### Explanation:

This is due to Update static route is enable which removes the static route entry referencing the interface if the interface is dead



### NEW QUESTION 8

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

### NEW QUESTION 9

Refer to the exhibit.

```
config system settings
    set firewall-session-dirty check-new
end
```

Based on the exhibit, which two actions does FortiGate perform on sessions after a firewall policy change? (Choose two.)

- A. FortiGate flushes all sessions.
- B. FortiGate terminates the old sessions.
- C. FortiGate does not change existing sessions.
- D. FortiGate evaluates new sessions.

**Answer:** CD

#### Explanation:

FortiGate not to flag existing impacted session as dirty by setting firewall-session-dirty to check new. The results is that FortiGate evaluates only new session against the new firewall policy.

### NEW QUESTION 10

Refer to the exhibits.

Exhibit A

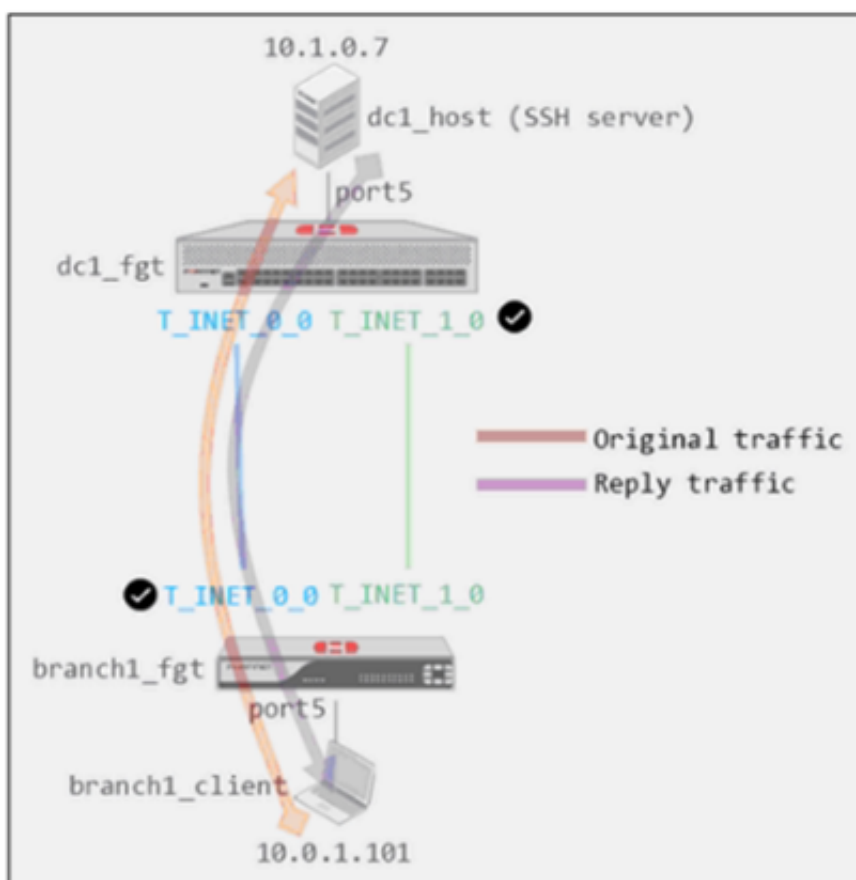


Exhibit B

```
dc1_fgt # show system global
config system global
    set admin-https-redirect disable
    set admintimeout 480
    set alias "FortiGate-VM64"
    set hostname "dc1_fgt"
    set timezone 04
end

dc1_fgt # show system settings
config system settings
    set tcp-session-without-syn enable
    set allow-subnet-overlap enable
    set gui-allow-unnamed-policy enable
    set gui-multiple-interface-policy enable
end
```

Exhibit A shows a site-to-site topology between two FortiGate devices: branch1\_fgt and dc1\_fgt. Exhibit B shows the system global and system settings configuration on dc1\_fgt.

When branch1\_client establishes a connection to dc1\_host, the administrator observes that, on dc1\_fgt, the reply traffic is routed over T\_INET\_0\_0, even though

T\_INET\_1\_0 is the preferred member in the matching SD-WAN rule.

Based on the information shown in the exhibits, what configuration change must be made on dc1\_fgt so dc1\_fgt routes the reply traffic over T\_INET\_1\_0?

- A. Enable auxiliary-session under config system settings.
- B. Disable tp-session-without-syn under config system settings.
- C. Enable snat-route-change under config system global.
- D. Disable allow-subnet-overlap under config system settings.

**Answer: A**

**Explanation:**

Controlling return path with auxiliary session When multiple incoming or outgoing interfaces are used in ECMP or for load balancing, changes to routing, incoming, or return traffic interfaces impacts how an existing sessions handles the traffic. Auxiliary sessions can be used to handle these changes to traffic patterns.<https://docs.fortinet.com/document/fortigate/7.0.11/administration-guide/14295/controlling-return-path>

**NEW QUESTION 10**

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**

**NEW QUESTION 15**

Refer to the exhibit.

```
branch1_fgt # diagnose sys sdwan service 1

Service(3): Address Mode(IPV4) flags=0x200 use-shortcut-sla
Gen(6), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(manual)
Members(2):
  1: Seq_num(3 T_INET_0_0), alive, selected
  2: Seq_num(4 T_INET_1_0), alive, selected
Src address(1):
  10.0.1.0-10.0.1.255

Dst address(1):
  10.0.0.0-10.255.255.255

branch1_fgt # diagnose sys sdwan member | grep T_INET_
Member(3): interface: T_INET_0_0, flags=0x4 , gateway: 100.64.1.1, priority: 10 1024,
weight: 0
Member(4): interface: T_INET_1_0, flags=0x4 , gateway: 100.64.1.9, priority: 0 1024,
weight: 0

branch1_fgt # get router info routing-table all | grep T_INET_
S      10.0.0.0/8 [1/0] via T_INET_1_0 tunnel 100.64.1.9
```

An administrator is troubleshooting SD-WAN on FortiGate. A device behind branch1\_fgt generates traffic to the 10.0.0.0/8 network. The administrator expects the traffic to match SD-WAN rule ID 1 and be routed over T\_INET\_0\_0. However, the traffic is routed over T\_INET\_1\_0.

Based on the output shown in the exhibit, which two reasons can cause the observed behavior? (Choose two.)

- A. The traffic matches a regular policy route configured with T\_INET\_1\_0 as the outgoing device.
- B. T\_INET\_1\_0 has a lower route priority value (higher priority) than T\_INET\_0\_0.
- C. T\_INET\_0\_0 does not have a valid route to the destination.
- D. T\_INET\_1\_0 has a higher member configuration priority than T\_INET\_0\_0.

**Answer: AC**

**NEW QUESTION 16**

In the default SD-WAN minimum configuration, which two statements are correct when traffic matches the default implicit SD-WAN rule? (Choose two )

- A. Traffic has matched none of the FortiGate policy routes.
- B. Matched traffic failed RPF and was caught by the rule.
- C. The FIB lookup resolved interface was the SD-WAN interface.
- D. An absolute SD-WAN rule was defined and matched traffic.

**Answer: AC**

**NEW QUESTION 20**

.....

## Thank You for Trying Our Product

\* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

\* One year free update

You can enjoy free update one year. 24x7 online support.

\* Trusted by Millions

We currently serve more than 30,000,000 customers.

\* Shop Securely

All transactions are protected by VeriSign!

**100% Pass Your NSE7\_SDW-7.0 Exam with Our Prep Materials Via below:**

[https://www.certleader.com/NSE7\\_SDW-7.0-dumps.html](https://www.certleader.com/NSE7_SDW-7.0-dumps.html)