Fortinet

Exam Questions NSE7_SDW-7.0

Fortinet NSE 7 - SD-WAN 7.0

NEW QUESTION 1
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

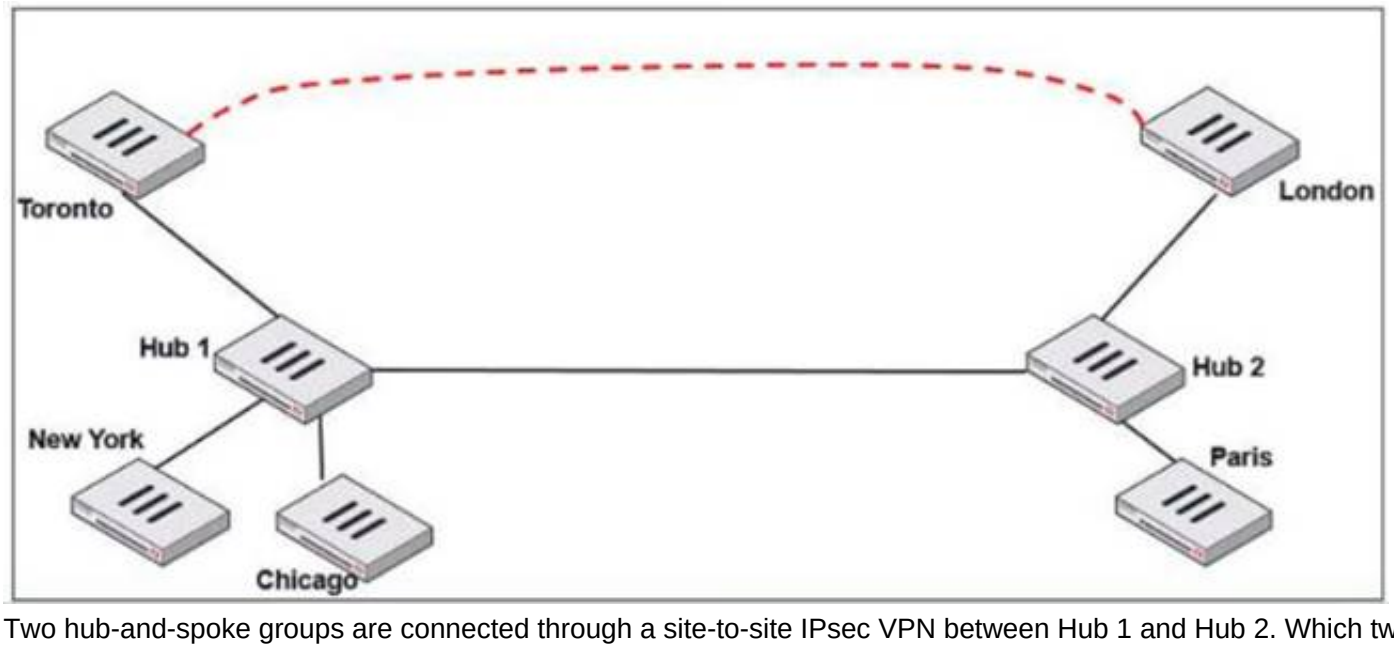
```
3.874431 T_INET_1_0 in 10.0.1.101 -> 10.1.0.7: icmp: echo request
3.874630 port5 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
3.874895 T_INET_0_0 in 10.0.1.101 -> 10.1.0.7: icmp: echo request
3.875125 T_MPLS_0 in 10.0.1.101 -> 10.1.0.7: icmp: echo request
3.875054 port5 in 10.1.0.7 -> 10.0.1.101: 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 2
Refer to the exhibit.



Two hub-and-spoke groups are connected through a site-to-site IPsec VPN between Hub 1 and Hub 2. Which two configuration settings are required for Toronto and London spokes to establish an ADVPN
shortcut? (Choose two.)

A. On the hubs, auto-discovery-sender must be enabled on the IPsec VPNs to spokes.
B. On the spokes, auto-discovery-receiver must be enabled on the IPsec VPN to the hub.
C. auto-discovery-forwarder must be enabled on all IPsec VPNs.
D. On the hubs, net-device must be enabled on all IPsec VPNs.

Answer: AB

NEW QUESTION 3
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 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

NEW QUESTION 5
What is a benefit of using application steering in SD-WAN?

A. The traffic always skips the regular policy routes.
B. You steer traffic based on the detected application.
C. You do not need to enable SSL inspection.
D. You do not need to configure firewall policies that accept the SD-WAN traffic.

Answer: B

NEW QUESTION 6
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: BC

NEW QUESTION 7
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 8
Exhibit A –

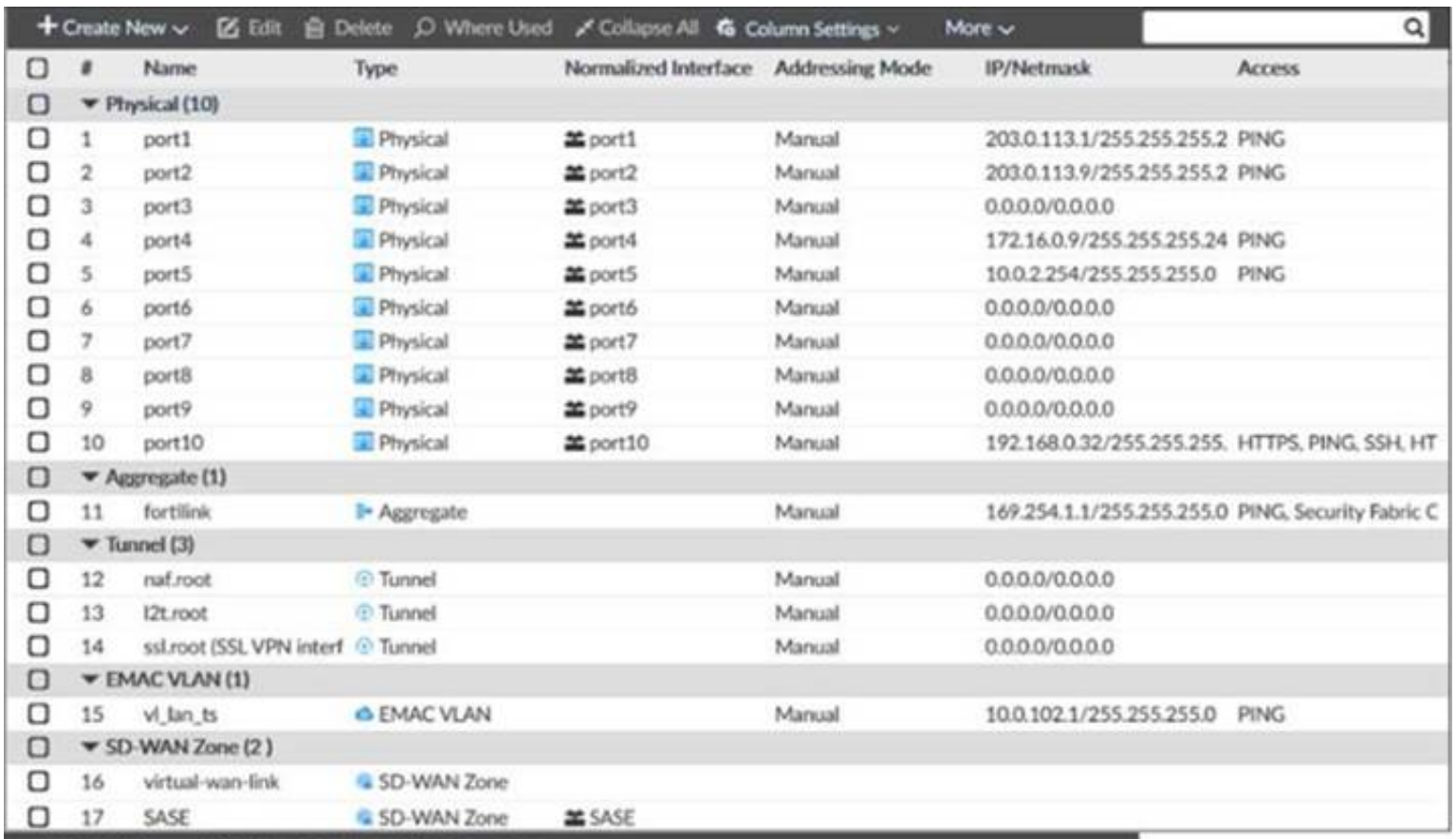


Exhibit B –

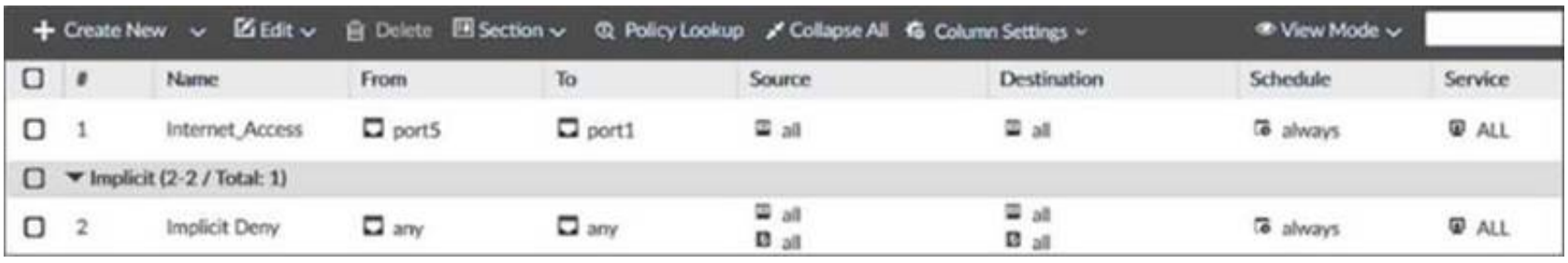


Exhibit A shows the system interface with the static routes and exhibit B shows the firewall policies on the managed FortiGate.
Based on the FortiGate configuration shown in the exhibits, what issue might you encounter when creating an SD-WAN zone for port1 and port2?

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 9
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 10
Which diagnostic command can you use to show the configured SD-WAN zones and their assigned members?

A. diagnose sys sdwan zone
B. diagnose sys sdwan service
C. diagnose sys sdwan member
D. diagnose sys sdwan interface

Answer: A

NEW QUESTION 10
Refer to the exhibits.
Exhibit A

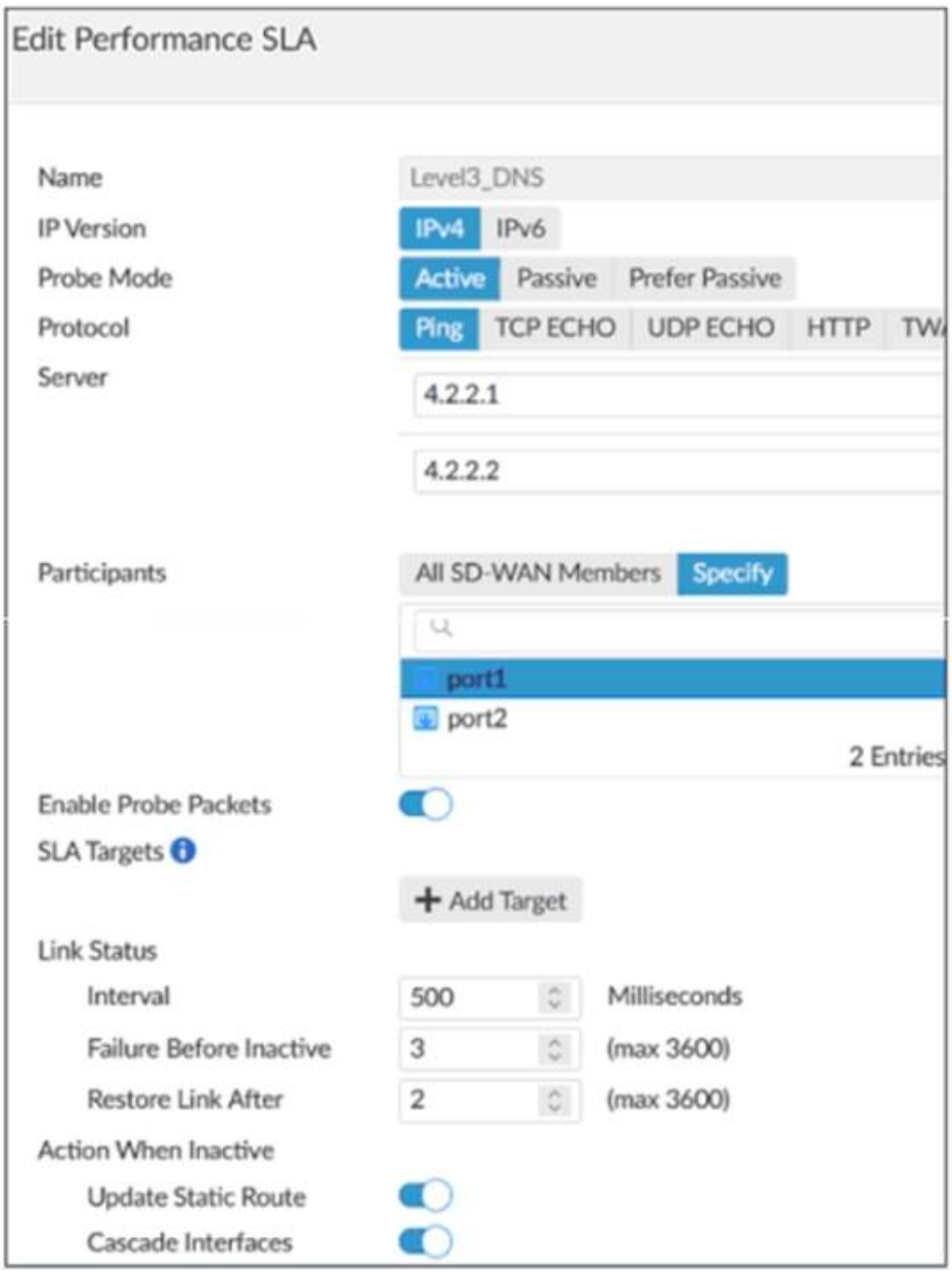


Exhibit B

```
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 11
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 14
Refer to the exhibits. Exhibit A

```
config system sdwan
    config health-check
        edit "Passive"
            set detect-mode passive
            set members 3 4
        next
    end
end

config system sdwan
    config service
        edit 1
            set name "Facebook-YouTube"
            set src "all"
            set internet-service enable
            set internet-service-app-ctrl 15832 31077
            set health-check "Passive"
            set priority-member 3 4
            set passive-measurement enable
        next
    end
end

branch1_fgt # get application name status | grep "id: 15832" -B1
app-name: "Facebook"
id: 15832

branch1_fgt # get application name status | grep "id: 31077" -B1
app-name: "YouTube"
id: 31077
```

Exhibit B

```
config firewall policy
    edit 1
        set name "DIA"
        set uuid b973e4ec-5f90-51ec-cadb-017c830d9418
        set srcintf "port5"
        set dstintf "underlay"
        set action accept
        set srcaddr "LAN-net"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set passive-wan-health-measurement enable
        set utm-status enable
        set ssl-ssh-profile "certificate-inspection"
        set application-list "default"
        set logtraffic all
        set auto-asic-offload disable
        set nat enable
    next
end

branch1_fgt # diagnose sys sdwan zone | grep underlay -A1
Zone underlay index=3
        members(2): 3(port1) 4(port2)
```

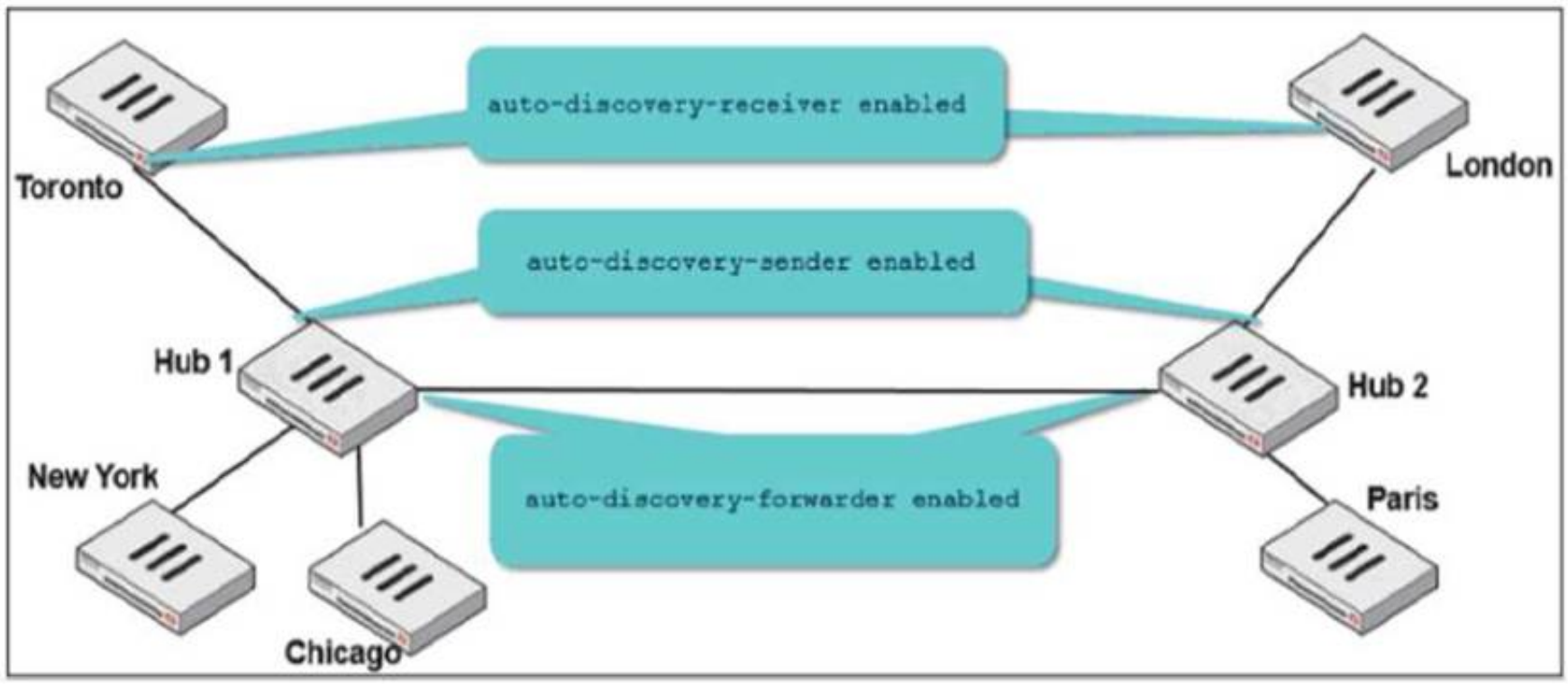
Exhibit A shows the SD-WAN performance SLA configuration, the SD-WAN rule configuration, and the application IDs of Facebook and YouTube. Exhibit B shows the firewall policy configuration and the underlay zone status.
Based on the exhibits, which two statements are correct about the health and performance of port1 and port2? (Choose two.)

A. The performance is an average of the metrics measured for Facebook and YouTube traffic passing through the member.
B. FortiGate is unable to measure jitter and packet loss on Facebook and YouTube traffic.
C. FortiGate identifies the member as dead when there is no Facebook and YouTube traffic passing through the member.
D. Non-TCP Facebook and YouTube traffic are not used for performance measurement.

Answer: AD

Explanation:
Study Guide 7.0, pages 88 - 89.
Study Guide 7.2, pages 103 - 104.
Another comment said "because without using application Control on the firewall policy, SDWAN can't work" but there is a app control "default" defined on config.

NEW QUESTION 16
Two hub-and-spoke groups are connected through a site-to-site IPsec VPN between Hub 1 and Hub 2. The administrator configured ADVPN on both hub-and-spoke groups.



Which two outcomes are expected if a user in Toronto sends traffic to London? (Choose two.)

A. London generates an IKE information message that contains the Toronto public IP address.
B. Traffic from Toronto to London triggers the dynamic negotiation of a direct site-to-site VPN.
C. Toronto needs to establish a site-to-site tunnel with Hub 2 to bypass Hub 1.
D. The first packets from Toronto to London are routed through Hub 1 then to Hub 2.

Answer: BD

NEW QUESTION 18
Which two tasks are part of using central VPN management? (Choose two.)

A. You can configure full mesh, star, and dial-up VPN topologies.
B. You must enable VPN zones for SD-WAN deployments.
C. FortiManager installs VPN settings on both managed and external gateways.
D. You configure VPN communities to define common IPsec settings shared by all VPN gateways.

Answer: AD

NEW QUESTION 23
Which three matching traffic criteria are available in SD-WAN rules? (Choose three.)

A. Type of physical link connection
B. Internet service database (ISDB) address object
C. Source and destination IP address
D. URL categories
E. Application signatures

Answer: BCE

NEW QUESTION 28
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 30
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 33
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 37
.....

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-7.0 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 FirstTry

* NSE7_SDW-7.0 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year