

Exam Questions NSE7_SDW-7.0

Fortinet NSE 7 - SD-WAN 7.0

https://www.2passeasy.com/dumps/NSE7_SDW-7.0/



NEW QUESTION 1

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 2

What is the route-tag setting in an SD-WAN rule used for?

- A. To indicate the routes for health check probes.
- B. To indicate the destination of a rule based on learned BGP prefixes.
- C. To indicate the routes that can be used for routing SD-WAN traffic.
- D. To indicate the members that can be used to route SD-WAN traffic.

Answer: B

NEW QUESTION 3

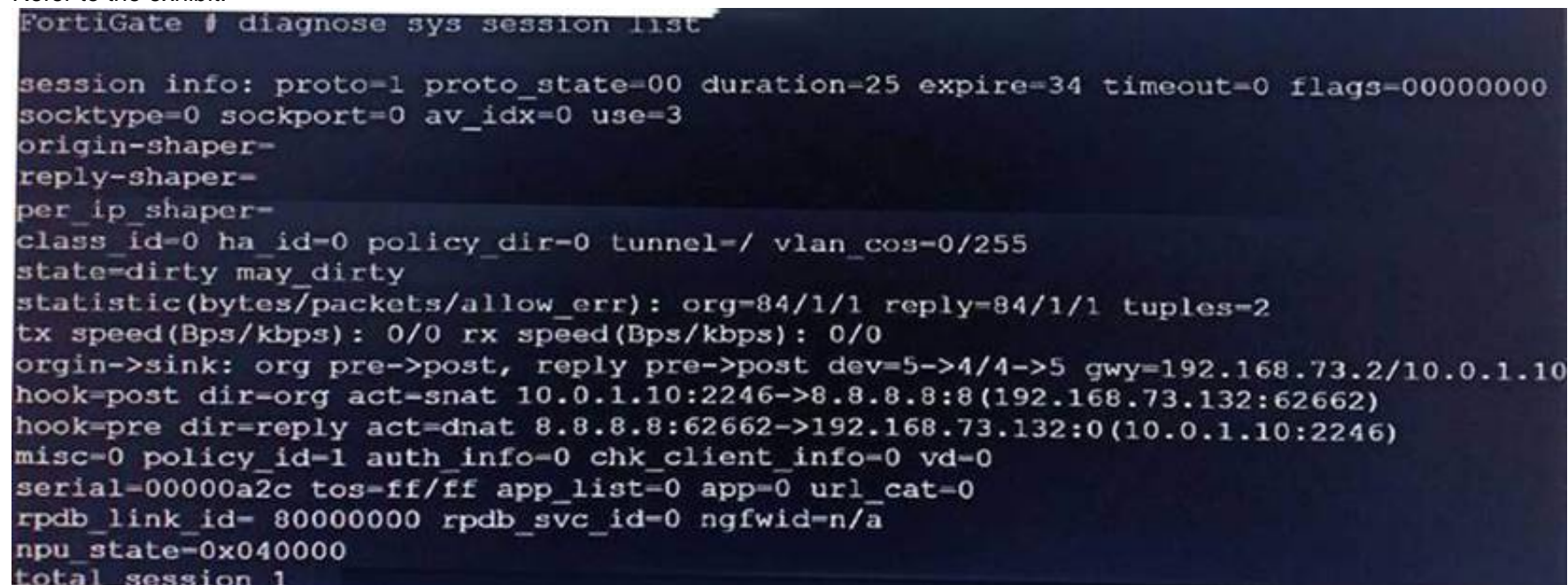
What is a benefit of using application steering in SD-WAN?

- 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 4

Refer to the exhibit.



```
FortiGate # diagnose sys session list

session info: proto=1 proto_state=00 duration=25 expire=34 timeout=0 flags=00000000
socktype=0 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=dirty may_dirty
statistic(bytes/packets/allow_err): org=84/1/1 reply=84/1/1 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
origin->sink: org pre->post, reply pre->post dev=5->4/4->5 gwy=192.168.73.2/10.0.1.10
hook=post dir=org act=snat 10.0.1.10:2246->8.8.8.8:8 (192.168.73.132:62662)
hook=pre dir=reply act=dnat 8.8.8.8:62662->192.168.73.132:0 (10.0.1.10:2246)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00000a2c tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id= 80000000 rpdb_svc_id=0 ngfwid=n/a
npu_state=0x040000
total session 1
```

Based on the exhibit, which statement about FortiGate re-evaluating traffic is true?

- A. The type of traffic defined and allowed on firewall policy ID 1 is UDP.
- B. FortiGate has terminated the session after a change on policy ID 1.
- C. Changes have been made on firewall policy ID 1 on FortiGate.
- D. Firewall policy ID 1 has source NAT disabled.

Answer: C

NEW QUESTION 5

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 6

Refer to the exhibit.

```
config system sdwan
  set fail-detect enable
  set fail-alert-interfaces "port5"
  config health-check
    edit "Level3_DNS"
      set update-cascade-interface enable
      set members 1 2
    next
    edit "HQ"
      set update-cascade-interface enable
      set members 3
    next
  end
end
```

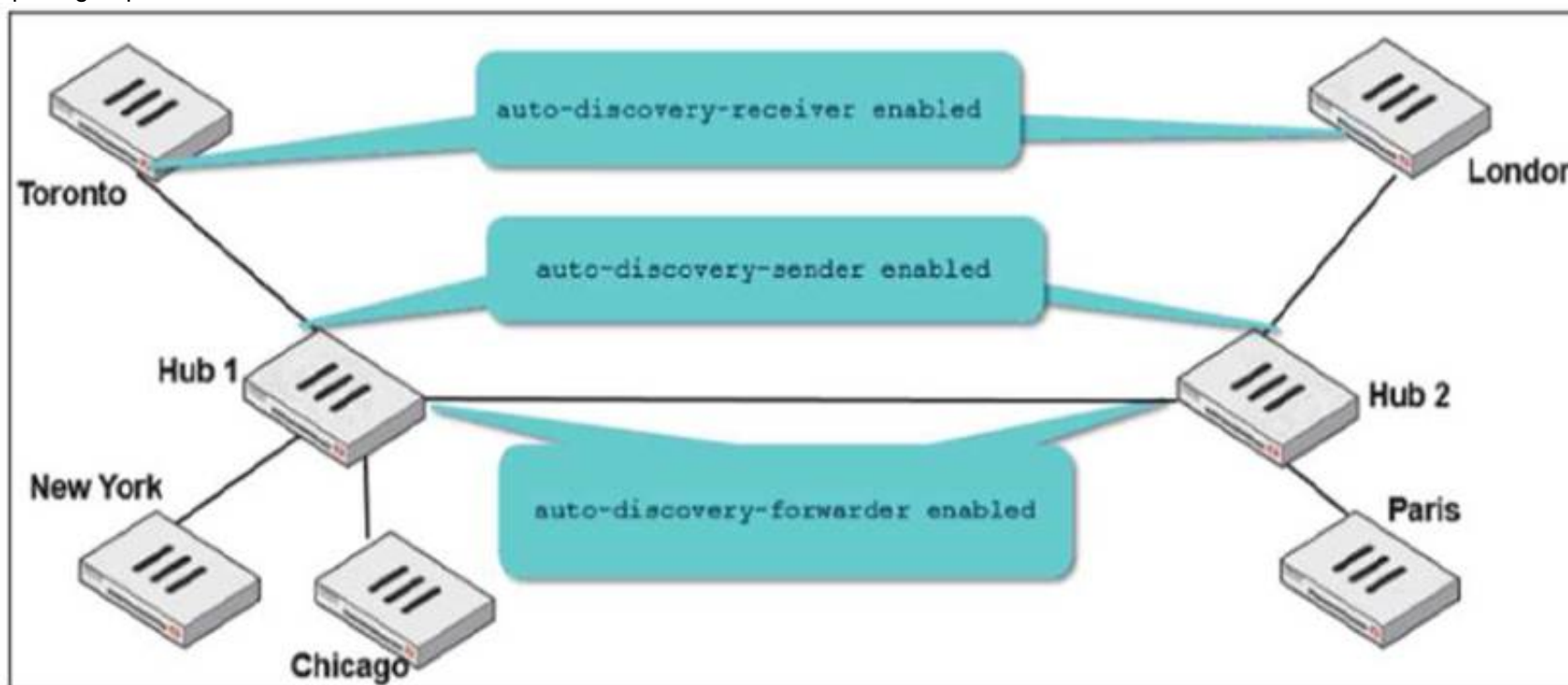
Based on the exhibit, which action does FortiGate take?

- A. FortiGate bounces port5 after it detects all SD-WAN members as dead.
- B. FortiGate fails over to the secondary device after it detects all SD-WAN members as dead.
- C. FortiGate brings up port5 after it detects all SD-WAN members as alive.
- D. FortiGate brings down port5 after it detects all SD-WAN members as dead.

Answer: B

NEW QUESTION 7

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 8

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 9

Which statement is correct about SD-WAN and ADVPN?

- A. Routes for ADVPN shortcuts must be manually configured.
- B. SD-WAN can steer traffic to ADVPN shortcuts, established over IPsec overlays, configured as SD-WAN members.
- C. SD-WAN does not monitor the health and performance of ADVPN shortcuts.
- D. You must use IKEv2 on IPsec tunnels.

Answer: B

NEW QUESTION 10

Refer to the exhibit.

```
# diagnose sys session list

session info: proto=6 proto_state=01 duration=39 expire=3593 timeout=3600 flags=00000000
socktype=0 sockport=0 av_idx=0 use=4
state=may_dirty npu
origin->sink: org pre->post, reply pre->post dev=7->5/5->7 gwy=10.10.10.1/10.9.31.160
hook=pre dir=org act=noop 10.9.31.160:7932->10.0.1.7:22(0.0.0.0:0)
hook=post dir=reply act=noop 10.0.1.7:22->10.9.31.160:7932(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00045e02 tos=ff/ff app_list=0 app=0 url_cat=0
sdwan_mbr_seq=1 sdwan_service_id=1
rpd_b_link_id=800000000 rpd_b_svc_id=0 ngfwid=n/a
npu_state=0x4000c00
npu info: flag=0x81/0x81, offload=8/8, ips_offload=0/0, epid=64/76, ipid=76/64,
vlan=0x0000/0x0000
vlifid=76/64, vtag_in=0x0000/0x0000 in_npu=1/1, out_npu=1/1, fwd_en=0/0, qid=2/2
reflect info 0:
dev=7->6/6->7
npu_state=0x4000800
npu info: flag=0x00/0x81, offload=0/8, ips_offload=0/0, epid=0/76, ipid=0/65, vlan=0x0000/0x0000
vlifid=0/65, vtag_in=0x0000/0x0000 in_npu=0/1, out_npu=0/1, fwd_en=0/0, qid=0/2
total reflect session num: 1
total session 1

# diagnose netlink interface list

if=port1 family=00 type=1 index=5 mtu=1500 link=0 master=0
if=port2 family=00 type=1 index=6 mtu=1500 link=0 master=0
if=port3 family=00 type=1 index=7 mtu=1500 link=0 master=0
```

The exhibit shows the details of a session and the index numbers of some relevant interfaces on a FortiGate appliance that supports hardware offloading. Based on the information shown in the exhibits, which two statements about the session are true? (Choose two.)

- A. The reply direction of the asymmetric traffic flows from port2 to port3.
- B. The auxiliary session can be offloaded to hardware.
- C. The original direction of the symmetric traffic flows from port3 to port2.
- D. The main session cannot be offloaded to hardware.

Answer: AB

NEW QUESTION 10

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 12

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 17

Refer to the exhibits.

Exhibit A

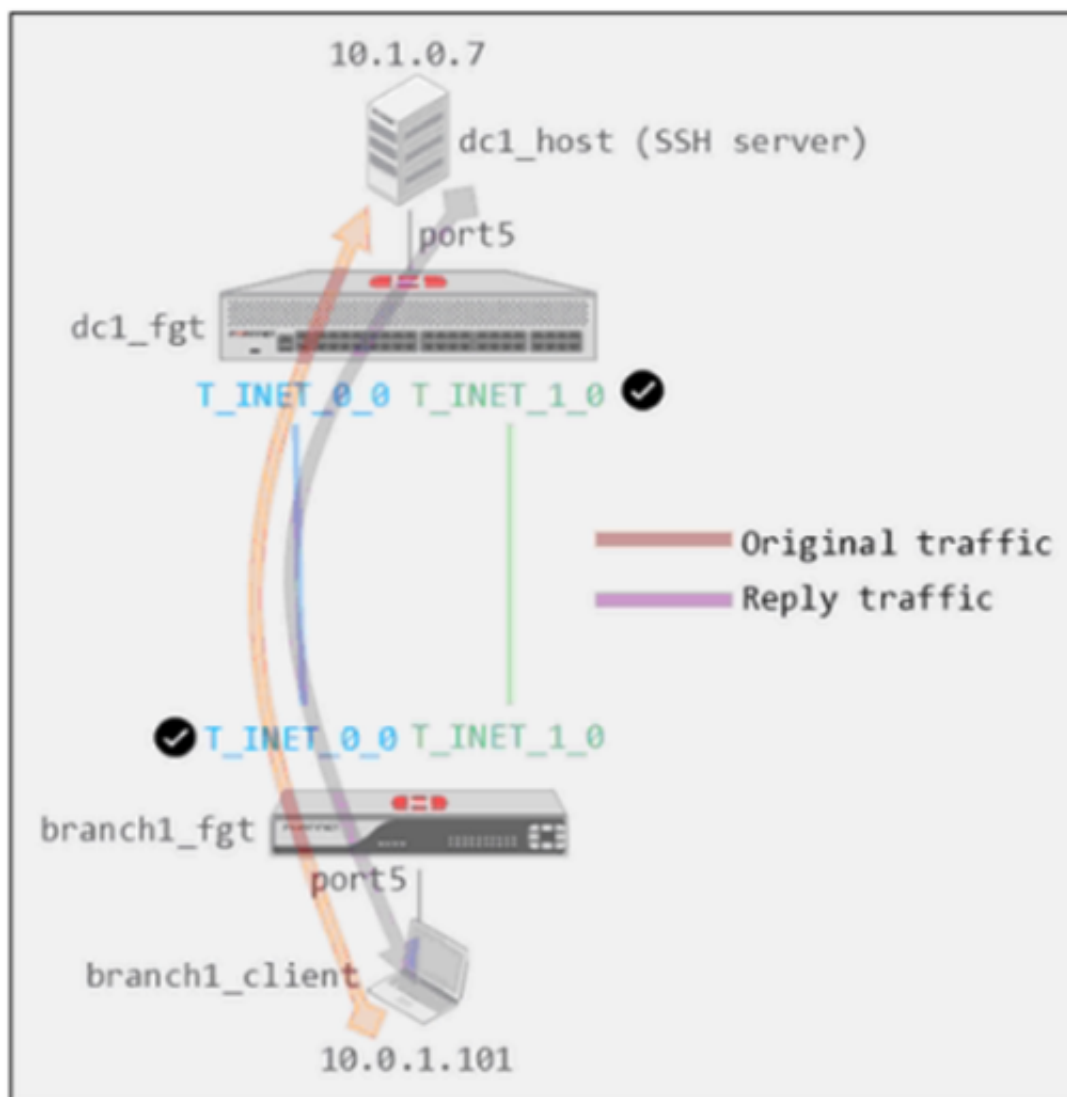


Exhibit B

```
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 preferred member 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.

Answer: A

Explanation:

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>

NEW QUESTION 20

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

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

Passing Certification Exams Made Easy

visit - <https://www.2PassEasy.com>

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.

Answer: B

NEW QUESTION 23

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual NSE7_SDW-7.0 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the NSE7_SDW-7.0 Product From:

https://www.2passeasy.com/dumps/NSE7_SDW-7.0/

Money Back Guarantee

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