Fortinet

Exam Questions NSE7_SDW-7.2

Fortinet NSE 7 - SD-WAN 7.2

NEW QUESTION 1
Refer to the exhibit.

```
branch1_fgt # diagnose firewall proute list
list route policy info(vf=root):

id=1 dscp_tag=0xff 0xff flags=0x0 tos=0x00 tos_mask=0x00 protocol=17 sport=0-65535 iif=7
dport=53 path(1) oif=3(port1)
source wildcard(1): 0.0.0.0/0.0.0.0
destination wildcard(1): 4.2.2.1/255.255.255.255
hit_count=0 last_used=2022-03-25 10:53:26

id=2131165185(0x7f070001) vwl_service=1(Critical-DIA) vwl_mbr_seq=1 2 dscp_tag=0xff 0xff
flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 sport=0-65535 iif=0 dport=1-65535 path(2)
oif=3(port1) oif=4(port2)
source(1): 10.0.1.0-10.0.1.255
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(3): GoToMeeting(4294836966,0,0,0, 16354)
Microsoft.Office.365.Portal(4294837474,0,0,0, 41468) Salesforce(4294837976,0,0,0, 16920)
hit_count=0 last_used=2022-03-24 12:18:16

id=2131165186(0x7f070002) vwl_service=2(Non-Critical-DIA) vwl_mbr_seq=2 dscp_tag=0xff
0xff flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 sport=0-65535 iif=0 dport=1-65535
path(1) oif=4(port2)
source(1): 10.0.1.0-10.0.1.255
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(2): Facebook(4294836806,0,0,0, 15832) Twitter(4294838278,0,0,0, 16001)
hit_count=0 last_used=2022-03-24 12:18:16

id=2131165187(0x7f070003) vwl_service=3(all_rules) vwl_mbr_seq=1 dscp_tag=0xff 0xff
flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 sport=0-65535 iif=0 dport=1-65535 path(1)
oif=3(port1)
source(1): 0.0.0.0-255.255.255.255
destination(1): 0.0.0.0-255.255.255.255
hit_count=0 last_used=2022-03-25 10:58:12
```

Based on the output, which two conclusions are true? (Choose two.)

A. There is more than one SD-WAN rule configured.
B. The SD-WAN rules take precedence over regular policy routes.
C. The all_rules rule represents the implicit SD-WAN rule.
D. Entry 1(id=1) is a regular policy route.

Answer: AD

NEW QUESTION 2
Which diagnostic command can you use to show the SD-WAN rules, interface information, and state?

A. diagnose sys sdwan service
B. diagnose sys sdwan route-tag-list
C. diagnose sys sdwan member
D. diagnose sys sdwan neighbor

Answer: A

NEW QUESTION 3
Refer to the exhibits.
Exhibit A

```
config system global
    set snat-route-change enable
end
```

Exhibit B

```
branch1_fgt # get router info routing-table all
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
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [1/0] via 192.2.0.2, port2, [1/0]
                  [1/0] via 192.2.0.10, port1 [10/0]
...
```

Exhibit A shows the source NAT (SNAT) global setting and exhibit B shows the routing table on FortiGate.
Based on the exhibits, which two actions does FortiGate perform on existing sessions established over port2, if the administrator increases the static route priority on port2 to 20? (Choose two.)

A. FortiGate flags the sessions as dirty.
B. FortiGate continues routing the sessions with no SNAT, over port2.
C. FortiGate performs a route lookup for the original traffic only.
D. FortiGate updates the gateway information of the sessions with SNAT so that they use port1 instead of port2.

Answer: BD

NEW QUESTION 4
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 5
Refer to the exhibit.
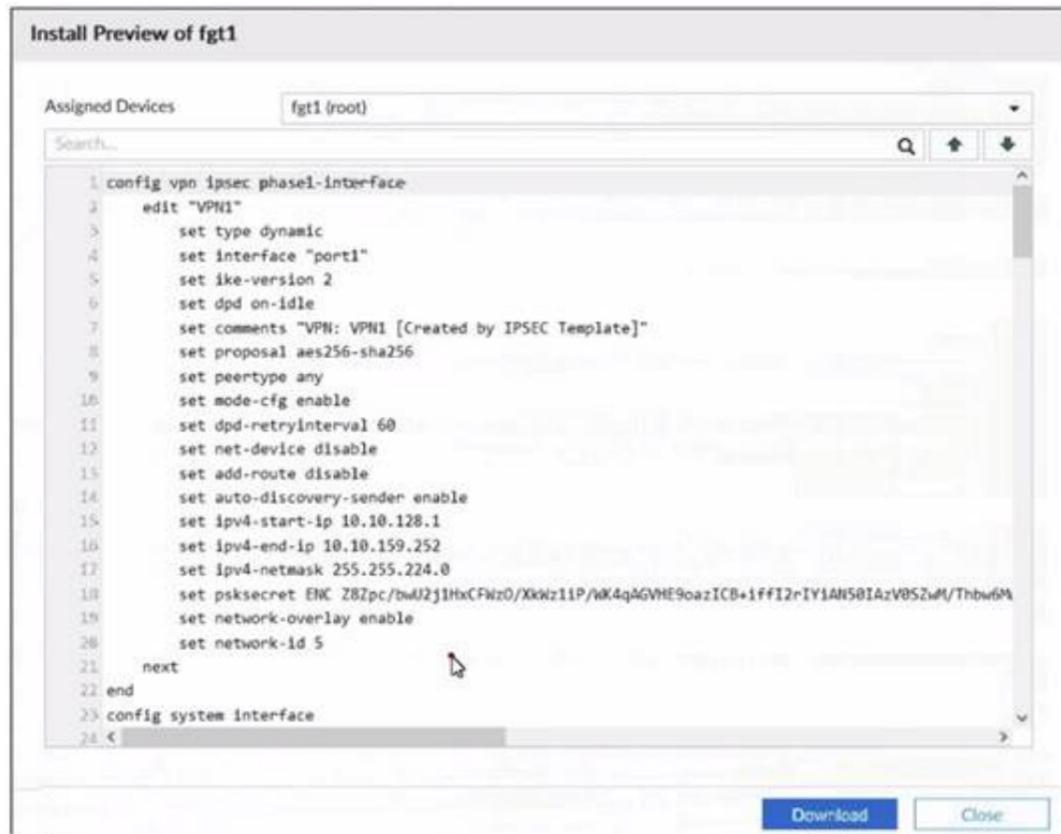
An administrator used the SD-WAN overlay template to prepare an IPsec configuration for a hub-and-spoke SD-WAN topology. The exhibit shows the installation preview for one FortiGate device. In the exhibit, which statement best describes the configuration applied to the FortiGate device?

A. It is a hub devic
B. It can send ADVPN shortcut offers.
C. It is a spoke device that establishes dynamic IPsec tunnels to the hu
D. The subnet range is 10.10.128.0/23.
E. It is a spoke device that establishes dynamic IPsec tunnels to the hu
F. It can send ADVPN shortcut requests.
G. It is a hub device and will automatically discover the spoke devices that are in the SD- WAN topology.

Answer: C

Explanation:
According to the SD-WAN 7.2 Study Guide, the SD-WAN overlay template simplifies the configuration of IPsec tunnels in a hub-and-spoke topology. The template defines the following parameters:
? type: dynamic for spokes, static for hubs
? interface: the WAN interface to use for the IPsec tunnel
? network-overlay: enable for spokes, disable for hubs
? network-id: a unique identifier for each spoke
? auto-discovery-sender: enable for hubs, disable for spokes
? auto-discovery-receiver: enable for spokes, disable for hubs Based on the exhibit, the FortiGate device has the following configuration:
? type: dynamic
? interface: port1
? network-overlay: enable
? network-id: 5
? auto-discovery-sender: disable
? auto-discovery-receiver: enable
Therefore, the FortiGate device is a spoke that establishes dynamic IPsec tunnels to the hub. It also has the network-overlay and auto-discovery-receiver options enabled, which means it can send ADVPN shortcut requests to other spokes when it receives a shortcut offer from the hub

NEW QUESTION 6
Refer to the Exhibits:

Exhibit A	Exhibit B

Link Status

Check interval	500	ms
Failures before inactive ⓘ	3	
Restore link after ⓘ	2	check(s)

Actions when Inactive

Update static route ⓘ 🔵

Exhibit A	Exhibit B

```
NGFW-1 # diagnose sys sdwan health-check
Health Check (Ping):
Seq (1 port1): state (alive), packet-loss (0.000%) latency
(6.196), jitter (0.079) sla_map=0x0
Seq (2 port2): state (dead), packet-loss (6.000%) sla_map=0x0
```

Exhibit A, which shows the SD-WAN performance SLA and exhibit B shows the health of the participating SD-WAN members.
Based on the exhibits, which statement is correct?

A. The dead member interface stays unavailable until an administrator manually brings the interface back.
B. Port2 needs to wait 500 milliseconds to change the status from alive to dead.
C. Static routes using port2 are active in the routing table.
D. FortiGate has not received three consecutive requests from the SLA server configured for port2.

Answer: C

NEW QUESTION 7
Refer to the exhibit.

Exhibit A

```
fgt # show vpn ipsec phase1-interface T_INET_1
config vpn ipsec phase1-interface
        edit "T_INET_1"
            set type dynamic
            set interface "port2"
            set ike-version 2
            set keylife 28800
            set peertype any
            set net-device disable
            set proposal aes128-sha256
            set add-route disable
            set auto-discovery-sender enable
            set psksecret ENC MXtFGKOxLV+x4p3e9Xq2HGJoU+QOgg5YMqiXb2T73fZpSXS/
            jv9oshNeQ1NEjOJEtuqqD8mAw7G2ZLT1sR3/ihAaAY4tvjveS+9CuTnO0J2tuddoM9
            uz4vaBTNbNrh3/KhbJytsCag==
        next
    end
```

Exhibit B

```
fgt # diag vpn tunnel list name T_INET_1_0
list ipsec tunnel by names in vd 0
--------------------------------------------------------
name=T_INET_1_0 ver=2 serial=a 100.64.1.9:0->192.2.0.9:0 tun_id=192.2.0.9 tun_id6=::10.0.0.10
dst_mtu=0 dpd-link=on weight=1
bound_if=4 lgwy=static/1 tun=intf mode=dial_inst/3 encap=none/74408 options[122a8]=npu rgwy-chg
frag-rfc run_state=0 role=primary acc
ept_traffic=1 overlay_id=0
parent=T_INET_1 index=0
proxyid_num=1 child_num=0 refcnt=6 ilast=0 olast=42955943 ad=/0
stat: rxp=32 txp=0 rxb=1280 txb=0
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
fec: egress=0 ingress=0
proxyid=T_INET_1_0 proto=0 sa=1 ref=2 serial=1
src: 0:0.0.0.0-255.255.255.255:0
dst: 0:10.0.1.0-10.0.1.255:0
SA: ref=3 options=20603 type=00 soft=0 mtu=1280 expire=1774/0B replaywin=2048
seqno=1 esn=0 replaywin_lastseq=00000021 qat=0 rekey=0 hash_search_len=1
life: type=01 bytes=0/0 timeout=1791/1800
dec: spi=7c176e24 esp=aes key=16 8547efb42d148c6692fb2af0d01ff12d
ah=sha1 key=20 f0d3ac8192d2e79fbbe29162f9ccf406f1a161b5
enc: spi=809f9d49 esp=aes key=16 cb67f6d5f6a1f9fe5ab38b953dd4782f
ah=sha1 key=20 d0182dfe827a4785d9493d46e3907d49465391fb
dec:pkts/bytes=64/2560, enc:pkts/bytes=0/0
npu_flag=00 npu_rgwy=192.2.0.9 npu_lgwy=100.64.1.9 npu_selid=6 dec_npuid=0 enc_npuid=0
```

Which two statements about the IPsec VPN configuration and the status of the IPsec VPN tunnel are true? (Choose two.)

A. FortiGate does not install IPsec static routes for remote protected networks in the routing tabl
B. Most Voted
C. The phase 1 configuration supports the network-overlay settin
D. Most Voted
E. FortiGate facilitated the negotiation of the T_INET_1_0_0 ADVPN shortcut over T_INET_1_0.
F. Dead peer detection is disabled.

Answer: AC

NEW QUESTION 8

Refer to the exhibit.

```
config system interface
    edit "port2"
        set vdom "root"
        set ip 192.2.0.9 255.255.255.248
        set allowaccess ping
        set type physical
        set role wan
        set snmp-index 2
        set preserve-session-route enable
    next
end
```

Based on the exhibit, which two actions does FortiGate perform on traffic passing through port2? (Choose two.)

A. FortiGate does not change the routing information on existing sessions that use a valid gateway, after a route change.
B. FortiGate performs routing lookups for new sessions only, after a route change.
C. FortiGate always blocks all traffic, after a route change.
D. FortiGate flushes all routing information from the session table, after a route change.

Answer: AB

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

```
config duplication
    edit 1
        set srcaddr "10.0.1.0/24"
        set dstaddr "10.1.0.0/24"
        set srcintf "port5"
        set dstintf "overlay"
        set service "ALL"
        set packet-duplication force
    next
end
```

```
branch1_fgt # diagnose sys sdwan zone
Zone SASE index=2
        members(0):
Zone overlay index=4
        members(3): 19(T_INET_0_0) 20(T_INET_1_0) 21(T_MPLS_0)
Zone underlay index=3
        members(2): 3(port1) 4(port2)
Zone virtual-wan-link index=1
        members(0):
```

```
1.274665 port5 in 10.0.1.101 -> 10.1.0.7: icmp: echo request
1.275788 T_INET_0_0 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
1.275790 T_INET_1_0 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
1.275801 T_MPLS_0 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
1.278365 T_INET_1_0 in 10.1.0.7 -> 10.0.1.101: icmp: echo reply
1.278553 port5 out 10.1.0.7 -> 10.0.1.101: icmp: echo reply
```

Exhibit B

```
3.874431 T_INET_1_0 in 10.0.1.101 -> 10.1.0.7: icmp: echo request
3.874630 port5 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
3.874895 T_INET_0_0 in 10.0.1.101 -> 10.1.0.7: icmp: echo request
3.875125 T_MPLS_0 in 10.0.1.101 -> 10.1.0.7: icmp: echo request
3.875054 port5 in 10.1.0.7 -> 10.0.1.101: icmp: echo reply
3.875308 T_INET_1_0 out 10.1.0.7 -> 10.0.1.101: icmp: echo reply
```

Exhibit A shows the packet duplication rule configuration, the SD-WAN zone status output, and the sniffer output on FortiGate acting as the sender. Exhibit B shows the sniffer output on a FortiGate acting as the receiver.
The administrator configured packet duplication on both FortiGate devices. The sniffer output on the sender FortiGate shows that FortiGate forwards an ICMP echo request packet over three overlays, but it only receives one reply packet through T_INET_1_0.
Based on the output shown in the exhibits, which two reasons can cause the observed behavior? (Choose two.)

A. On the receiver FortiGate, packet-de-duplication is enabled.
B. The ICMP echo request packets sent over T_INET_0_0 and T_MPLS_0 were dropped along the way.
C. The ICMP echo request packets received over T_INET_0_0 and T_MPLS_0 were offloaded to NPU.
D. On the sender FortiGate, duplication-max-num is set to 3.

Answer: AD

NEW QUESTION 10
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

Explanation:
 Performance SLA (Service Level Agreement) protocols are used in SD-WAN to monitor the quality and performance of various network services. The two protocols that specifically allow for verifying a specific value in the server response are:
? HTTP (Hypertext Transfer Protocol): HTTP is the foundation of data communication on the World Wide Web. It allows for fetching resources, such as HTML documents. You can configure an HTTP performance SLA to send specific requests (e.g., GET or POST) and then check if the response body contains a particular string or value. This is useful for validating web server functionality and content delivery.
? DNS (Domain Name System): DNS is responsible for translating domain names into IP addresses. A DNS performance SLA can be set up to query a specific domain and verify that the returned IP address or other DNS record values match what is expected. This helps ensure proper name resolution and accessibility of resources.

NEW QUESTION 15
Which two statements about SLA targets and SD-WAN rules are true? (Choose two.)

A. When configuring an SD-WAN rule, you can select multiple SLA targets of the same performance SLA.
B. SD-WAN rules use SLA targets to check if the preferred members meet the SLA requirements.
C. SLA targets are used only by SD-WAN rules that are configured with Lowest Cost (SLA) or Maximize Bandwidth (SLA) as strategy.
D. Member metrics are measured only if an SLA target is configured.

Answer: BD

NEW QUESTION 18
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 20
What are two common use cases for remote internet access (RIA)? (Choose two.)

A. Provide direct internet access on spokes
B. Provide internet access through the hub
C. Centralize security inspection on the hub
D. Provide thorough inspection on spokes

Answer: BC

Explanation:
* B. Provide internet access through the hub: This involves routing branch or remote office internet traffic through a central hub, ensuring consistent security policies and possibly better management of network resources.
* C. Centralize security inspection on the hub: With this approach, all internet-bound traffic from various spokes is inspected at the hub, leveraging centralized security mechanisms for thorough inspection and policy enforcement.

NEW QUESTION 21
Exhibit.

```
7: […]logid="0101037141" type="event" subtype="vpn" level="notice" vd="root" logdesc="IPsec tunnel
statistics" msg="IPsec tunnel statistics" action="tunnel-stats" remip=100.64.1.9 locip=192.2.0.9
remport=500 locport=500 outintf="port2" cookies="773c72b48060051d/529ac435532959b6" user="N/A"
group="N/A" useralt="N/A" xauthuser="N/A" xauthgroup="N/A" assignip=10.202.1.1
vpntunnel="T_INET_1" tunnelip=N/A tunnelid=2595348112 tunneltype="ipsec" duration=3581
sentbyte=386431 rcvdbyte=387326 nextstat=600 advpnsc=0

8: […]logid="0101037141" type="event" subtype="vpn" level="notice" vd="root" logdesc="IPsec tunnel
statistics" msg="IPsec tunnel statistics" action="tunnel-stats" remip=172.16.0.9 locip=172.16.0.1
remport=500 locport=500 outintf="port4" cookies="0624890597f0096d/ed1bd5247375c46f" user="N/A"
group="N/A" useralt="N/A" xauthuser="N/A" xauthgroup="N/A" assignip=N/A vpntunnel="T_MPLS_0"
tunnelip=0.0.0.0 tunnelid=2595348102 tunneltype="ipsec" duration=223 sentbyte=115040
rcvdbyte=345160 nextstat=600 advpnsc=1

9: […]logid="0101037141" type="event" subtype="vpn" level="notice" vd="root" logdesc="IPsec tunnel
statistics" msg="IPsec tunnel statistics" action="tunnel-stats" remip=100.64.1.1 locip=192.2.0.1
remport=500 locport=500 outintf="port1" cookies="747b432459497188/6616a969a6937853" user="N/A"
group="N/A" useralt="N/A" xauthuser="N/A" xauthgroup="N/A" assignip=10.201.1.1
vpntunnel="T_INET_0" tunnelip=N/A tunnelid=2595348115 tunneltype="ipsec" duration=3580
sentbyte=388020 rcvdbyte=387994 nextstat=600 advpnsc=0
```

The exhibit shows VPN event logs on FortiGate. In the output shown in the exhibit, which statement is true?

A. There are no IPsec tunnel statistics log messages for ADVPN cuts.
B. There is one shortcut tunnel built from master tunnel T_MPLS_0.
C. The VPN tunnel T_MPLS_0 is a shortcut tunnel.
D. The master tunnel T_INET_0 cannot accept the ADVPN shortcut.

Answer: B

Explanation:
 VPN event logs record the status of VPN tunnels, such as the establishment, termination, or failure of a tunnel. The output includes the following information:
? logid: the log ID number
? type: the log type, either traffic or event
? subtype: the log subtype, either vpn or ipsec
? level: the log level, either error, warning, or notice
? vd: the virtual domain name
? logdesc: the log description
? msg: the log message
? action: the log action, such as tunnel-up, tunnel-down, or tunnel-stats
? remip: the remote IP address
? locip: the local IP address
? remport: the remote port number
? locport: the local port number
? outintf: the outgoing interface name
? cookies: the IKE SA cookies
? user: the user name
? group: the user group name
? useralt: the alternative user name
? xauthuser: the XAuth user name
? authgroup: the XAuth user group name
? assignip: the assigned IP address
? vpntunnel: the VPN tunnel name
? tunnellip: the tunnel loopback IP address
? tunnelid: the tunnel ID number
? tunneltype: the tunnel type, either ipsec or ssl
? duration: the tunnel duration in seconds
? sentbyte: the number of bytes sent
? rcvdbyte: the number of bytes received
? nextstat: the next statistics interval in seconds
? advpnsc: the ADVPN shortcut flag, either 0 or 1 Based on the exhibit, the following statement is true:
? There is one shortcut tunnel built from master tunnel T_MPLS_0. This means that the VPN tunnel T_MPLS_0 is a master tunnel that can send ADVPN shortcut offers to other spokes, and the VPN tunnel T_MPLS_0_0 is a shortcut tunnel that is built from the master tunnel T_MPLS_01. In the exhibit, the log action for T_MPLS_0 is tunnel-up, and the log action for T_MPLS_0_0 is shortcut-up. The advpnsc flag for T_MPLS_0 is 0, indicating that it is not a shortcut tunnel, while the advpnsc flag for T_MPLS_0_0 is 1, indicating that it is a shortcut tunnel.

NEW QUESTION 24
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), heath-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_N1PLS_0 has a latency of 80 ms.

Answer: D

NEW QUESTION 25
What are two advantages of using an IPsec recommended template to configure an IPsec tunnel in an hub-and-spoke topology? (Choose two.)

A. It ensures consistent settings between phase1 and phase2.
B. It guides the administrator to use Fortinet recommended settings.
C. It automatically install IPsec tunnels to every spoke when they are added to the FortiManager ADOM.
D. The VPN monitor tool provides additional statistics for tunnels defined with an IPsec recommended template.

Answer: AB

Explanation:
The use of an IPsec recommended template offers the advantage of ensuring consistent settings between phase1 and phase2 (A), which is essential for the stability and security of the IPsec tunnel. Additionally, it guides the administrator to use Fortinet's recommended settings (B), which are designed to optimize performance and security based on Fortinet's best practices. References: The benefits of using IPsec recommended templates are outlined in Fortinet's SD-WAN documentation, which emphasizes the importance of consistency and adherence to recommended configurations.

NEW QUESTION 28
Refer to the exhibit, which shows an SD-WAN zone configuration on the FortiGate GUI.
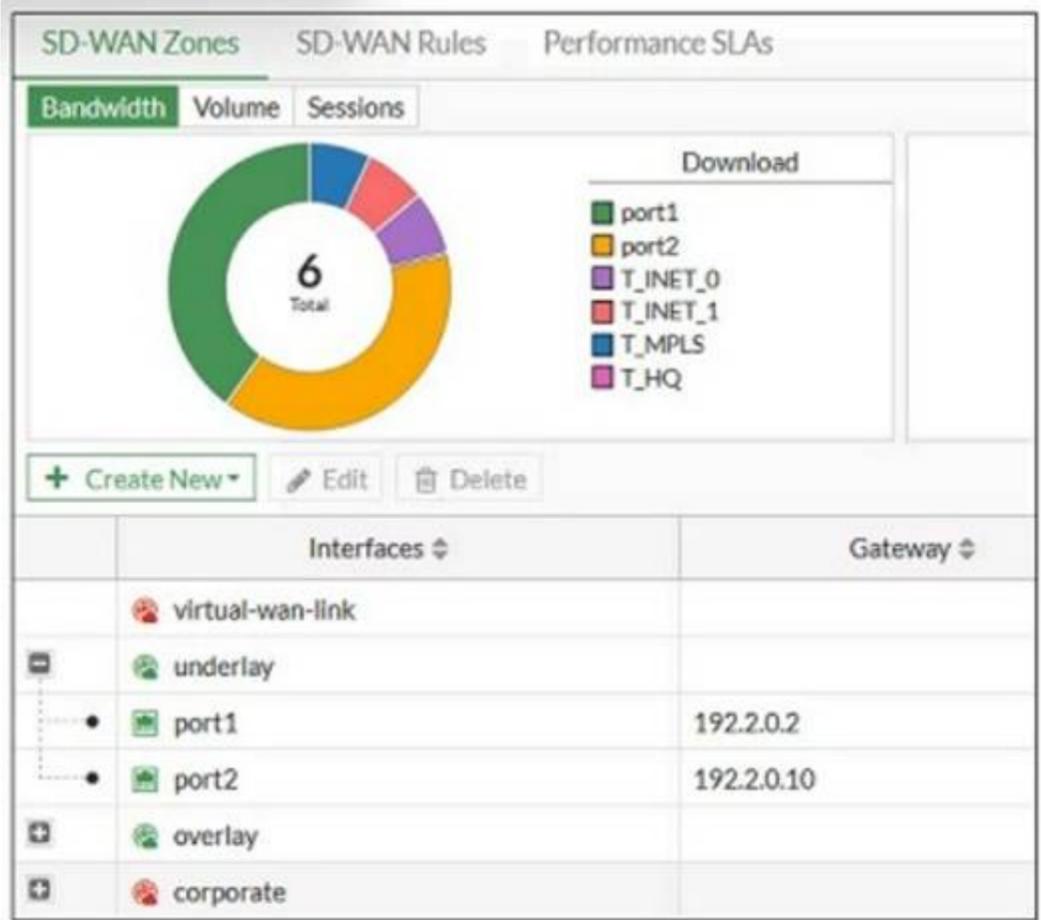
Based on the exhibit, which statement is true?

A. You can delete the virtual-wan-link zone because it contains no member.
B. The corporate zone contains no member.
C. You can move port1 from the underlay zone to the overlay zone.
D. The overlay zone contains four members.

Answer: B

Explanation:
Based on the exhibit, the "corporate" zone contains no member (B). In the FortiGate GUI, zones without members do not display any interfaces listed under them, which is the case for the corporate zone in the exhibit. References: This conclusion is based on standard Fortinet GUI interpretation and the operational logic of SD-WAN zones as per Fortinet's guidelines and user interface standards.

NEW QUESTION 31
In a hub-and-spoke topology, what are two advantages of enabling ADVPN on the IPsec overlays? (Choose two.)

A. It provides the benefits of a full-mesh topology in a hub-and-spoke network.
B. It provides direct connectivity between spokes by creating shortcuts.
C. It enables spokes to bypass the hub during shortcut negotiation.
D. It enables spokes to establish shortcuts to third-party gateways.

Answer: AB

NEW QUESTION 34
Refer to the exhibit.

```
id=20085 trace_id=847 func=print_pkt_detail line=5428 msg="vd-root:0 received a
packet(proto=6, 10.1.10.1:33920->74.125.195.93:443) from port3. flag [.], seq
2018554516, ack 4141536963, win 2238"
id=20085 trace_id=847 func=resolve_ip_tuple_fast line=5508 msg="Find an existing
session, id-000008c1, original direction"
id=20085 trace_id=847 func=shaper_handler line=821 msg="exceeded shaper limit, drop"
```

Which conclusion about the packet debug flow output is correct?

A. The original traffic exceeded the maximum packets per second of the outgoing interface, and the packet was dropped.
B. The reply traffic exceeded the maximum bandwidth configured in the traffic shaper, and the packet was dropped.
C. The original traffic exceeded the maximum bandwidth of the outgoing interface, and the packet was dropped.
D. The original traffic exceeded the maximum bandwidth configured in the traffic shaper, and the packet was dropped.

Answer: D

NEW QUESTION 37
Refer to the exhibit.
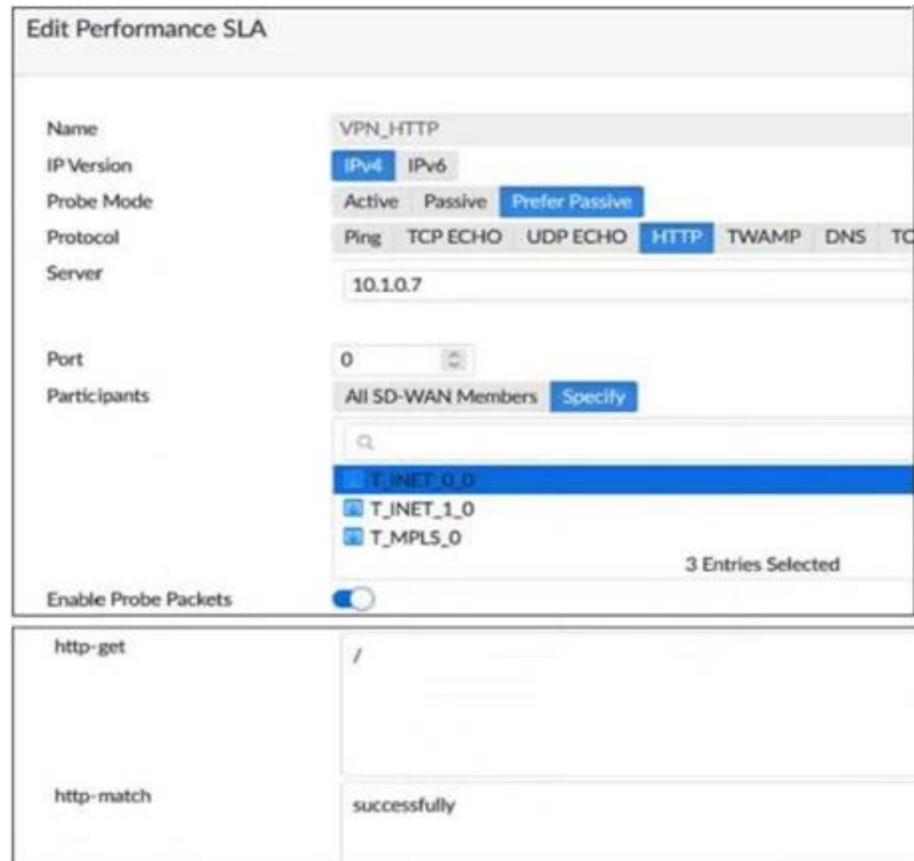
Based on the exhibit, which two statements are correct about the health of the selected members? (Choose two.)

A. After FortiGate switches to active mode, FortiGate never fails back to passive monitoring.
B. During passive monitoring, FortiGate can't detect dead members.
C. FortiGate can offload the traffic that is subject to passive monitoring to hardware.
D. FortiGate passively monitors the member if TCP traffic is passing through the member.

Answer: BD

NEW QUESTION 42
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+KywxBG4ZDT7jWHKd8YaL8j4+pRpYOx/N7mSgc7VL0BW2ZHQUXWJ6zvFxNKktiPYNtA8aP
i6ly7gDx2lP/OfKexTQQJzgCGRYzLM8eFTOnK7K6AuX0bFDCpBBhEIdf+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

NEW QUESTION 43
Which two statements about SD-WAN central management are true? (Choose two.)

A. The objects are saved in the ADOM common object database.
B. It does not support meta fields.
C. It uses templates to configure SD-WAN on managed devices.
D. It supports normalized interfaces for SD-WAN member configuration.

Answer: AC

Explanation:
Normalized interfaces are not supported for SD-WAN templates. You can create multiple SD-WAN zones and add interface members to the SD-WAN zones. You must bind the interface members by name to physical interfaces or VPN interfaces.https://docs.fortinet.com/document/fortigate/7.0.0/sd-wan-new-features/794804/new-sd-wan-template-fmg

NEW QUESTION 47
The SD-WAN overlay template helps to prepare SD-WAN deployments. To complete the tasks performed by the SD-WAN overlay template, the administrator must perform some post-run tasks. What are three mandatory post-run tasks that must be performed? (Choose three.)

A. Create policy packages for branch devices.
B. Assign an sdwan_id metadata variable to each device (branch and hub}.
C. Configure routing through overlay tunnels created by the SD-WAN overlay template.
D. Assign a branch_id metadata variable to each branch device.
E. Configure SD-WAN rules.

Answer: ABC

NEW QUESTION 51
Refer to the exhibits. Exhibit A -

Edit Performance SLA

Name	Level3_DNS
IP Version	**IPv4** IPv6
Probe Mode	**Active** Passive Prefer Passive
Protocol	**Ping** TCP ECHO UDP ECHO HTTP TWA
Server	4.2.2.1
	4.2.2.2
Participants	All SD-WAN Members **Specify**
	🔍
	port1
	port2
	2 Entries
Enable Probe Packets	⬤
SLA Targets ⓘ	
	+ Add Target

Link Status

Interval	500	Milliseconds
Failure Before Inactive	3	(max 3600)
Restore Link After	2	(max 3600)

Action When Inactive

Update Static Route	⬤
Cascade Interfaces	⬤

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 54
Refer to the exhibit.

```
config router bgp
    set as 65000
    set router-id 10.1.0.1
    set ibgp-multipath enable
    set additional-path enable
    set additional-path-select 3
    config neighbor-group
        edit "Branches_INET_0"
            set interface "T_INET_0_0"
            set remote-as 65000
            set update-source "T_INET_0_0"
        next
        edit "Branches_INET_1"
            set interface "T_INET_1_0"
            set remote-as 65000
            set update-source "T_INET_1_0"
        next
        edit "Branches_MPLS"
            set interface "T_MPLS_0"
            set remote-as 65000
            set update-source "T_MPLS_0"
        next
    end
    config neighbor-range
        edit 1
            set prefix 10.201.1.0 255.255.255.0
            set neighbor-group "Branches_INET_0"
        next
        edit 2
            set prefix 10.202.1.0 255.255.255.0
            set neighbor-group "Branches_INET_1"
        next
        edit 3
            set prefix 10.203.1.0 255.255.255.0
            set neighbor-group "Branches_MPLS"
        next
    end
    ...
end
```

The exhibit shows the BGP configuration on the hub in a hub-and-spoke topology. The administrator wants BGP to advertise prefixes from spokes to other spokes over the IPsec overlays, including additional paths. However, when looking at the spoke routing table, the administrator does not see the prefixes from other spokes and the additional paths.

Based on the exhibit, which three settings must the administrator configure inside each BGP neighbor group so spokes can learn other spokes prefixes and their additional paths? (Choose three.)

A. Set additional-path to send
B. Enable route-reflector-client
C. Set advertisement-interval to the number of additional paths to advertise
D. Set adv-additional-path to the number of additional paths to advertise
E. Enable soft-reconfiguration

Answer: ABD

NEW QUESTION 56
Refer to the exhibit.

Create New SD-WAN Interface Member

Sequence Number	1
Interface Member	
SD-WAN Zone	virtual-wan-link
Gateway IP	0.0.0.0
Cost	0
Status	(on)
Priority	0

Advanced Options >

Which two SD-WAN template member settings support the use of FortiManager meta fields? (Choose two.)

A. Cost
B. Interface member
C. Priority
D. Gateway IP

Answer: BD

NEW QUESTION 60
Exhibit A shows the firewall policy and exhibit B shows the traffic shaping policy.

Exhibit A	Exhibit B	

Edit Policy

Name ⓘ	Internet Access
Incoming interface	port3
Outgoing interface	virtual-wan link
Source	all ✕ +
Destination	all ✕ +
Schedule	always
Service	ALL ✕ +
Action	✓ ACCEPT ⊘ DENY
Inspection Mode	Flow-based Proxy-based

Firewall / Network Options

NAT	(on)
IP Pool Configuration	Use Outgoing Interface Address Use Dynamic
Preserve Source Port	(off)
Protocol Options	PROT default

| Exhibit A | Exhibit B | |

Edit Traffic Shaping Policy

Name	inbound_outbound_shaper
Status	🛈 Enabled ❗ Disabled
Comments	Write a comment... 0/255

If Traffic Matches:

Source	🖥 all ✕ +
Destination	🖥 all ✕ +
Schedule	⬭
Service	👤 ALL ✕ +
Application ℹ	+
URL Category	Streaming Media and Download ✕ +

Then:

Action	Apply Shaper Assign Shaping Class ID
Outgoing interface	🌐 virtual-wan link ✕ +
Shared shaper 🟢	guarantee-10mbps ▼

The traffic shaping policy is being applied to all outbound traffic; however, inbound traffic is not being evaluated by the shaping policy.
Based on the exhibits, what configuration change must be made in which policy so that traffic shaping can be applied to inbound traffic?

A. Create a new firewall policy, and the select the SD-WAN zone as Incoming Interface.
B. In the traffic shaping policy, select Assign Shaping Class ID as Action.
C. In the firewall policy, select Proxy-based as Inspection Mode.
D. In the traffic shaping policy, enable Reverse shaper, and then select the traffic shaper to use.

Answer: D

NEW QUESTION 61
Which CLI command do you use to perform real-time troubleshooting for ADVPN negotiation?

A. get router info routing-table all
B. diagnose debug application ike
C. diagnose vpn tunnel list
D. get ipsec tunnel list

Answer: B

Explanation:
IKE real-time debug - useful when debugging ADVPN shortcut messages and spoke-to- spoke negotiations.
• diagnose debug console timestamp enable
• diagnose vpn ike log filter clear
• diagnose vpn ike log filter mdst-addr4 <ip.of.hub> <ip.of.spoke>
• diagnose debug application ike -1
• diagnose debug enable

NEW QUESTION 63
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 65
Which statement about using BGP routes in SD-WAN is true?

A. Learned routes can be used as dynamic destinations in SD-WAN rules.
B. You must use BGP to route traffic for both overlay and underlay links.
C. You must configure AS path prepending.
D. You must use external BGP.

Answer: A

NEW QUESTION 68
Refer to the exhibit.

```
# diagnose firewall shaper per-ip-shaper list
name FTP_5M
maximum-bandwidth 625 KB/sec
maximum-concurrent-session 5
tos ff/ff
packets dropped 65
bytes dropped 81040
        addr=10.1.0.1 status: bps=0 ses=1
        addr=10.1.0.100 status: bps=0 ses=1
        addr=10.1.10.1 status: bps=1656 ses=3
```

Which are two expected behaviors of the traffic that matches the traffic shaper? (Choose two.)

A. The number of simultaneous connections among all source IP addresses cannot exceed five connections.
B. The traffic shaper limits the combined bandwidth of all connections to a maximum of 5 MB/sec.
C. The number of simultaneous connections allowed for each source IP address cannot exceed five connections.
D. The traffic shaper limits the bandwidth of each source IP address to a maximum of 625 KB/sec.

Answer: CD

NEW QUESTION 71
Which two statements reflect the benefits of implementing the ADVPN solution to replace conventional VPN topologies? (Choose two.)

A. It creates redundant tunnels between hub-and-spokes, in case failure takes place on the primary links.
B. It dynamically assigns cost and weight between the hub and the spokes, based on the physical distance.
C. It ensures that spoke-to-spoke traffic no longer needs to flow through the tunnels through the hub.
D. It provides direct connectivity between all sites by creating on-demand tunnels betweenspokes.

Answer: CD

NEW QUESTION 75
......

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

NSE7_SDW-7.2 Practice Exam Features:

* NSE7_SDW-7.2 Questions and Answers Updated Frequently

* NSE7_SDW-7.2 Practice Questions Verified by Expert Senior Certified Staff

* NSE7_SDW-7.2 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* NSE7_SDW-7.2 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The NSE7_SDW-7.2 Practice Test Here](https://www.certshared.com/exam/NSE7_SDW-7.2/)

Thank You for Trying Our Product