NSE7_SDW-7.0 Q&As

Fortinet NSE 7 - SD-WAN 7.0

Pass Fortinet NSE7_SDW-7.0 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/nse7_sdw-7-0.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

What are two roles that SD-WAN orchestrator plays when it works with FortiManager? (Choose two)

A. It configures and monitors SD-WAN networks on FortiGate devices that are managed by FortiManager.

B. It acts as a standalone device to assist FortiManager to manage SD-WAN interfaces on the managed FortiGate devices.

C. It acts as a hub FortiGate with an SD-WAN interface enabled and managed along with other FortiGate devices by FortiManager.

D. It acts as an application that is released and signed by Fortinet to run as a part of management extensions on FortiManager.

Correct Answer: AD

SD-WAN 6.4 Guide Page 158. https://docs2.fortinet.com/document/fortimanager/6.4.0/sd-wan-orchestrator-6-4-0-administration-guide/91581/introduction

QUESTION 2

Refer to the exhibit.

```
FortGate # 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
```

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

A. The traffic shaper drops packets if the bandwidth exceeds 6250 KBps.

B. The traffic shaper limits the bandwidth of each source IP to a maximum of 6250 KBps.

C. The traffic shaper drops packets if the bandwidth is less than 2500 KBps.

D. The measured bandwidth is less than 100 KBps.

Correct Answer: AD

QUESTION 3

Refer to the exhibit.

```
# get router info routing-table all
...
B       10.0.2.0/24 [200/0] via 10.201.1.2 [3] (recursive via VPN0 tunnel 100.64.1.1), 00:00:54
                    [200/0] via 10.202.1.2 [3] (recursive via VPN1 tunnel 100.64.1.9), 00:00:54
                    [200/0] via 10.203.1.1 [3] (recursive via VPN2 tunnel 172.16.1.5), 00:00:54
...
```

The device exchanges routes using IBGP.

Which two statements are correct about the IBGP configuration and routing information on the device? (Choose two.)

A. Each BGP route is three hops away from the destination.

B. ibgp-multipath is disabled.

C. additional-path is enabled.

D. You can run the get router info routing-table database command to display the additional paths.

Correct Answer: CD

QUESTION 4

Which action FortiGate performs on traffic that is subject to a per-IP traffic shaper of 10 Mbps?

A. FortiGate shares 10 Mbps of bandwidth equally among all source IP addresses.

B. FortiGate applies traffic shaping to the original traffic direction only.

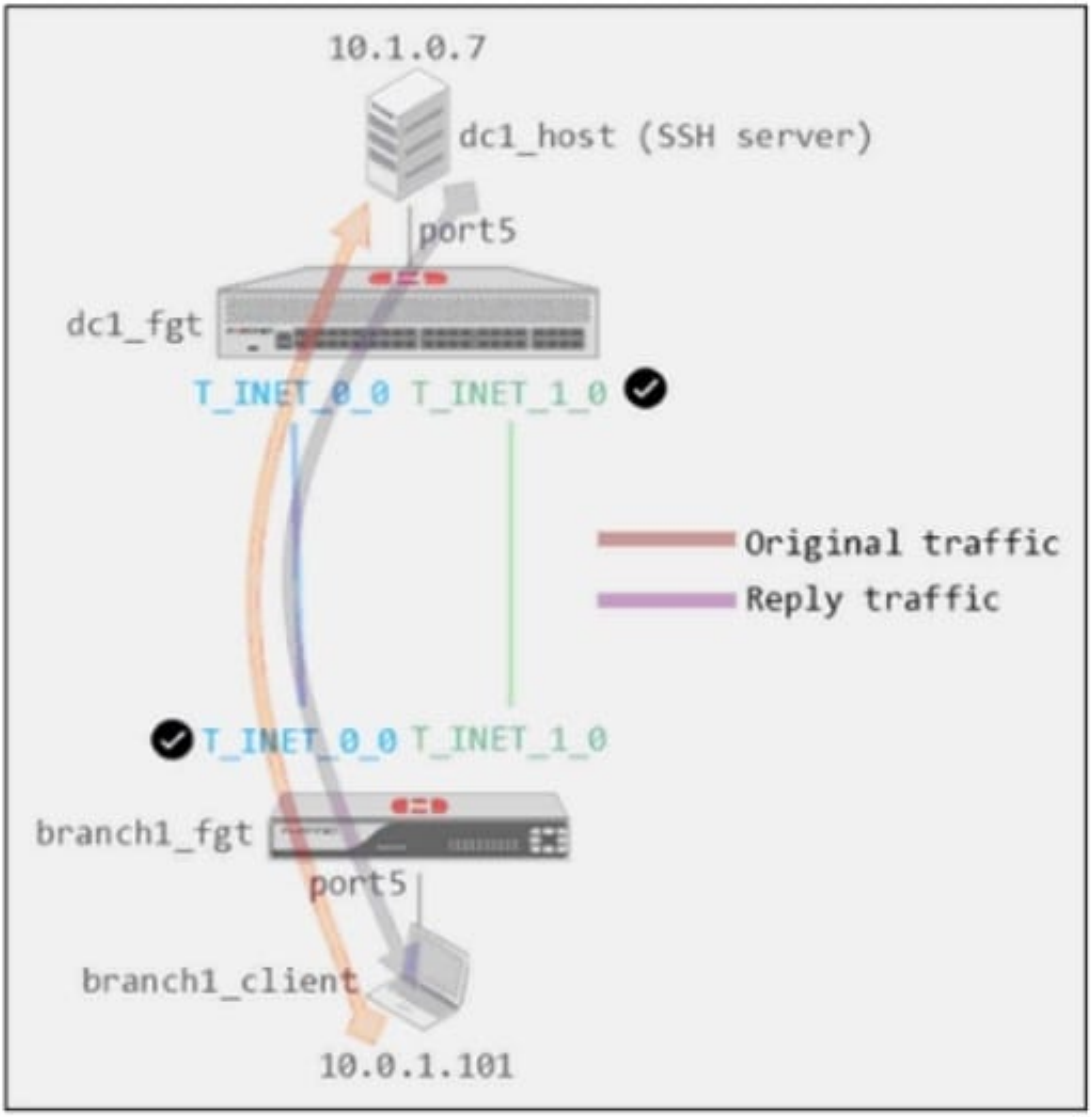
C. FortiGate limits each source IP address to a maximum bandwidth of 10 Mbps.

D. FortiGate guarantees a minimum of 10 Mbps of bandwidth to each source IP address.

Correct Answer: C

QUESTION 5

Refer to the exhibits. Exhibit A Exhibit B


10.1.0.7
dc1_host (SSH server)
port5
dc1_fgt
T_INET_0_0
T_INET_1_0
Original traffic
Reply traffic
T_INET_0_0
T_INET_1_0
branch1_fgt
port5
branch1_client
10.0.1.101

```
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 preferredmember 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.

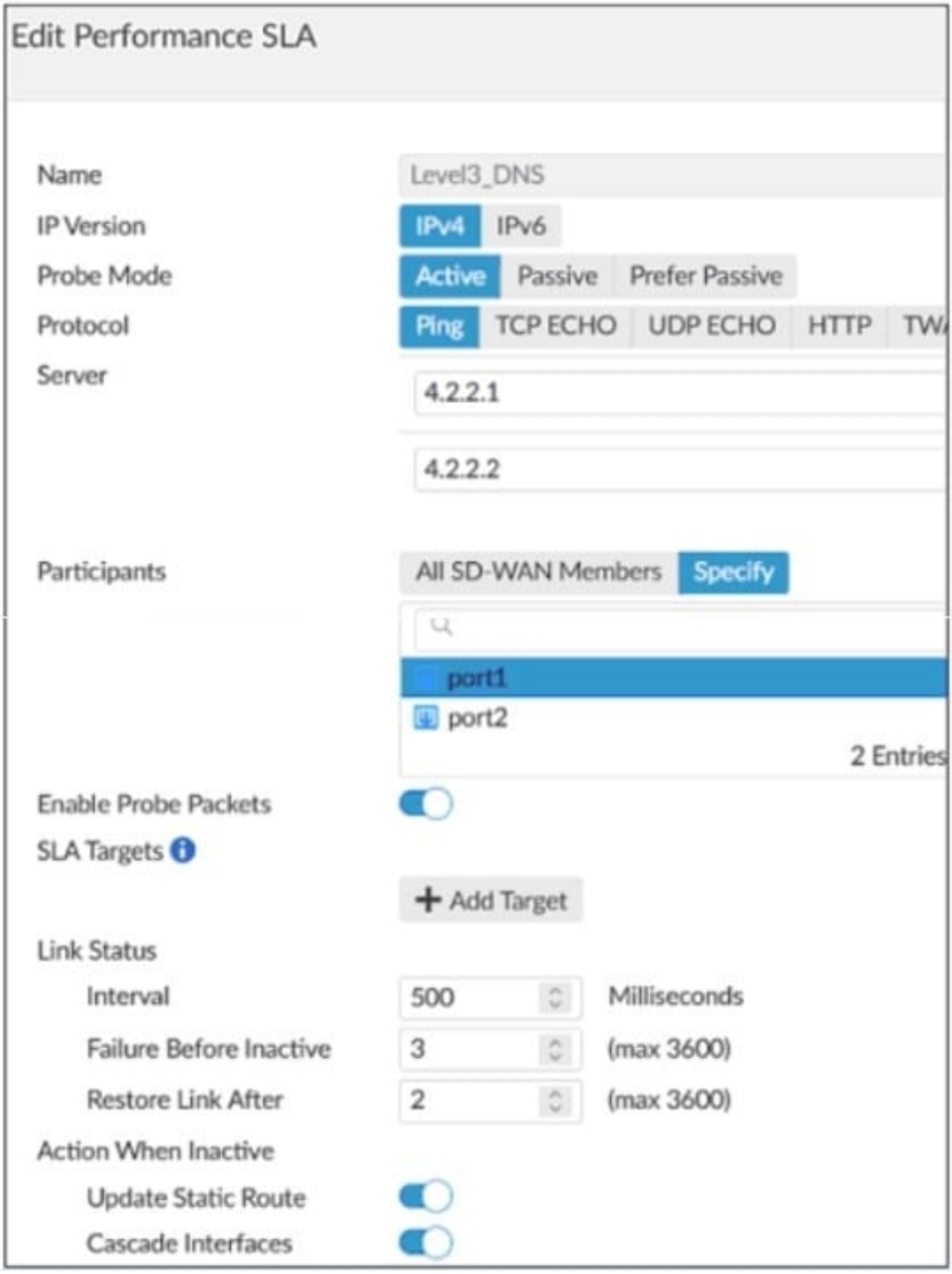
D. Disable allow-subnet-overlap under config system settings.

Correct Answer: A

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-with-auxiliary-session

QUESTION 6

Refer to the exhibits. Exhibit A Exhibit B


Edit Performance SLA
Name
Level3_DNS
IP Version
IPv4
IPv6
Probe Mode
Active
Passive
Prefer Passive
Protocol
Ping
TCP ECHO
UDP ECHO
HTTP
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

```
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.

Correct Answer: B

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

QUESTION 7

Refer to the exhibit.

```
# 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
```

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

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.

Correct Answer: BC

QUESTION 8

Which two protocols in the IPsec suite are most used for authentication and encryption? (Choose two.)

A. Encapsulating Security Payload (ESP)

B. Secure Shell (SSH)

C. Internet Key Exchange (IKE)

D. Security Association (SA)

Correct Answer: AC

QUESTION 9

Refer to exhibits.

Exhibit A | Exhibit B

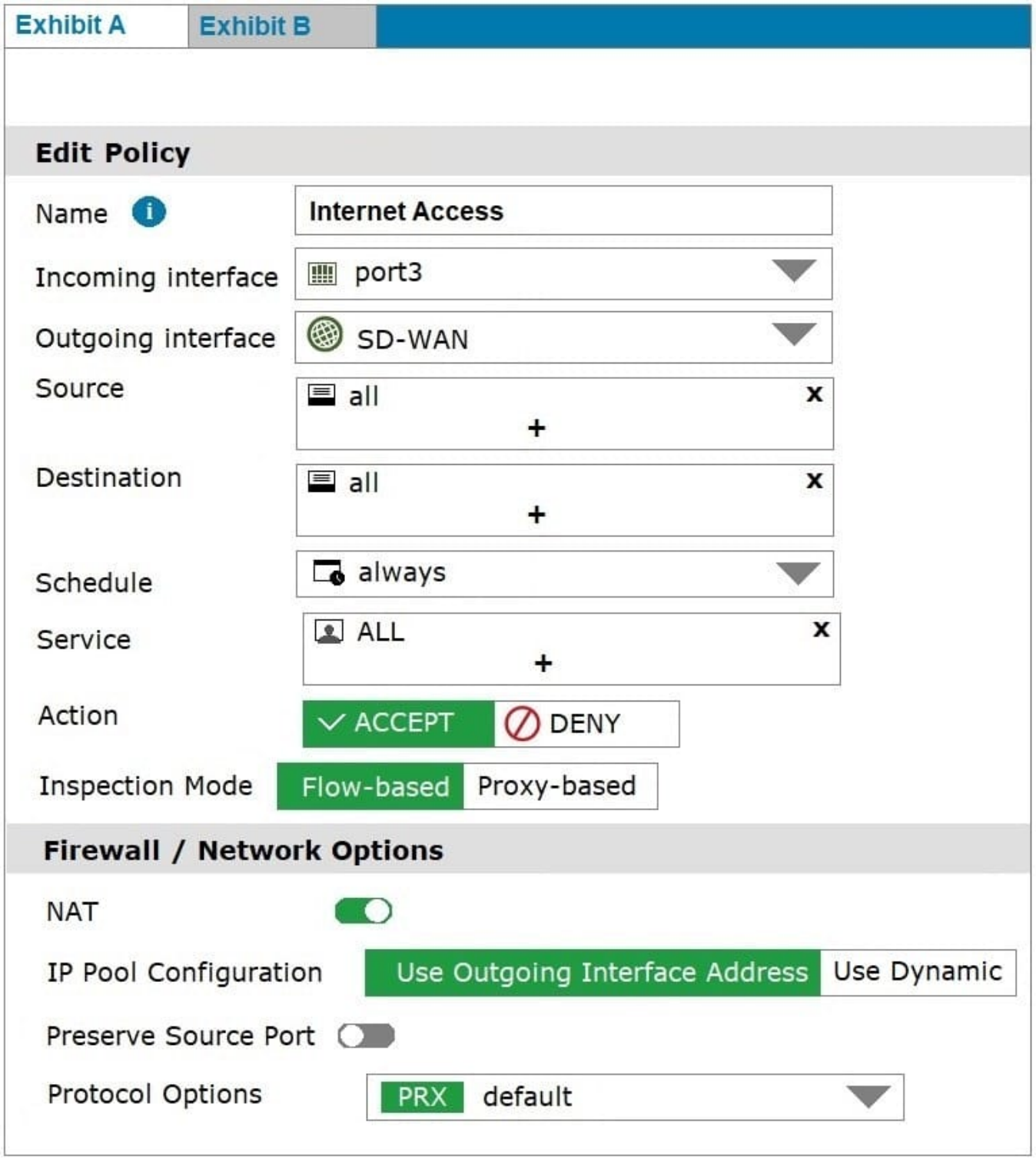


Exhibit A | Exhibit B

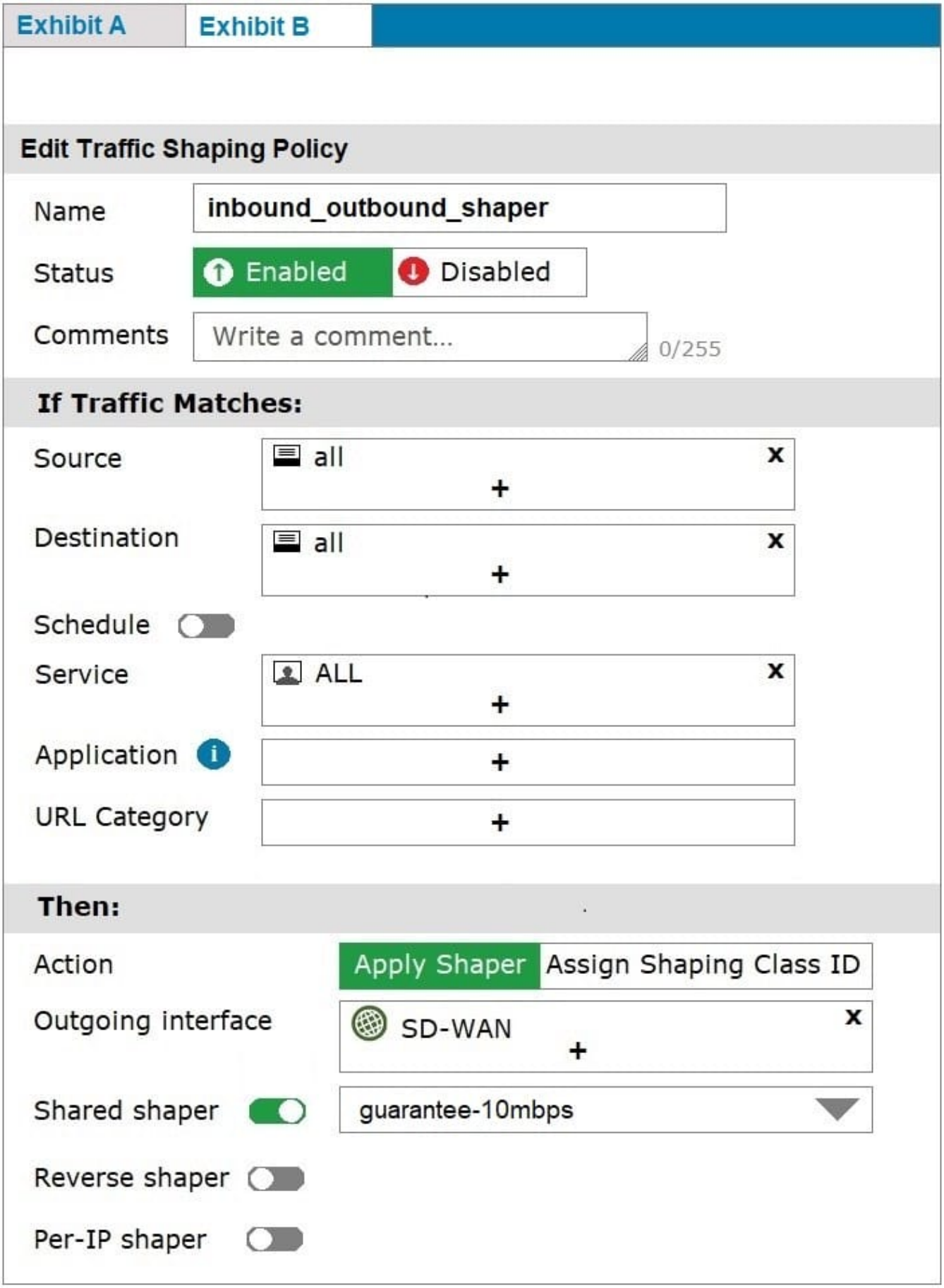


Exhibit A shows the firewall policy and exhibit B shows the traffic shaping policy.

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. The reverse shaper option must be enabled and a traffic shaper must be selected

B. The guaranteed-10mbps option must be selected as the reverse shaper option.

C. A new firewall policy must be created and SD-WAN must be selected as the incoming interface.

D. The guaranteed-10mbps option must be selected as the per-IP shaper option

Correct Answer: A

QUESTION 10

Which feature enables SD-WAN to combine IPsec VPN dynamic shortcut tunnels between spokes and a static tunnel to the hub?

A. ADVPN

B. GRE

C. SSLVPN

D. OCVPN

Correct Answer: A

QUESTION 11

Which statement reflects how BGP tags work with SD-WAN rules?

A. BGP tags match the SD-WAN rule based on the order that these rules were installed.

B. BGP tags require that the adding of static routes be enabled on all ADVPN interfaces

C. Route tags are used for a BGP community and the SD-WAN rules are assigned the same tag

D. VPN topologies are formed using only BGP dynamic routing with SD-WAN

Correct Answer: C

QUESTION 12

FortiGate is connected to the internet and is obtaining the IP address on its egress interlace from the DHCP server

Which statement is due when FortiGate restarts and receives preconfigured settings to install as part of a zero-touch provisioning process?

A. FortiDeploy connects with FortiGate and provides the initial configuration to contact FortiManager

B. The zero-touch provisioning process completes internally, behind FortiGate

C. FortiManager registers FortiGate after the restart and retrieves the existing configuration

D. The FortiGate cloud key added to the FortiGate cloud portal and FortiGate performs a factory reset before the restart

Correct Answer: A

QUESTION 13

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.

Correct Answer: A

QUESTION 14

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.

Correct Answer: AC

QUESTION 15

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

Correct Answer: B