Free Questions for NSE7_SDW-7.2 by dumpssheet

Shared by Dickson on 09-08-2024

For More Free Questions and Preparation Resources

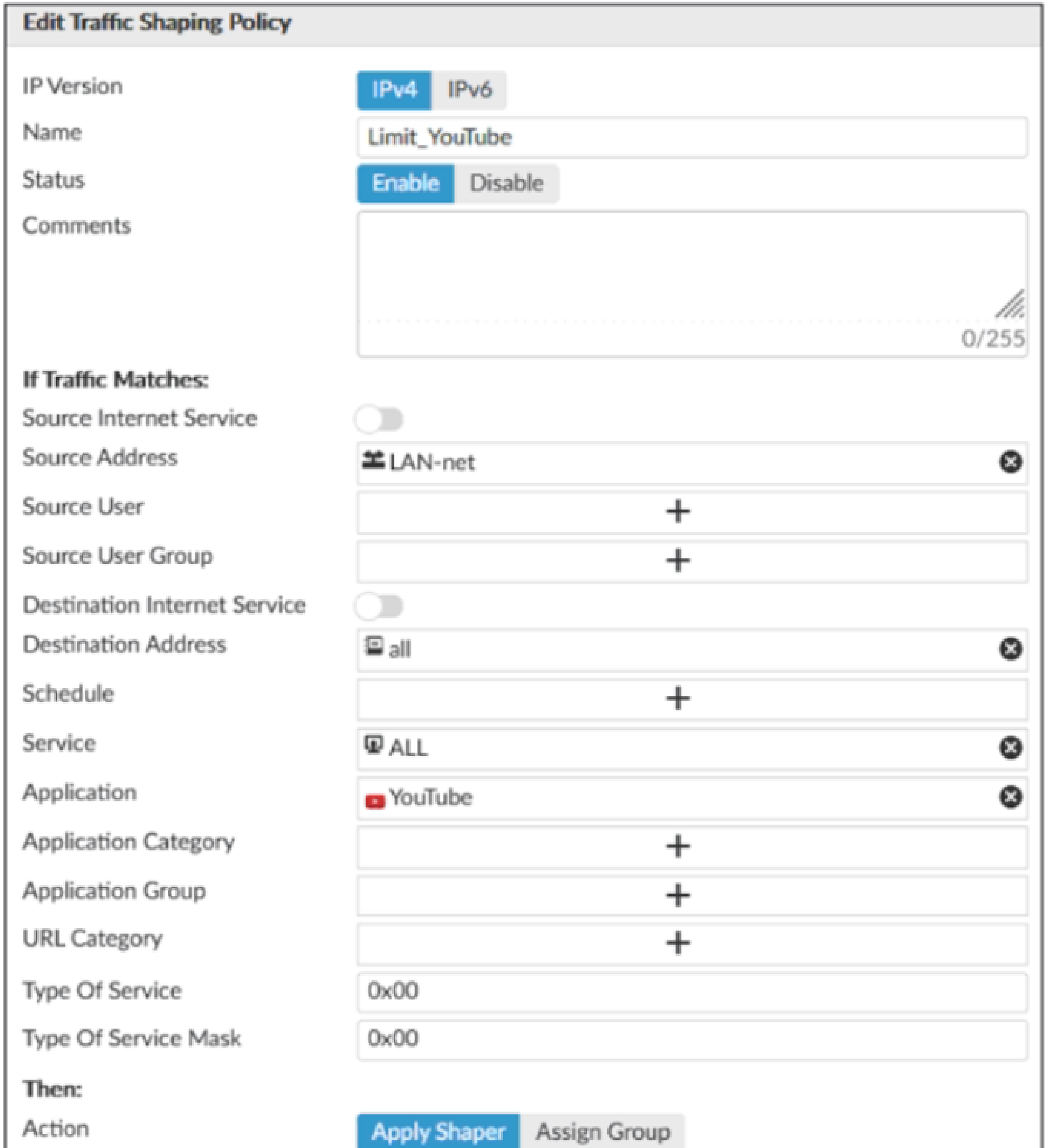
Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Refer to the exhibits.

Exhibit A -



Edit Traffic Shaping Policy

IP Version	[✓ IPv4] IPv6
Name	Limit_YouTube
Status	[✓ Enable] Disable
Comments	0/255

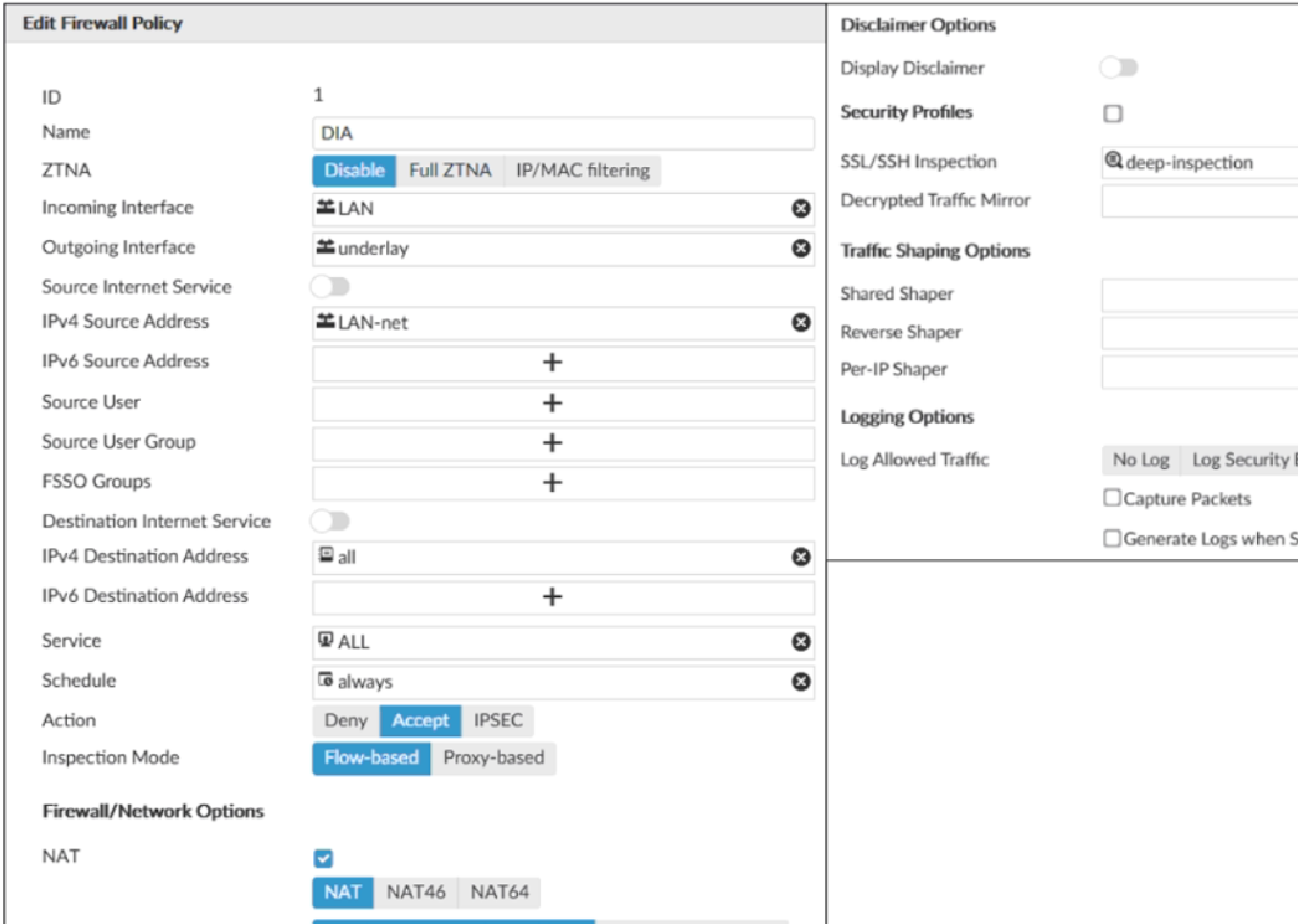
If Traffic Matches:

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

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

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 I
	□ Capture Packets
	□ Generate Logs when S

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?

Options:

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.

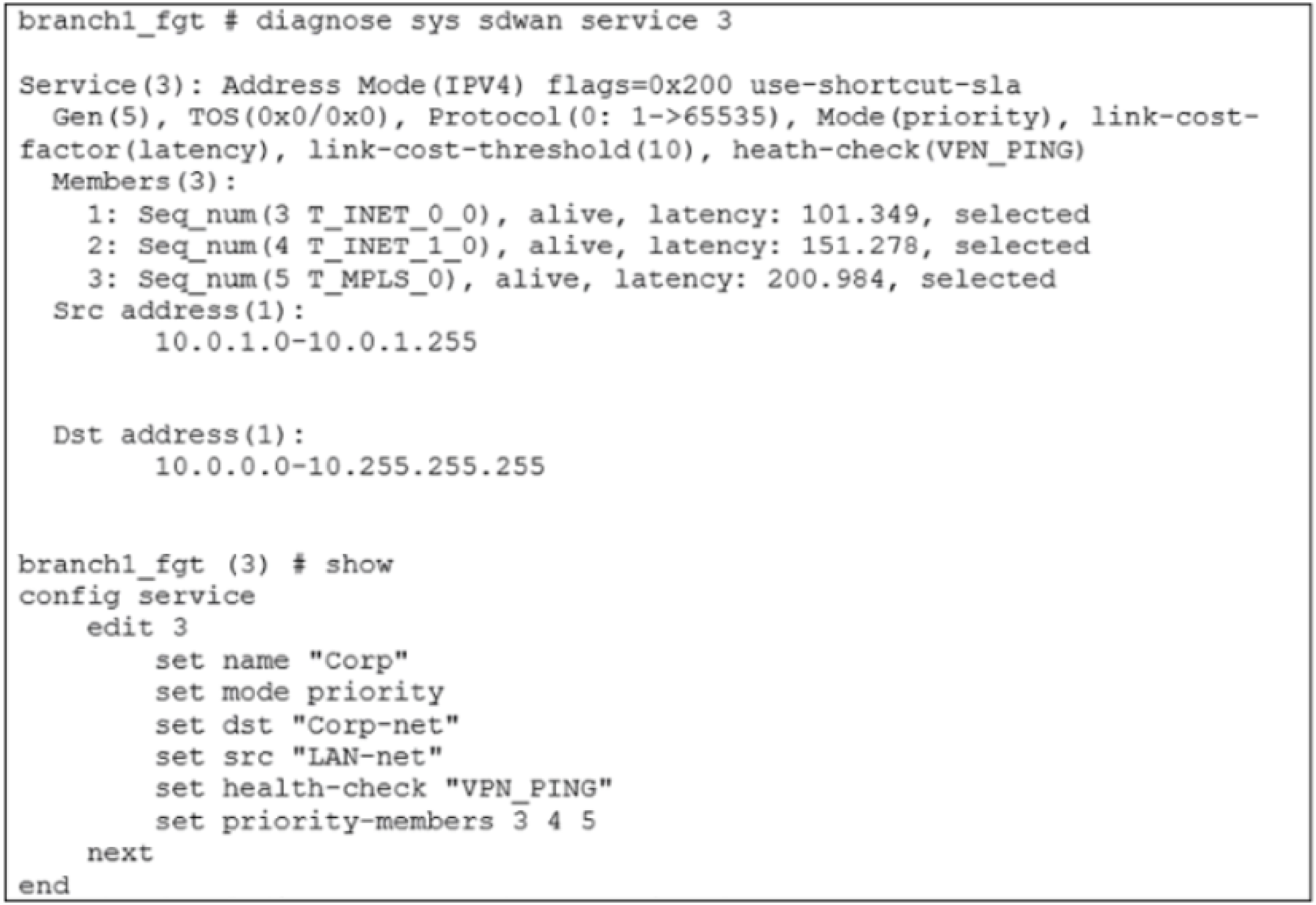
Answer:

C

Question 2

Question Type: **MultipleChoice**

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?

Options:

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.

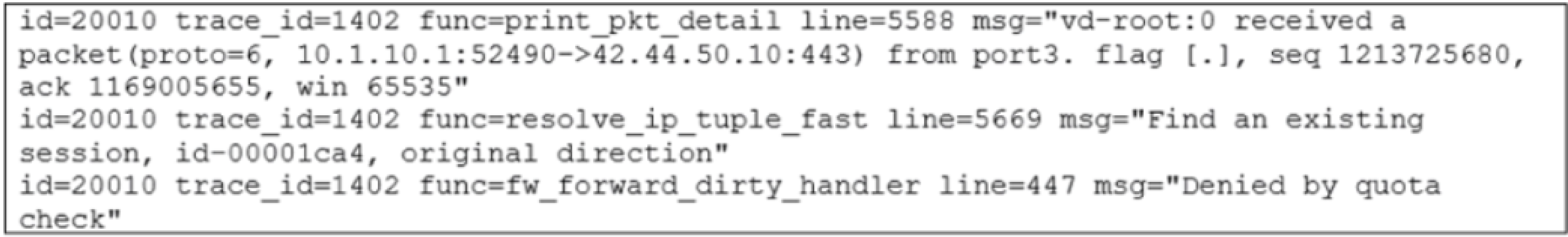
Answer:

D

Question 3

Question Type: **MultipleChoice**

Exhibit.



```
id=20010 trace_id=1402 func=print_pkt_detail line=5588 msg="vd-root:0 received a
packet(proto=6, 10.1.10.1:52490->42.44.50.10:443) from port3. flag [.], seq 1213725680,
ack 1169005655, win 65535"
id=20010 trace_id=1402 func=resolve_ip_tuple_fast line=5669 msg="Find an existing
session, id-00001ca4, original direction"
id=20010 trace_id=1402 func=fw_forward_dirty_handler line=447 msg="Denied by quota
check"
```

Which conclusion about the packet debug flow output is correct?

Options:

A- The total number of daily sessions for 10.1.10.1 exceeded the maximum number of concurrent sessions configured in the traffic shaper, and the packet was dropped.

B- The packet size exceeded the outgoing interface MTU.

C- The number of concurrent sessions for 10.1.10.1 exceeded the maximum number of concurrent sessions configured in the traffic shaper, and the packet was dropped.

D- The number of concurrent sessions for 10.1.10.1 exceeded the maximum number of concurrent sessions configured in the firewall policy, and the packet was dropped.

Answer:

C

Explanation:

In a Per-IP shaper configuration, if an IP address exceeds the configured concurrent session limit, the message 'Denied by quota check' appears. SD-WAN 7.0 Study Guide page 287

Question 4

Question Type: **MultipleChoice**

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

Options:

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:

A, C

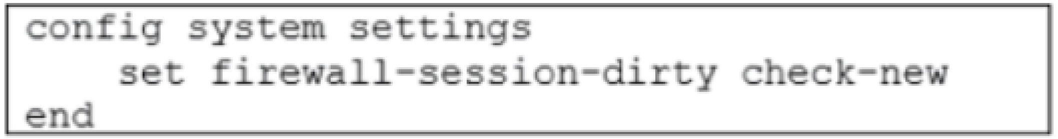
Explanation:

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

Question 5

Question Type: **MultipleChoice**

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.)

Options:

A- FortiGate flushes all sessions.

B- FortiGate terminates the old sessions.

C- FortiGate does not change existing sessions.

D- FortiGate evaluates new sessions.

Answer:

C, D

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.

Question 6

Question Type: MultipleChoice

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

Options:

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:

A, C

Explanation:

sdwan_service_id is 0 = match SD-WAN implicit rule, study guide 7.0 page 120, 7.2 page 149 SD-WAN rules internally are interpreted as a Policy route, so when the traffic doesn't match with any policy route, it will be flowing by implict policy.

Question 7

Question Type: **MultipleChoice**

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

Options:

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

Question 8

Question Type: **MultipleChoice**

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

Options:

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:

B, C

Question 9

Question Type: **MultipleChoice**

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

Options:

A- http

B- icmp

C- twamp

D- dns

Answer:

A, D

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.

Question 10

Question Type: MultipleChoice

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

Options:

A- Encapsulating Security Payload (ESP)

B- Secure Shell (SSH)

C- Internet Key Exchange (IKE)

D- Security Association (SA)

Answer:

A, C

Question 11

Question Type: **MultipleChoice**

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

Options:

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

B- Member metrics are measured only if an SLA target is configured

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

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

Answer:

A, D

20%
DISCOUNT