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.pass4itsure.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

QUESTION 1

Which three parameters are available to configure SD-WAN rules? (Choose three.)

A. Application signatures

B. Type of physical link connection

C. URL categories

D. Source and destination IP address

E. Internet service database (ISDB) address object

Correct Answer: ADE

SD-WAN 6.4.5 Guide Page 76. https://docs.fortinet.com/document/fortigate/7.2.1/administration-guide/22371/sd-wan-rules-best-quality

QUESTION 2

Which three performance SLA protocols are available on the FortiGate CLI only? (Choose three.)

A. tcp-echo

B. icmp

C. twamp

D. udp-echo

E. smtp

Correct Answer: ACD

Command output from a fortigate:

FW-01 (test-health-check) # set protocol

ping Use PING to test the link with the server.

tcp-echo Use TCP echo to test the link with the server. udp-echo Use UDP echo to test the link with the server. http Use HTTP-GET to test the link with the server. twamp Use TWAMP to test the link with the server. dns Use DNS query to test

the link with the server. tcp-connect Use a full TCP connection to test the link with the server.

ftp Use FTP to test the link with the server.

QUESTION 3

Which statement about using BGP routes in SD-WAN is true?

A. Adding static routes must be enabled on all ADVPN interfaces.

B. VPN topologies must be form using only BGP dynamic routing with SD-WAN

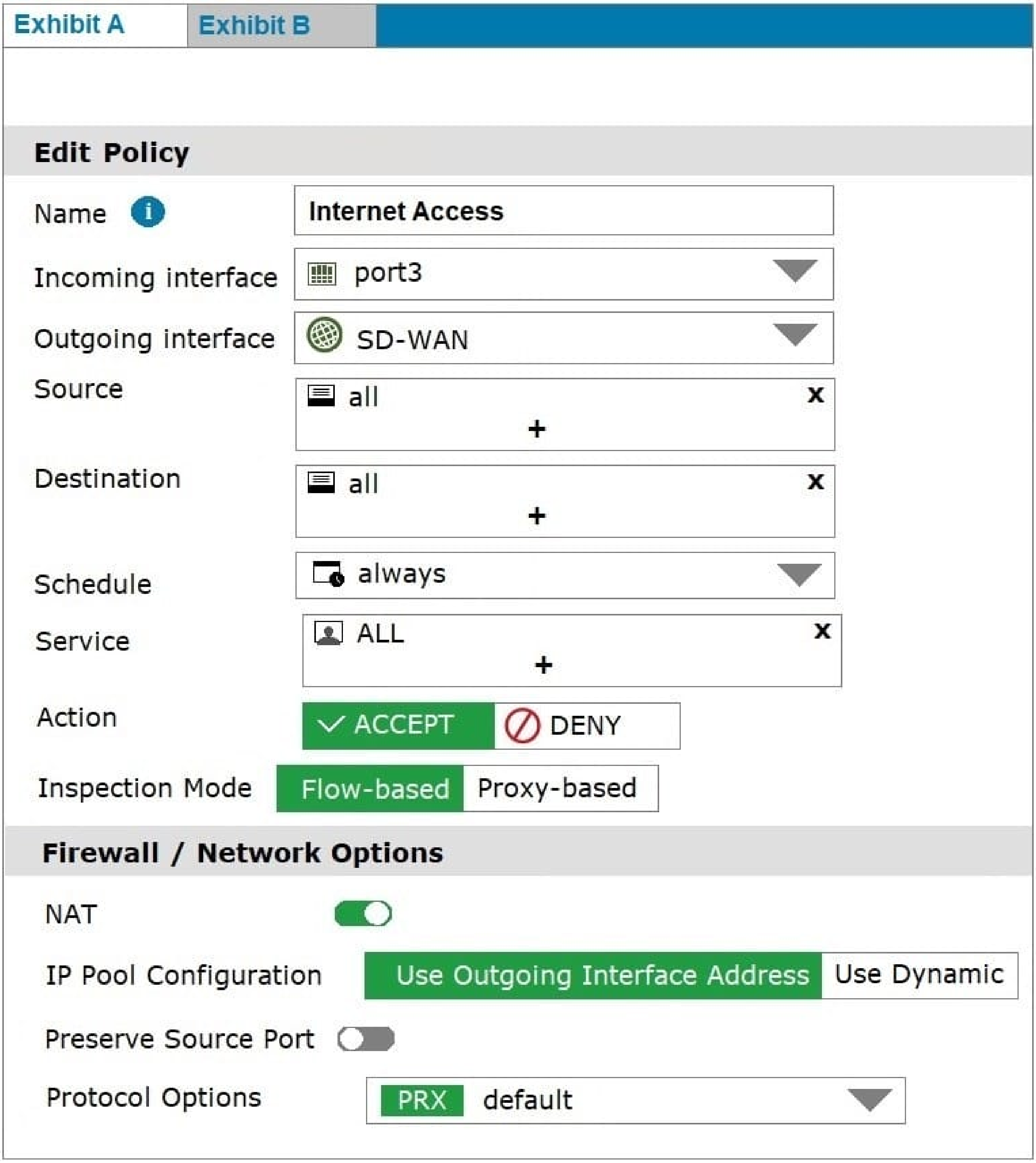
C. Learned routes can be used as dynamic destinations in SD-WAN rules

D. Dynamic routing protocols can be used only with non-encrypted traffic

Correct Answer: C

QUESTION 4

Refer to exhibits.

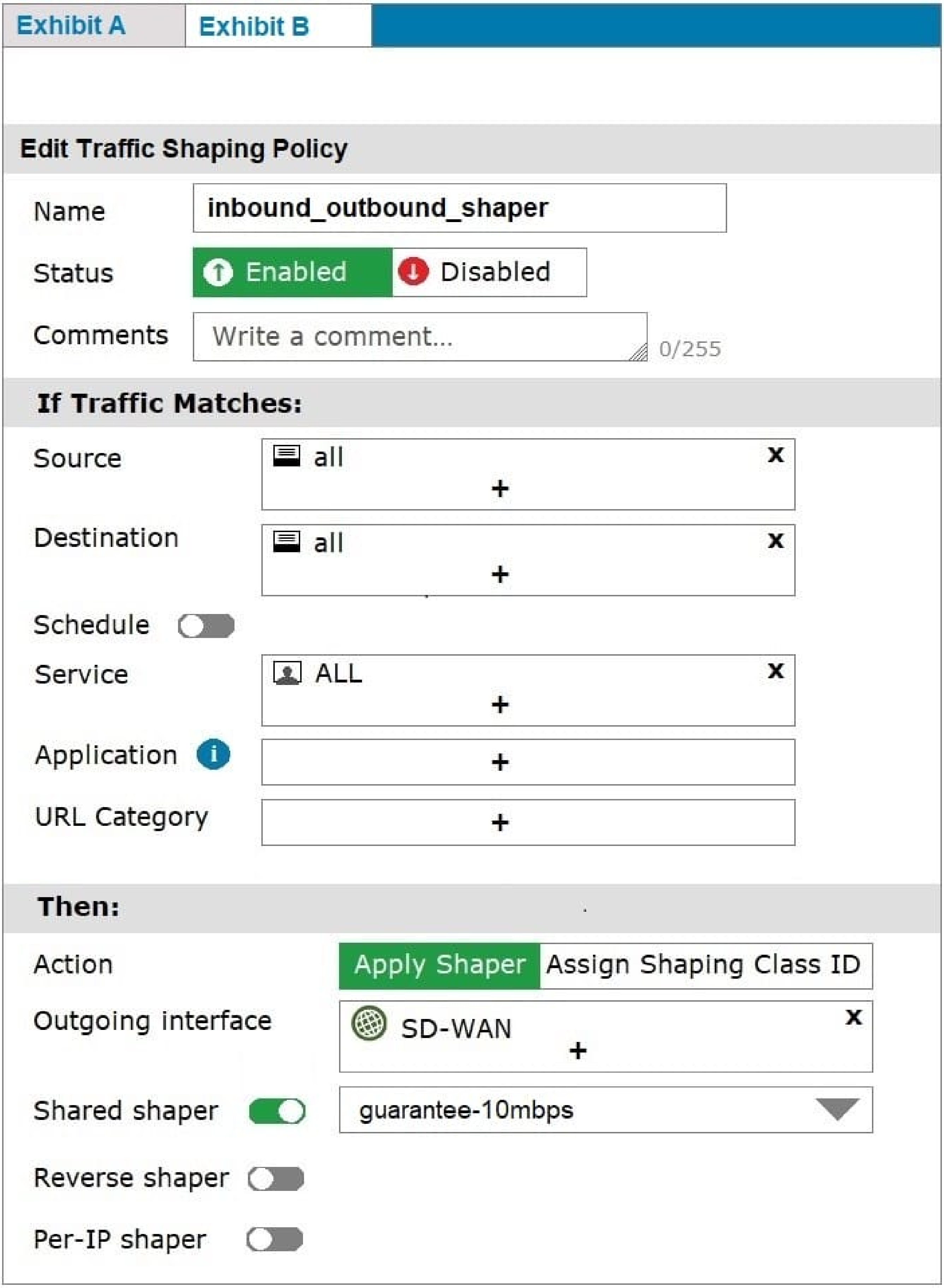


Edit Policy

Name	Internet Access
Incoming interface	port3
Outgoing interface	SD-WAN
Source	all
Destination	all
Schedule	always
Service	ALL
Action	[✓ ACCEPT] DENY
Inspection Mode	[✓ Flow-based] Proxy-based

Firewall / Network Options

NAT	●
IP Pool Configuration	[✓ Use Outgoing Interface Address] Use Dynamic
Preserve Source Port	○
Protocol Options	PRX default



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	
URL Category	

Then:

Action	[✓ Apply Shaper] Assign Shaping Class ID
Outgoing interface	SD-WAN
Shared shaper ●	guarantee-10mbps
Reverse shaper	○
Per-IP shaper	○

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.

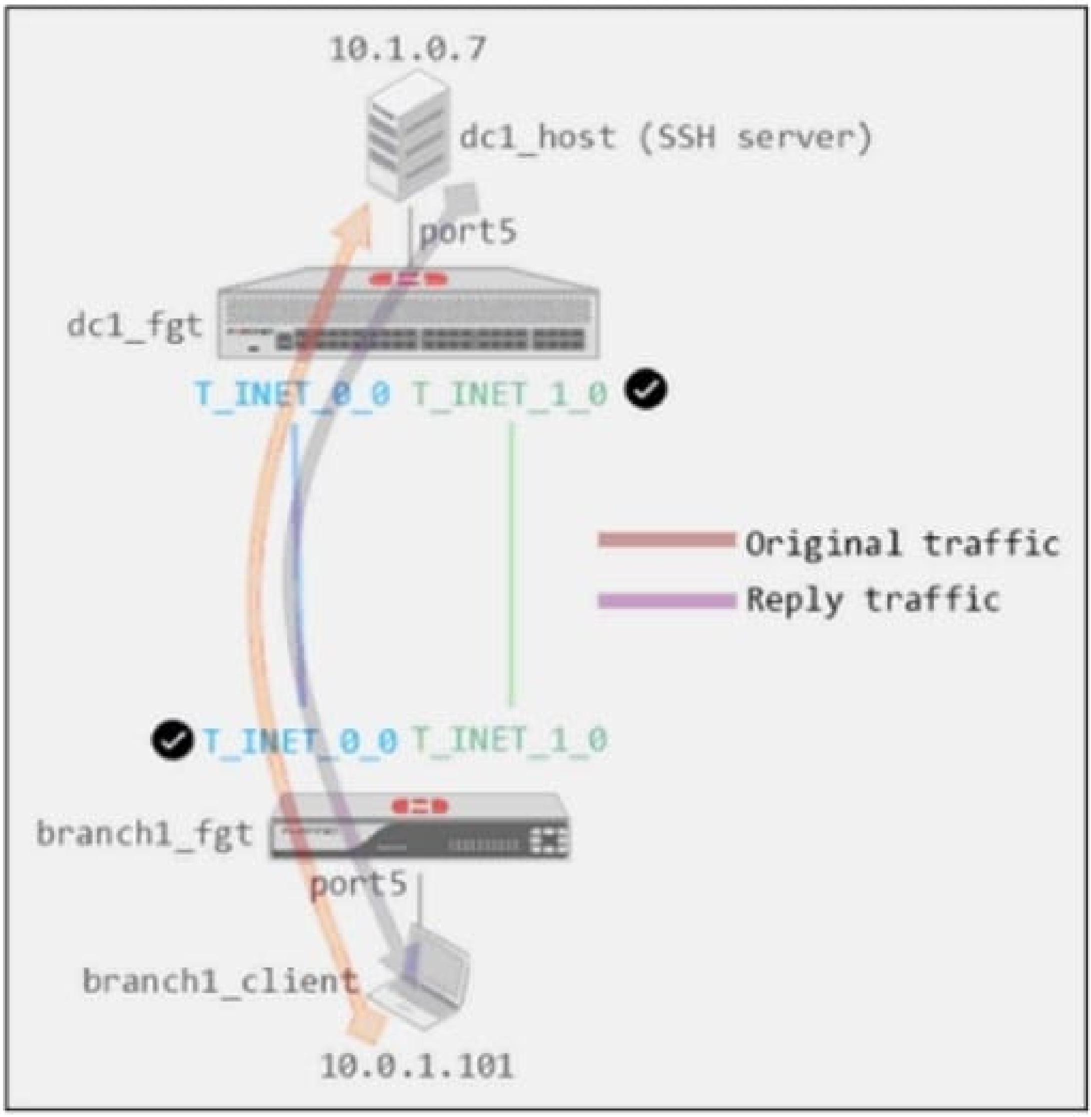
C. A new firewall policy must be created and SD-WAN must be selected as the incoming interface.

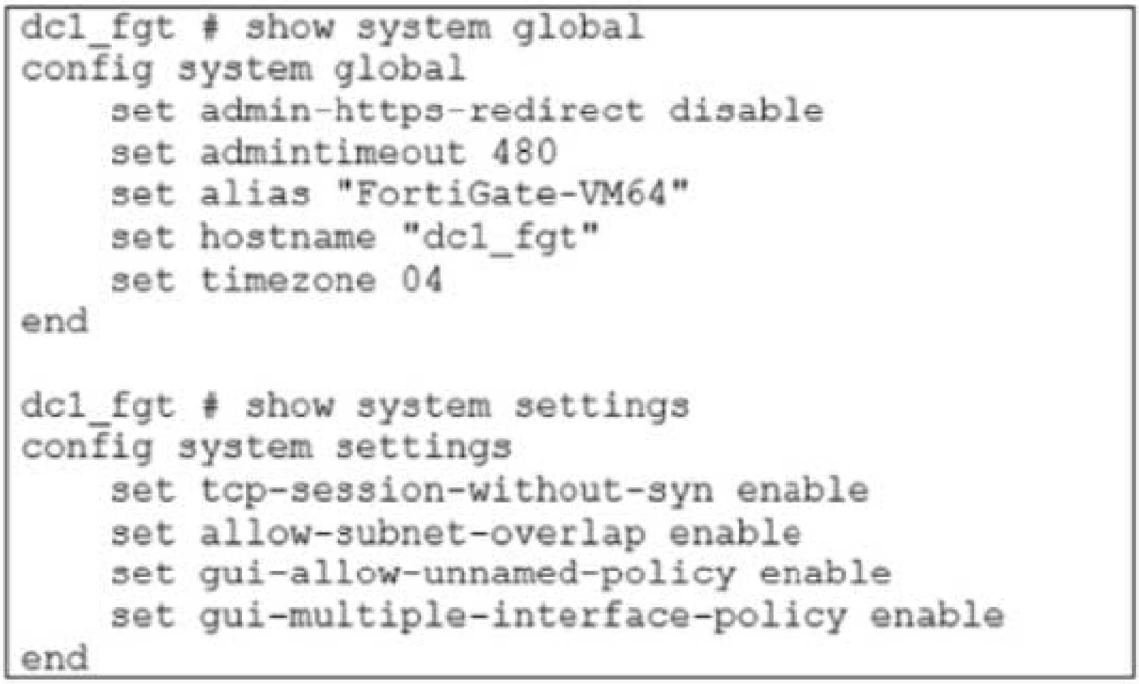
D. The guaranteed-10mbps option must be selected as the per-IP shaper option

Correct Answer: A

QUESTION 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.

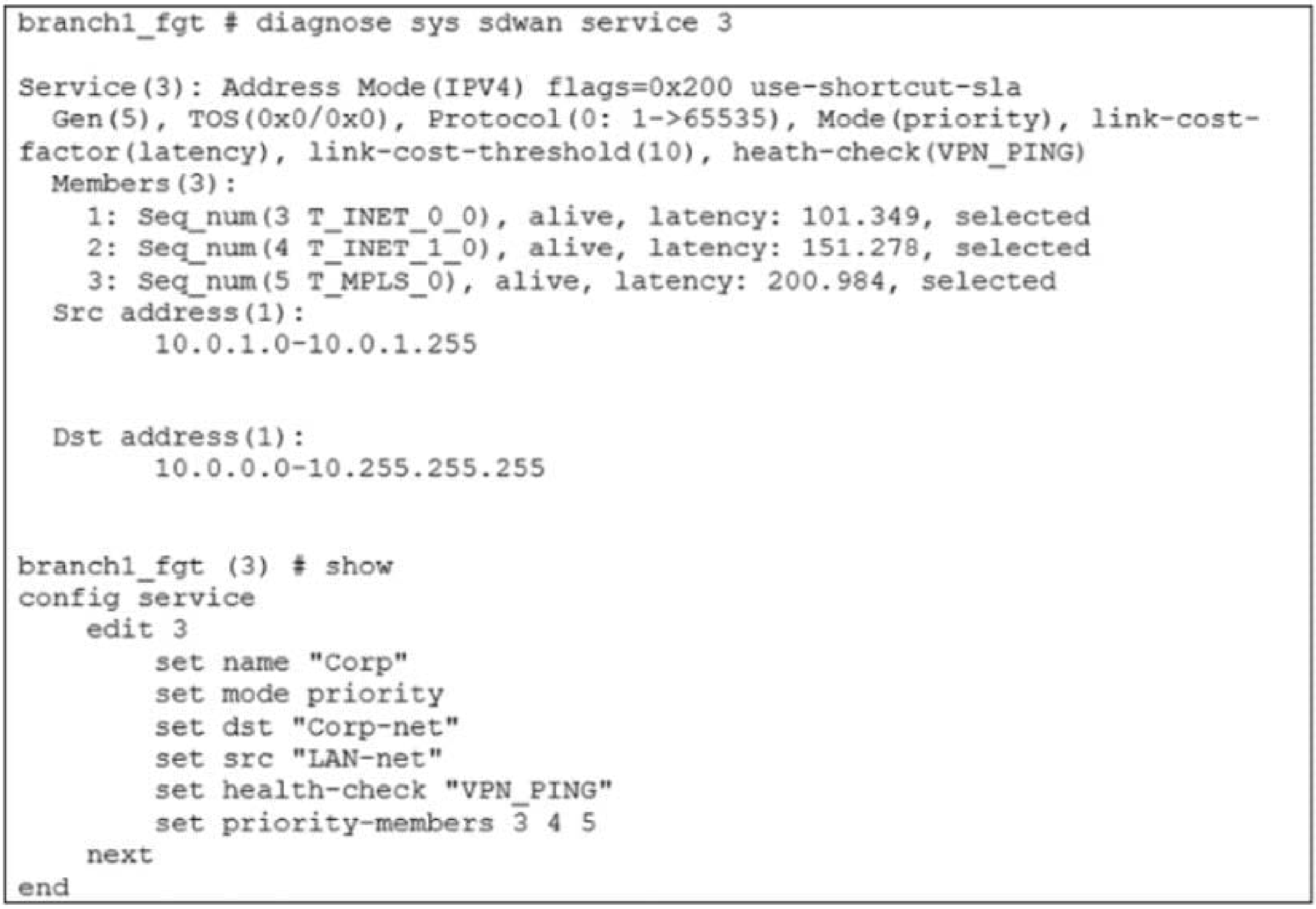
D. Disable allow-subnet-overlap under config system settings.

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 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.

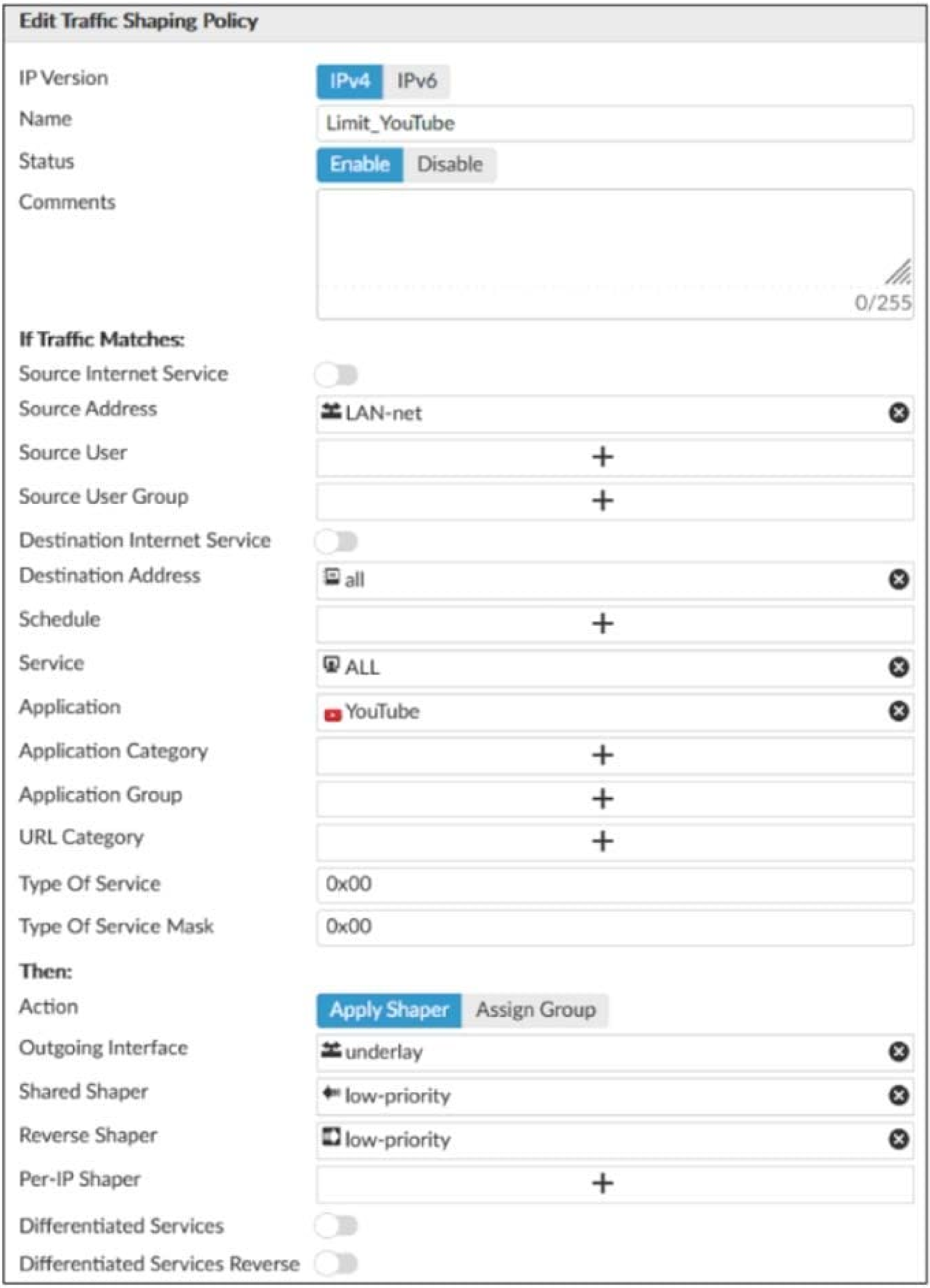
C. When T_INET_0_0 has a latency of 250 ms.

D. When T_N1PLS_0 has a latency of 80 ms.

Correct Answer: D

QUESTION 7

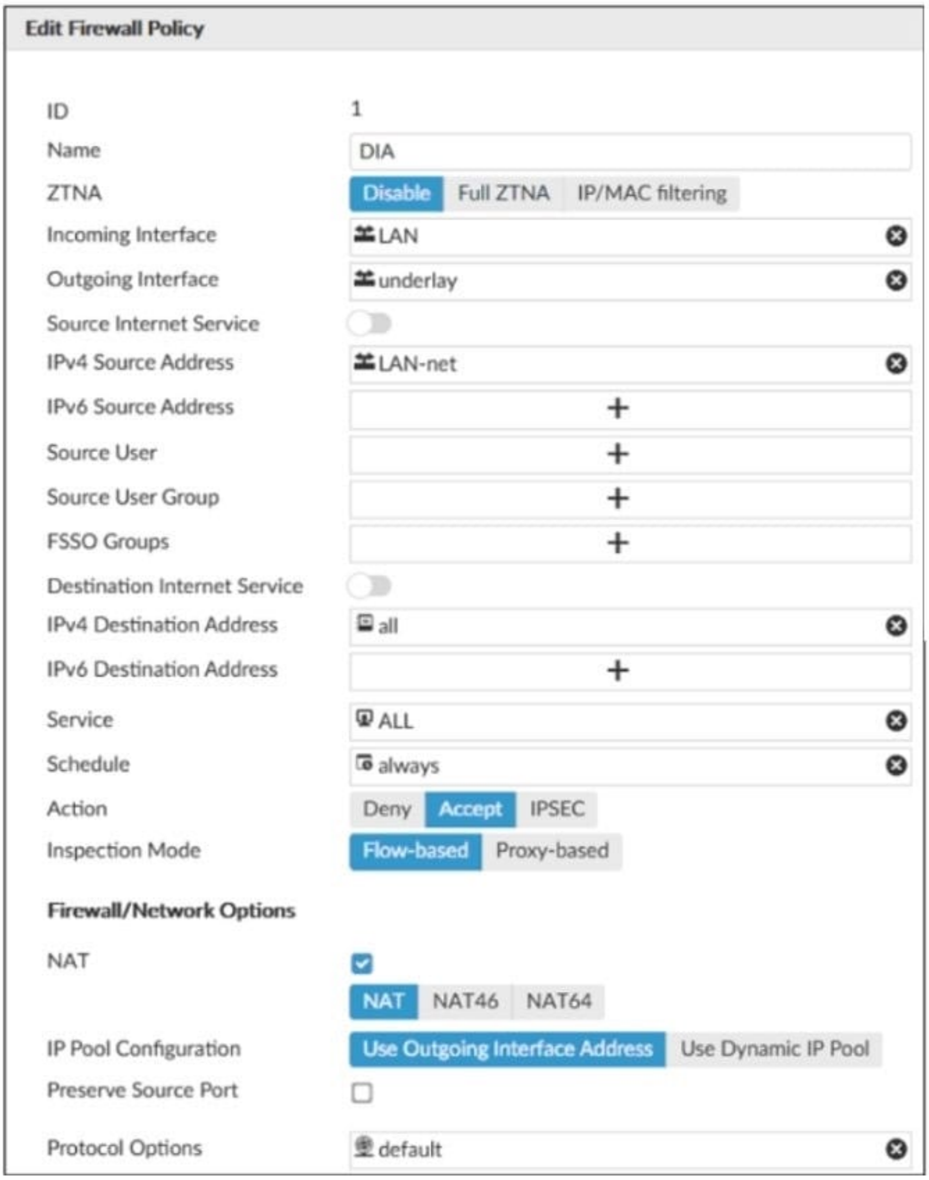
Refer to the exhibits. Exhibit A



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

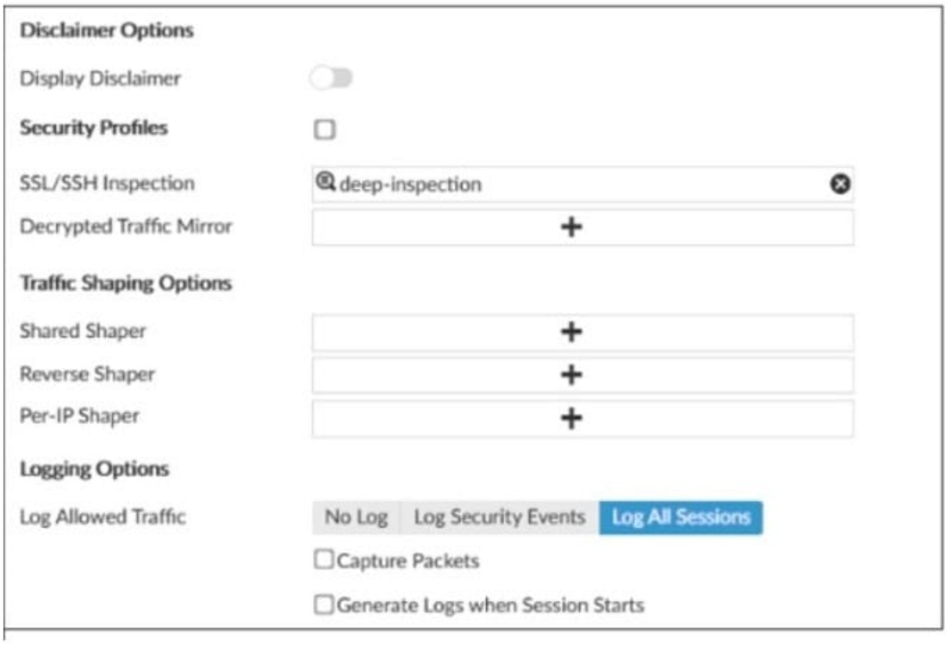


Edit Firewall Policy

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.

Correct Answer: B

QUESTION 8

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 9

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.

Correct Answer: AC

QUESTION 10

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

A. Member metrics are measured only if an SLA target is configured.

B. SLA targets are used only by SD-WAN rules that are configured with Lowest Cost (SLA) or Maximize Bandwidth (SLA) as strategy.

C. When configuring an SD-WAN rule, you can select multiple SLA targets of the same performance SLA.

D. SD-WAN rules use SLA targets to check if the preferred members meet the SLA requirements.

Correct Answer: BD

QUESTION 11

Which two statements describe how IPsec phase 1 aggressive mode is different from main 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.

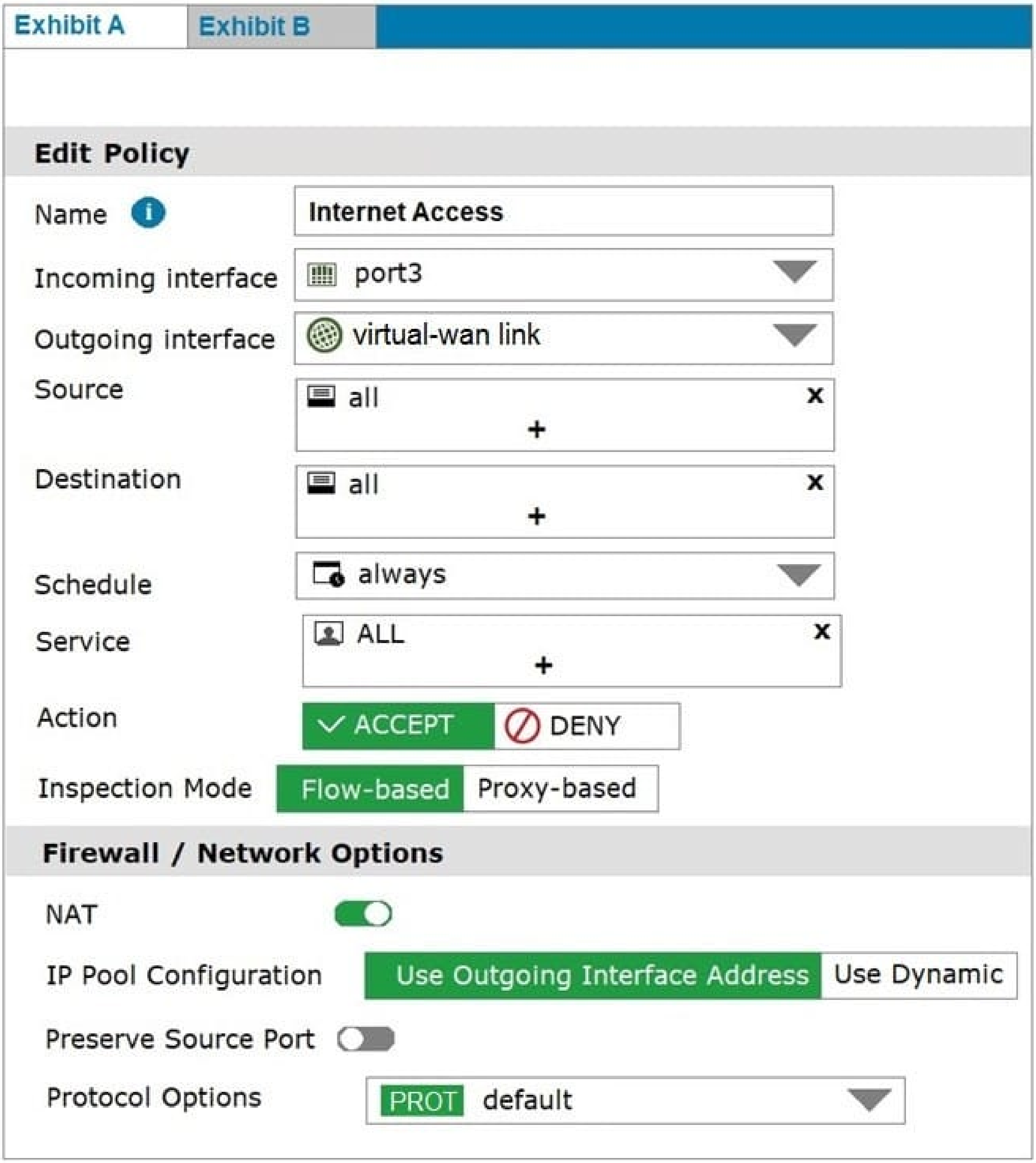
C. A total of six packets are exchanged between an initiator and a responder instead of three packets.

D. The use of Diffie Hellman keys is limited by the responder and needs initiator acceptance.

Correct Answer: AC

QUESTION 12

Refer to exhibits.

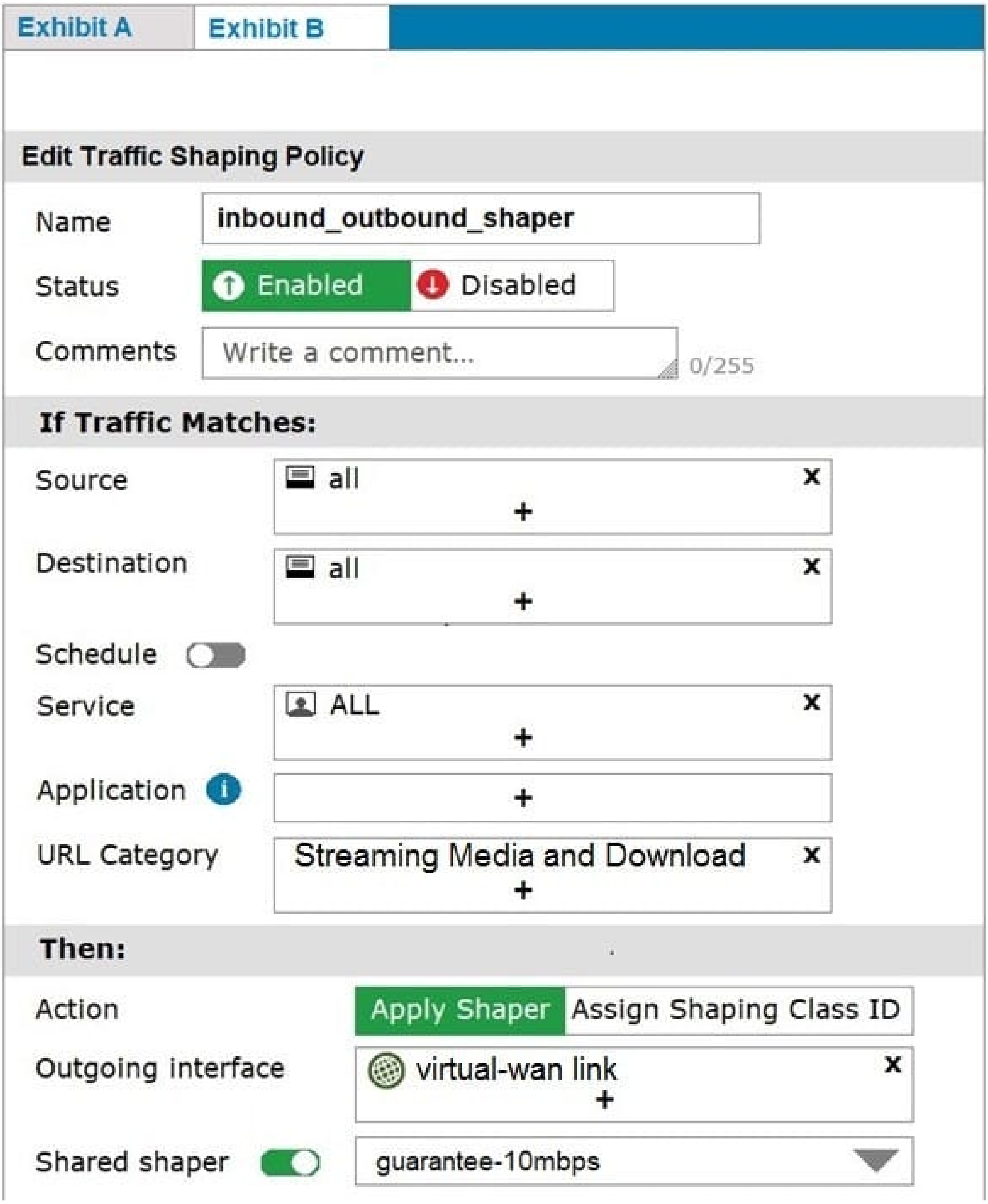


Edit Policy

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	●
IP Pool Configuration	Use Outgoing Interface Address / Use Dynamic
Preserve Source Port	○
Protocol Options	PROT default



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

URL Category: Streaming Media and Download

Then:

Action: Apply Shaper | Assign Shaping Class ID

Outgoing interface: virtual-wan link

Shared shaper: guarantee-10mbps

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. 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.

Correct Answer: D

QUESTION 13

Which statement defines how a per-IP traffic shaper of 10 Mbps is applied to the entire network?

A. FortiGate allocates each IP address a maximum 10 Mbps of bandwidth.

B. Each IP is guaranteed a minimum 10 Mbps of bandwidth

C. A single user uses the allocated bandwidth divided by total number of users.

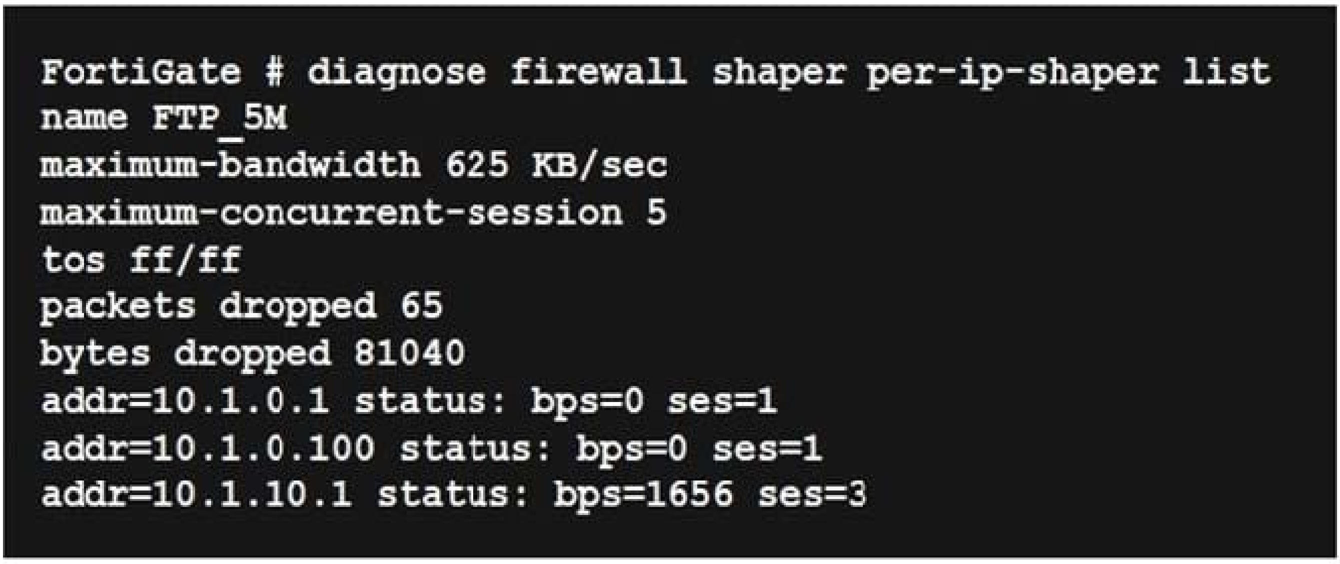
D. The 10 Mbps bandwidth is shared equally among the IP addresses.

Correct Answer: A

Reference: https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/885253/per-ip-traffic-shaper

QUESTION 14

Refer to the exhibit.



```
FortiGate # 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 two statements about the debug output are correct? (Choose two)

A. The debug output shows per-IP shaper values and real-time readings.

B. This traffic shaper drops traffic that exceeds the set limits.

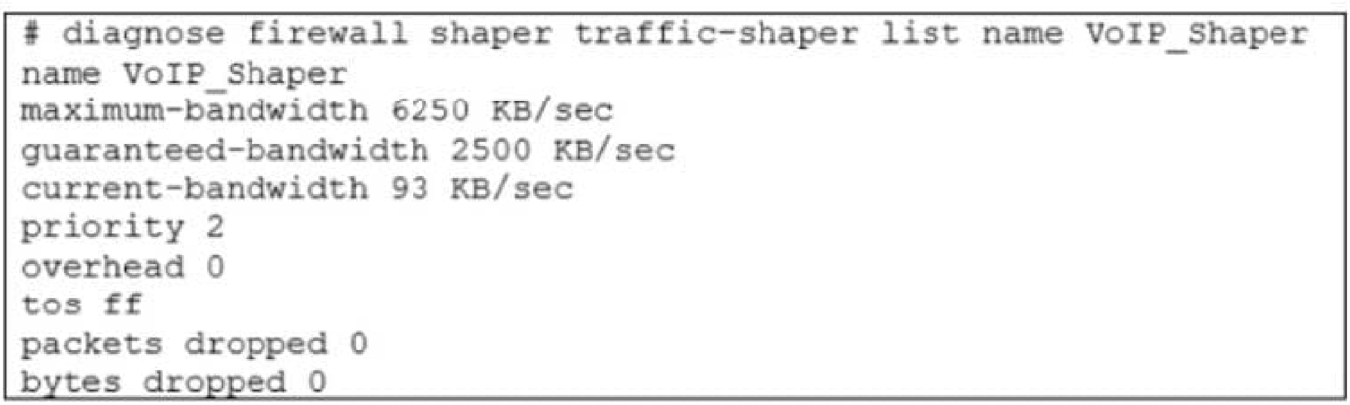
C. Traffic being controlled by the traffic shaper is under 1 Kbps.

D. FortiGate provides statistics and reading based on historical traffic logs.

Correct Answer: AB

QUESTION 15

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