

# Fortinet

## Exam Questions NSE7\_SDW-7.0

Fortinet NSE 7 - SD-WAN 7.0



**NEW QUESTION 1**

Which two statements are correct when traffic matches the implicit SD-WAN rule? (Choose two.)

- A. The `sdwan_service_id` flag in the session information is 0.
- B. All SD-WAN rules have the default setting enabled.
- C. Traffic does not match any of the entries in the policy route table.
- D. Traffic is load balanced using the algorithm set for the `v4-ecmp-mode` setting.

**Answer: AC**

**NEW QUESTION 2**

Exhibit A –

The screenshot shows the FortiGate configuration page for system interfaces and static routes. The system interface table lists 17 interfaces, including physical ports (port1-port10), an aggregate interface (fortilink), tunnel interfaces (raf.root, l2t.root, ssl.root), an EMAC VLAN (vl\_lan\_bs), and SD-WAN zones (virtual-wan-link, SASE). The static route table shows two routes: route 1 with destination 0.0.0.0/0.0.0.0 and gateway 203.0.113.2 on port1, and route 2 with destination 0.0.0.0/0.0.0.0 and gateway 203.0.113.10 on port2. Both routes are enabled.

#	Name	Type	Normalized Interface	Addressing Mode	IP/Netmask	Access
<b>Physical (10)</b>						
1	port1	Physical	port1	Manual	203.0.113.1/255.255.255.2	PING
2	port2	Physical	port2	Manual	203.0.113.9/255.255.255.2	PING
3	port3	Physical	port3	Manual	0.0.0.0/0.0.0.0	
4	port4	Physical	port4	Manual	172.16.0.9/255.255.255.24	PING
5	port5	Physical	port5	Manual	10.0.2.254/255.255.255.0	PING
6	port6	Physical	port6	Manual	0.0.0.0/0.0.0.0	
7	port7	Physical	port7	Manual	0.0.0.0/0.0.0.0	
8	port8	Physical	port8	Manual	0.0.0.0/0.0.0.0	
9	port9	Physical	port9	Manual	0.0.0.0/0.0.0.0	
10	port10	Physical	port10	Manual	192.168.0.32/255.255.255.	HTTPS, PING, SSH, HT
<b>Aggregate (1)</b>						
11	fortilink	Aggregate		Manual	169.254.1.1/255.255.255.0	PING, Security Fabric C
<b>Tunnel (3)</b>						
12	raf.root	Tunnel		Manual	0.0.0.0/0.0.0.0	
13	l2t.root	Tunnel		Manual	0.0.0.0/0.0.0.0	
14	ssl.root (SSL VPN interf	Tunnel		Manual	0.0.0.0/0.0.0.0	
<b>EMAC VLAN (1)</b>						
15	vl_lan_bs	EMAC VLAN		Manual	10.0.102.1/255.255.255.0	PING
<b>SD-WAN Zone (2)</b>						
16	virtual-wan-link	SD-WAN Zone				
17	SASE	SD-WAN Zone	SASE			

#	ID	Destination	Gateway	Interface	Distance	Priority	Status	Description
<b>Static Route (2)</b>								
1	1	0.0.0.0/0.0.0.0	203.0.113.2	port1	10	0	Enable	
2	2	0.0.0.0/0.0.0.0	203.0.113.10	port2	10	0	Enable	

Exhibit B –

The screenshot shows the FortiGate configuration page for firewall policies. It displays two policies: 'Internet\_Access' and 'Implicit Deny'. The 'Implicit Deny' policy is highlighted as the implicit policy for the SD-WAN zone.

#	Name	From	To	Source	Destination	Schedule	Service
1	Internet_Access	port5	port1	all	all	always	ALL
<b>Implicit (2-2 / Total: 1)</b>							
2	Implicit Deny	any	any	all	all	always	ALL

Exhibit A shows the system interface with the static routes and exhibit B shows the firewall policies on the managed FortiGate. Based on the FortiGate configuration shown in the exhibits, what issue might you encounter when creating an SD-WAN zone for port1 and port2?

- A. port1 is assigned a manual IP address.
- B. port1 is referenced in a firewall policy.
- C. port2 is referenced in a static route.
- D. port1 and port2 are not administratively down.

**Answer: B**

**NEW QUESTION 3**

Refer to the exhibit.

```

config system sdwan
  set status enable
  set load-balance source-dest-ip-based
  config zone
    edit "virtual-wan-link"
    next
    edit "SASE"
    next
    edit "underlay"
    next
  end
  config members
    edit 1
      set interface "port1"
      set zone "underlay"
      set gateway 192.2.0.2
    next
    edit 2
      set interface "port2"
      set zone "underlay"
      set gateway 192.2.0.10
    next
  end
  ...
end

```

Which algorithm does SD-WAN use to distribute traffic that does not match any of the SD-WAN rules?

- A. All traffic from a source IP to a destination IP is sent to the same interface.
- B. All traffic from a source IP is sent to the same interface.
- C. All traffic from a source IP is sent to the most used interface.
- D. All traffic from a source IP to a destination IP is sent to the least used interface.

**Answer: A**

**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
Zv9n4Urfk0W4jj8vWI+KywxBG42DT7jWHKd8YaL8j4+pRpYOx/N7mSgc7VL0BW22HQUXWJ6zvFxnKktiPYntA8aP
i6ly7gDx2lP/OfKexTQQJzgCGRYzLM8eFTOnK7R6AuX0bFDCpBBhEIdf+03CYBMLwkF2mdU6RsT+qvybbiVX+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.

```
branch1_fgt # diagnose sys sdwan service 3

Service(3): Address Mode(IPV4) flags=0x200 use-shortcut-sla
Gen(5), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(priority), link-cost-
factor(latency), link-cost-threshold(10), health-check(VPN_PING)
Members(3):
  1: Seq_num(3 T_INET_0_0), alive, latency: 101.349, selected
  2: Seq_num(4 T_INET_1_0), alive, latency: 151.278, selected
  3: Seq_num(5 T_MPLS_0), alive, latency: 200.984, 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 (3) # show
config service
edit 3
  set name "Corp"
  set mode priority
  set dst "Corp-net"
  set src "LAN-net"
  set health-check "VPN_PING"
  set priority-members 3 4 5
next
end
```

The exhibit shows the SD-WAN rule status and configuration.

Based on the exhibit, which change in the measured latency will make T\_MPLS\_0 the new preferred member?

- A. When T\_INET\_0\_0 and T\_MPLS\_0 have the same latency.
- B. When T\_MPLS\_0 has a latency of 100 ms.
- C. When T\_INET\_0\_0 has a latency of 250 ms.
- D. When T\_MPLS\_0 has a latency of 80 ms.

**Answer: D**

**NEW QUESTION 6**

Which two performance SLA protocols enable you to verify that the server response contains a specific value? (Choose two.)

- A. http
- B. icmp
- C. twamp
- D. dns

**Answer: AD**

**NEW QUESTION 7**

What are two reasons for using FortiManager to organize and manage the network for a group of FortiGate devices? (Choose two )

- A. It simplifies the deployment and administration of SD-WAN on managed FortiGate devices.
- B. It improves SD-WAN performance on the managed FortiGate devices.
- C. It sends probe signals as health checks to the beacon servers on behalf of FortiGate.
- D. It acts as a policy compliance entity to review all managed FortiGate devices.
- E. It reduces WAN usage on FortiGate devices by acting as a local FortiGuard server.

**Answer: AE**

**NEW QUESTION 8**

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 9**

Refer to the exhibits.  
 Exhibit A

**Edit Traffic Shaping Policy**

IP Version: IPv4 IPv6

Name: Limit\_YouTube

Status: Enable Disable

Comments: 0/255

**If Traffic Matches:**

Source Internet Service:

Source Address: LAN-net

Source User: +

Source User Group: +

Destination Internet Service:

Destination Address: all

Schedule: +

Service: ALL

Application: YouTube

Application Category: +

Application Group: +

URL Category: +

Type Of Service: 0x00

Type Of Service Mask: 0x00

**Then:**

Action: Apply Shaper Assign Group

Outgoing Interface: underlay

Shared Shaper: low-priority

Reverse Shaper: low-priority

Per-IP Shaper: +

Differentiated Services:

Differentiated Services Reverse:

Exhibit B

**Edit Firewall Policy**

ID: 1

Name: DIA

ZTNA: Disable Full ZTNA IP/MAC filtering

Incoming Interface: LAN

Outgoing Interface: underlay

Source Internet Service:

IPv4 Source Address: LAN-net

IPv6 Source Address: +

Source User: +

Source User Group: +

FSSO Groups: +

Destination Internet Service:

IPv4 Destination Address: all

IPv6 Destination Address: +

Service: ALL

Schedule: always

Action: Deny Accept IPSEC

Inspection Mode: Flow-based Proxy-based

**Firewall/Network Options**

NAT:  NAT NAT46 NAT64

IP Pool Configuration: Use Outgoing Interface Address Use Dynamic IP Pool

Preserve Source Port:

Protocol Options: default

**Disclaimer Options**

Display Disclaimer:

**Security Profiles**

SSL/SSH Inspection: deep-inspection

Decrypted Traffic Mirror: +

**Traffic Shaping Options**

Shared Shaper: +

Reverse Shaper: +

Per-IP Shaper: +

**Logging Options**

Log Allowed Traffic: No Log Log Security Events Log All Sessions

Capture Packets

Generate Logs when Session Starts

Exhibit A shows the traffic shaping policy and exhibit B shows the firewall policy.

The administrator wants FortiGate to limit the bandwidth used by YouTube. When testing, the administrator determines that FortiGate does not apply traffic shaping on YouTube traffic.

Based on the policies shown in the exhibits, what configuration change must be made so FortiGate performs traffic shaping on YouTube traffic?

- A. Destination internet service must be enabled on the traffic shaping policy.
- B. Application control must be enabled on the firewall policy.
- C. Web filtering must be enabled on the firewall policy.
- D. Individual SD-WAN members must be selected as the outgoing interface on the traffic shaping policy.

**Answer: B**

**NEW QUESTION 10**

Refer to the exhibits.

Exhibit A

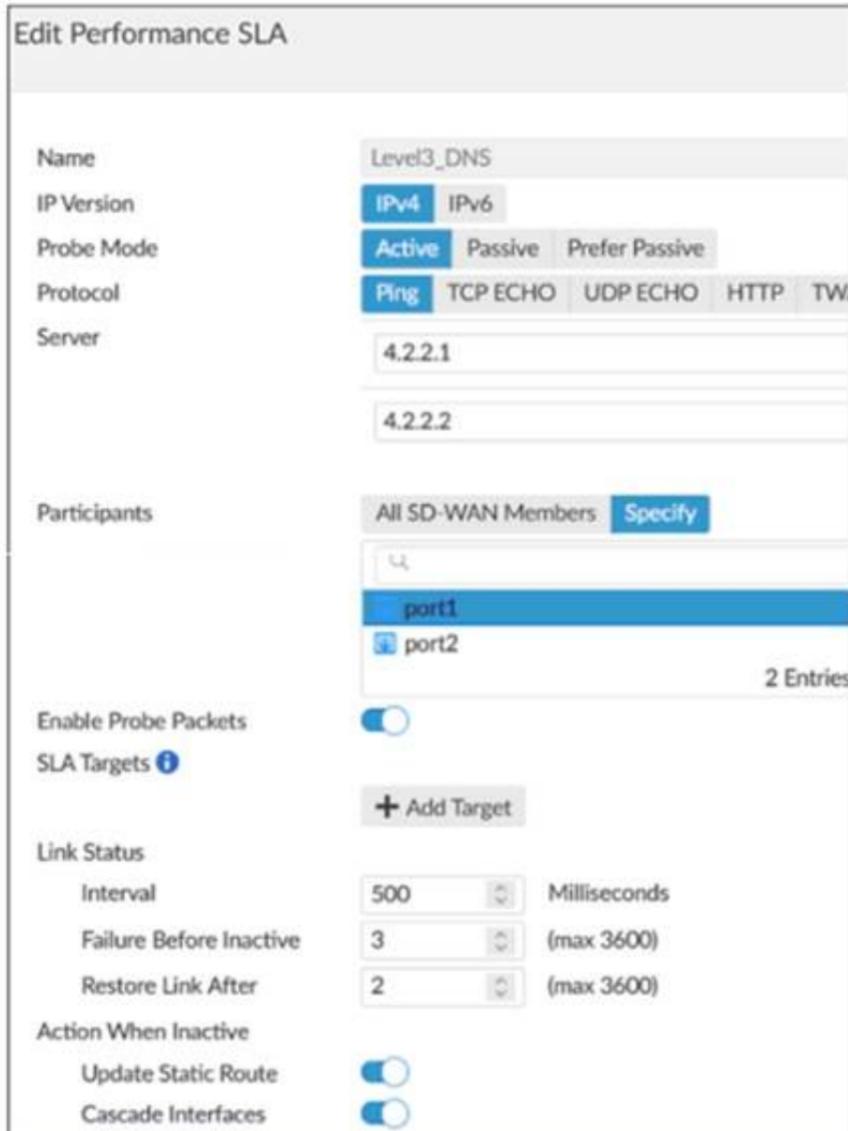


Exhibit B -

```
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 10**

Which two settings can you configure to speed up routing convergence in BGP? (Choose two.)

- A. update-source
- B. set-route-tag
- C. holdtime-timer
- D. link-down-failover

**Answer: CD**

**NEW QUESTION 11**

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 16**

Refer to the exhibits.

Exhibit A

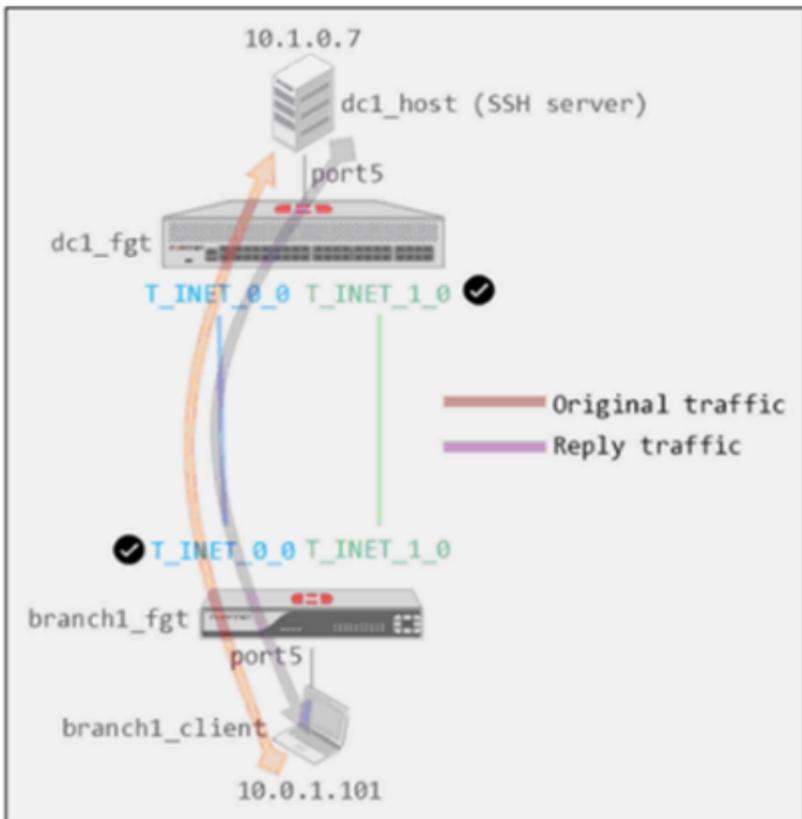


Exhibit B

```
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 19**

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 23**

.....

## **Thank You for Trying Our Product**

### **We offer two products:**

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### **NSE7\_SDW-7.0 Practice Exam Features:**

- \* NSE7\_SDW-7.0 Questions and Answers Updated Frequently
- \* NSE7\_SDW-7.0 Practice Questions Verified by Expert Senior Certified Staff
- \* NSE7\_SDW-7.0 Most Realistic Questions that Guarantee you a Pass on Your First Try
- \* NSE7\_SDW-7.0 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The NSE7\\_SDW-7.0 Practice Test Here](#)**