Fortinet

Exam Questions NSE7_SDW-7.2

Fortinet NSE 7 - SD-WAN 7.2

NEW QUESTION 1
What are two reasons for using FortiManager to organize and manage the network for a group of FortiGate devices? (Choose two.)

A. It simplifies the deployment and administration of SD-WAN on managed FortiGate devices.
B. It improves SD-WAN performance on the managed FortiGate devices.
C. It sends probe signals as health checks to the beacon servers on behalf of FortiGate.
D. It acts as a policy compliance entity to review all managed FortiGate devices.
E. It reduces WAN usage on FortiGate devices by acting as a local FortiGuard server.

Answer: AE

NEW QUESTION 2
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 3
Which are two benefits of using CLI templates in FortiManager? (Choose two.)

A. You can reference meta fields.
B. You can configure interfaces as SD-WAN members without having to remove references first.
C. You can configure FortiManager to sync local configuration changes made on the managed device, to the CLI template.
D. You can configure advanced CLI settings.

Answer: AD

NEW QUESTION 4
Which two statements about SD-WAN central management are true? (Choose two.)

A. It does not allow you to monitor the status of SD-WAN members.
B. It is enabled or disabled on a per-ADOM basis.
C. It is enabled by default.
D. It uses templates to configure SD-WAN on managed devices.

Answer: BD

NEW QUESTION 5
Refer to the exhibit.

Exhibit A

```
fgt # show vpn ipsec phase1-interface T_INET_1
config vpn ipsec phase1-interface
        edit "T_INET_1"
            set type dynamic
            set interface "port2"
            set ike-version 2
            set keylife 28800
            set peertype any
            set net-device disable
            set proposal aes128-sha256
            set add-route disable
            set auto-discovery-sender enable
            set psksecret ENC MXtFGKOxLV+x4p3e9Xq2HGJoU+QOgg5YMqiXb2T73fZpSXS/
            jv9oshNeQiNEjOJEtuqqD8mAw7G2ZLTlsR3/ihAaAY4tvjveS+9CuTn00J2tuddoM9
            uz4vaBTNbNrh3/KhbJytsCag==
        next
end
```

Exhibit B

```
fgt # diag vpn tunnel list name T_INET_1_0
list ipsec tunnel by names in vd 0
------------------------------------------------------
name=T_INET_1_0 ver=2 serial=a 100.64.1.9:0->192.2.0.9:0 tun_id=192.2.0.9 tun_id6=::10.0.0.10
dst_mtu=0 dpd-link=on weight=1
bound_if=4 lgwy=static/1 tun=intf mode=dial_inst/3 encap=none/74408 options[122a8]=npu rgwy-chg
frag-rfc run_state=0 role=primary acc
ept_traffic=1 overlay_id=0
parent=T_INET_1 index=0
proxyid_num=1 child_num=0 refcnt=6 ilast=0 olast=42955943 ad=/0
stat: rxp=32 txp=0 rxb=1280 txb=0
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
fec: egress=0 ingress=0
proxyid=T_INET_1_0 proto=0 sa=1 ref=2 serial=1
src: 0:0.0.0.0-255.255.255.255:0
dst: 0:10.0.1.0-10.0.1.255:0
SA: ref=3 options=20603 type=00 soft=0 mtu=1280 expire=1774/0B replaywin=2048
seqno=1 esn=0 replaywin_lastseq=00000021 qat=0 rekey=0 hash_search_len=1
life: type=01 bytes=0/0 timeout=1791/1800
dec: spi=7c176e24 esp=aes key=16 8547efb42d148c6692fb2af0d01ff12d
ah=sha1 key=20 f0d3ac8192d2e79fbbe29162f9ccf406f1a161b5
enc: spi=809f9d49 esp=aes key=16 cb67f6d5f6a1f9fe5ab38b953dd4782f
ah=sha1 key=20 d0182dfe827a4785d9493d46e3907d49465391fb
dec:pkts/bytes=64/2560, enc:pkts/bytes=0/0
npu_flag=00 npu_rgwy=192.2.0.9 npu_lgwy=100.64.1.9 npu_selid=6 dec_npuid=0 enc_npuid=0
```

Which two statements about the IPsec VPN configuration and the status of the IPsec VPN tunnel are true? (Choose two.)

A. FortiGate does not install IPsec static routes for remote protected networks in the routing tabl
B. Most Voted
C. The phase 1 configuration supports the network-overlay settin
D. Most Voted
E. FortiGate facilitated the negotiation of the T_INET_1_0_0 ADVPN shortcut over T_INET_1_0.
F. Dead peer detection is disabled.

Answer: AC

NEW QUESTION 6
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.)

A. FortiGate flushes all sessions.
B. FortiGate terminates the old sessions.
C. FortiGate does not change existing sessions.
D. FortiGate evaluates new sessions.

Answer: CD

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.

NEW QUESTION 7
Refer to the exhibit.

```
config firewall policy
    edit 1
        set anti-replay disable
    next
end
```

In a dual-hub hub-and-spoke SD-WAN deployment, which is a benefit of disabling the anti- replay setting on the hubs?

A. It instructs the hub to disable the reordering of TCP packets on behalf of the receiver, to improve performance.
B. It instructs the hub to disable TCP sequence number check, which is required for TCP sessions originated from spokes to fail over back and forth between the hubs.
C. It instructs the hub to not check the ESP sequence numbers on IPsec traffic, to improve performance.

D. It instructs the hub to skip content inspection on TCP traffic, to improve performance.

Answer: B

NEW QUESTION 8
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
orgin->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
rpdb_link_id=80000000 rpdb_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 9
Which two conclusions for traffic that matches the traffic shaper are true? (Choose two.)

```
# 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
```

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: BC

NEW QUESTION 10
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 10
Which SD-WAN setting enables FortiGate to delay the recovery of ADVPN shortcuts?

A. hold-down-time
B. link-down-failover
C. auto-discovery-shortcuts
D. idle-timeout

Answer: A

NEW QUESTION 13
Exhibit.

```
7: […]logid="0101037141" type="event" subtype="vpn" level="notice" vd="root" logdesc="IPsec tunnel
statistics" msg="IPsec tunnel statistics" action="tunnel-stats" remip=100.64.1.9 locip=192.2.0.9
remport=500 locport=500 outintf="port2" cookies="773c72b48060051d/529ac435532959b6" user="N/A"
group="N/A" useralt="N/A" xauthuser="N/A" xauthgroup="N/A" assignip=10.202.1.1
vpntunnel="T_INET_1" tunnelip=N/A tunnelid=2595348112 tunneltype="ipsec" duration=3581
sentbyte=386431 rcvdbyte=387326 nextstat=600 advpnsc=0

8: […]logid="0101037141" type="event" subtype="vpn" level="notice" vd="root" logdesc="IPsec tunnel
statistics" msg="IPsec tunnel statistics" action="tunnel-stats" remip=172.16.0.9 locip=172.16.0.1
remport=500 locport=500 outintf="port4" cookies="0624890597f0096d/ed1bd5247375c46f" user="N/A"
group="N/A" useralt="N/A" xauthuser="N/A" xauthgroup="N/A" assignip=N/A vpntunnel="T_MPLS_0"
tunnelip=0.0.0.0 tunnelid=2595348102 tunneltype="ipsec" duration=223 sentbyte=115040
rcvdbyte=345160 nextstat=600 advpnsc=1

9: […]logid="0101037141" type="event" subtype="vpn" level="notice" vd="root" logdesc="IPsec tunnel
statistics" msg="IPsec tunnel statistics" action="tunnel-stats" remip=100.64.1.1 locip=192.2.0.1
remport=500 locport=500 outintf="port1" cookies="747b432459497188/6616a969a6937853" user="N/A"
group="N/A" useralt="N/A" xauthuser="N/A" xauthgroup="N/A" assignip=10.201.1.1
vpntunnel="T_INET_0" tunnelip=N/A tunnelid=2595348115 tunneltype="ipsec" duration=3580
sentbyte=388020 rcvdbyte=387994 nextstat=600 advpnsc=0
```

The exhibit shows VPN event logs on FortiGate. In the output shown in the exhibit, which statement is true?

A. There are no IPsec tunnel statistics log messages for ADVPN cuts.
B. There is one shortcut tunnel built from master tunnel T_MPLS_0.
C. The VPN tunnel T_MPLS_0 is a shortcut tunnel.
D. The master tunnel T_INET_0 cannot accept the ADVPN shortcut.

Answer: B

Explanation:
VPN event logs record the status of VPN tunnels, such as the establishment, termination, or failure of a tunnel. The output includes the following information:
? logid: the log ID number
? type: the log type, either traffic or event
? subtype: the log subtype, either vpn or ipsec
? level: the log level, either error, warning, or notice
? vd: the virtual domain name
? logdesc: the log description
? msg: the log message
? action: the log action, such as tunnel-up, tunnel-down, or tunnel-stats
? remip: the remote IP address
? locip: the local IP address
? remport: the remote port number
? locport: the local port number
? outintf: the outgoing interface name
? cookies: the IKE SA cookies
? user: the user name
? group: the user group name
? useralt: the alternative user name
? xauthuser: the XAuth user name
? authgroup: the XAuth user group name
? assignip: the assigned IP address
? vpntunnel: the VPN tunnel name
? tunnellip: the tunnel loopback IP address
? tunnelid: the tunnel ID number
? tunneltype: the tunnel type, either ipsec or ssl
? duration: the tunnel duration in seconds
? sentbyte: the number of bytes sent
? rcvdbyte: the number of bytes received
? nextstat: the next statistics interval in seconds
? advpnsc: the ADVPN shortcut flag, either 0 or 1 Based on the exhibit, the following statement is true:
? There is one shortcut tunnel built from master tunnel T_MPLS_0. This means that the VPN tunnel T_MPLS_0 is a master tunnel that can send ADVPN shortcut offers to other spokes, and the VPN tunnel T_MPLS_0_0 is a shortcut tunnel that is built from the master tunnel T_MPLS_01. In the exhibit, the log action for T_MPLS_0 is tunnel-up, and the log action for T_MPLS_0_0 is shortcut-up. The advpnsc flag for T_MPLS_0 is 0, indicating that it is not a shortcut tunnel, while the advpnsc flag for T_MPLS_0_0 is 1, indicating that it is a shortcut tunnel.

NEW QUESTION 14
Refer to the exhibits. Exhibit A -

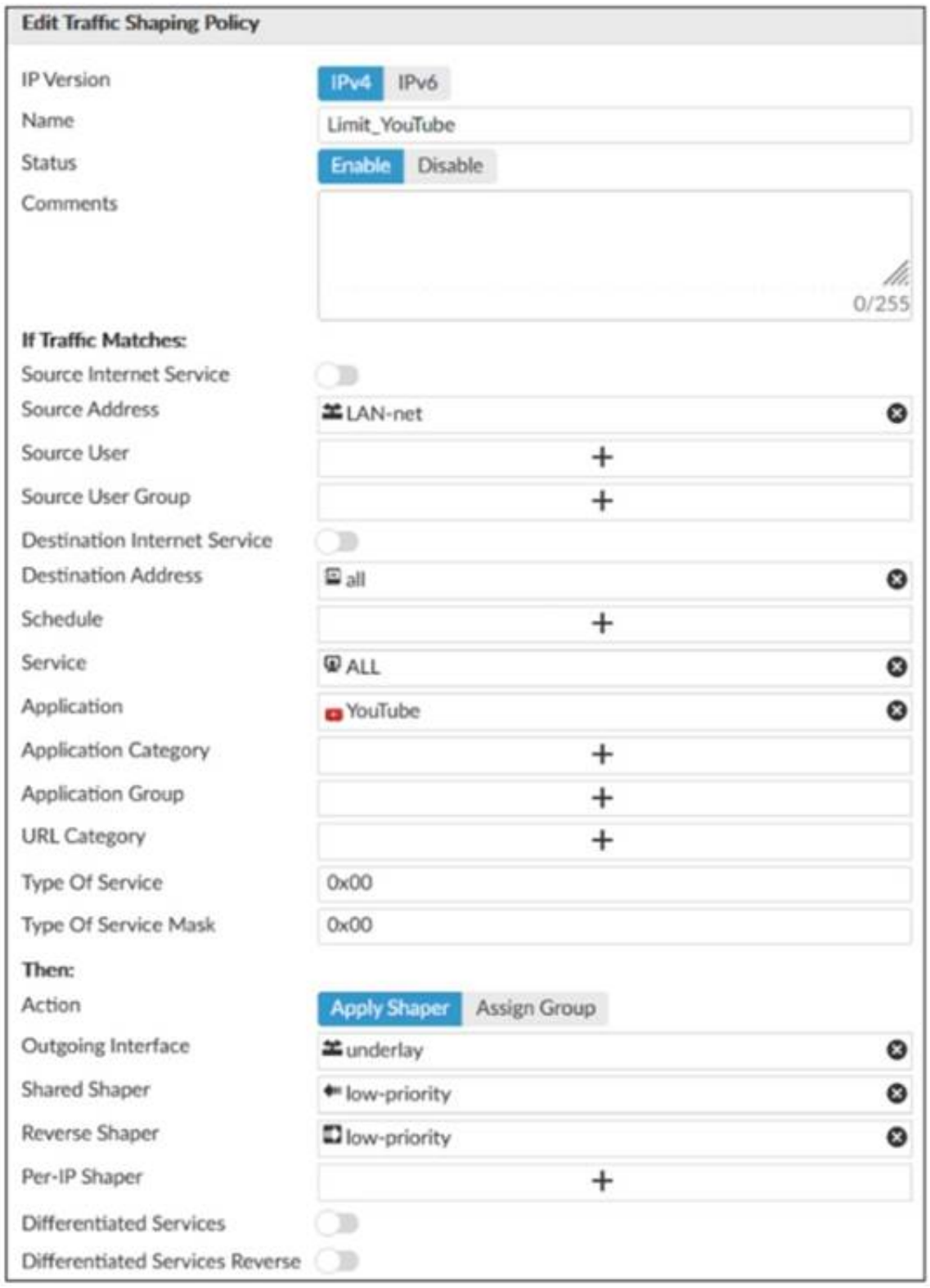


Exhibit B -

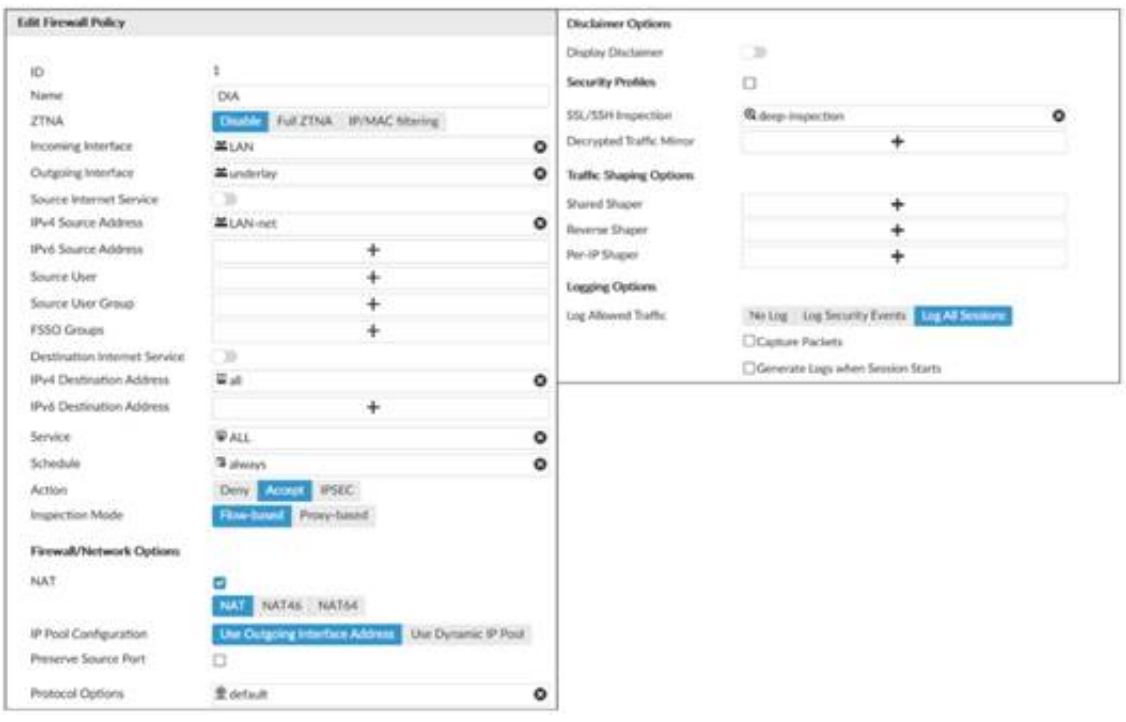


Exhibit A shows the traffic shaping policy and exhibit B shows the firewall policy.
The administrator wants FortiGate to limit the bandwidth used by YouTube. When testing, the administrator determines that FortiGate does not apply traffic shaping on YouTube traffic.
Based on the policies shown in the 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: C

NEW QUESTION 18
Refer to the exhibit.

```
config system virtual-wan-link
    set status enable
    set load-balance-mode source-ip-based
    config members
        edit 1
                    set interface "port1"
                    set gateway 100.64.1.254
                    set source 100.64.1.1
                    set cost 15
        next
        edit 2
                    set interface "port2"
                    set gateway 100.64.2.254
                    set priority 10
        next
    end
end
```

Based on the output shown in the exhibit, which two criteria on the SD-WAN member configuration can be used to select an outgoing interface in an SD-WAN rule? (Choose two.)

A. Set priority 10.
B. Set cost 15.
C. Set load-balance-mode source-ip-ip-based.
D. Set source 100.64.1.1.

Answer: AB

NEW QUESTION 21
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 7.2, 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 23
Which two statements about SD-WAN central management are true? (Choose two.)

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: AC

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

NEW QUESTION 27
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: A

NEW QUESTION 31
Refer to the exhibit.

```
config router bgp
    set as 65000
    set router-id 10.1.0.1
    set ibgp-multipath enable
    set additional-path enable
    set additional-path-select 3
    config neighbor-group
        edit "Branches_INET_0"
            set interface "T_INET_0_0"
            set remote-as 65000
            set update-source "T_INET_0_0"
        next
        edit "Branches_INET_1"
            set interface "T_INET_1_0"
            set remote-as 65000
            set update-source "T_INET_1_0"
        next
        edit "Branches_MPLS"
            set interface "T_MPLS_0"
            set remote-as 65000
            set update-source "T_MPLS_0"
        next
    end
    config neighbor-range
        edit 1
            set prefix 10.201.1.0 255.255.255.0
            set neighbor-group "Branches_INET_0"
        next
        edit 2
            set prefix 10.202.1.0 255.255.255.0
            set neighbor-group "Branches_INET_1"
        next
        edit 3
            set prefix 10.203.1.0 255.255.255.0
            set neighbor-group "Branches_MPLS"
        next
    end
...
end
```

The exhibit shows the BGP configuration on the hub in a hub-and-spoke topology. The administrator wants BGP to advertise prefixes from spokes to other spokes over the IPsec overlays, including additional paths. However, when looking at the spoke routing table, the administrator does not see the prefixes from other spokes and the additional paths.
Based on the exhibit, which three settings must the administrator configure inside each BGP neighbor group so spokes can learn other spokes prefixes and their additional paths? (Choose three.)

A. Set additional-path to send
B. Enable route-reflector-client
C. Set advertisement-interval to the number of additional paths to advertise
D. Set adv-additional-path to the number of additional paths to advertise
E. Enable soft-reconfiguration

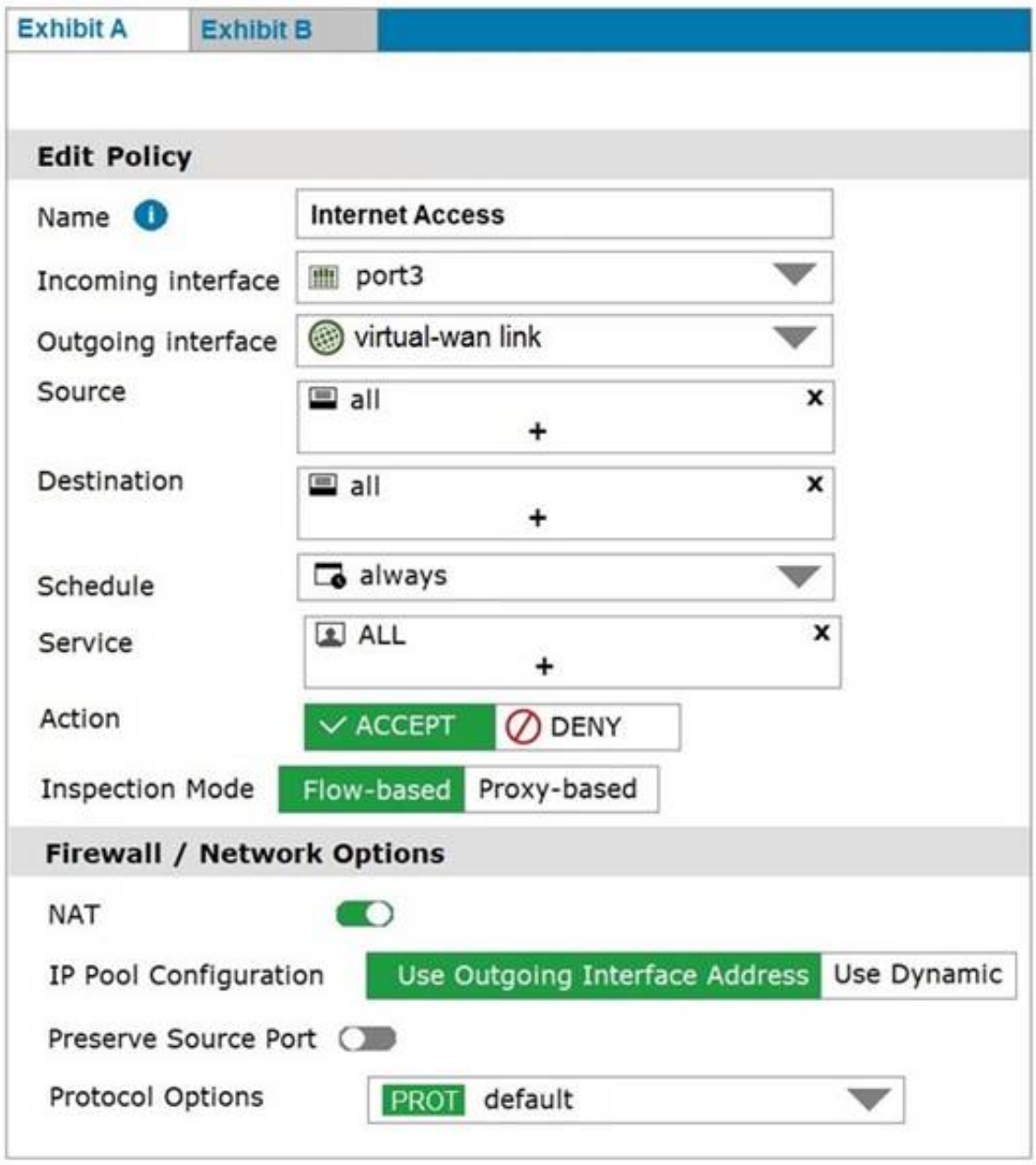
Answer: ABD

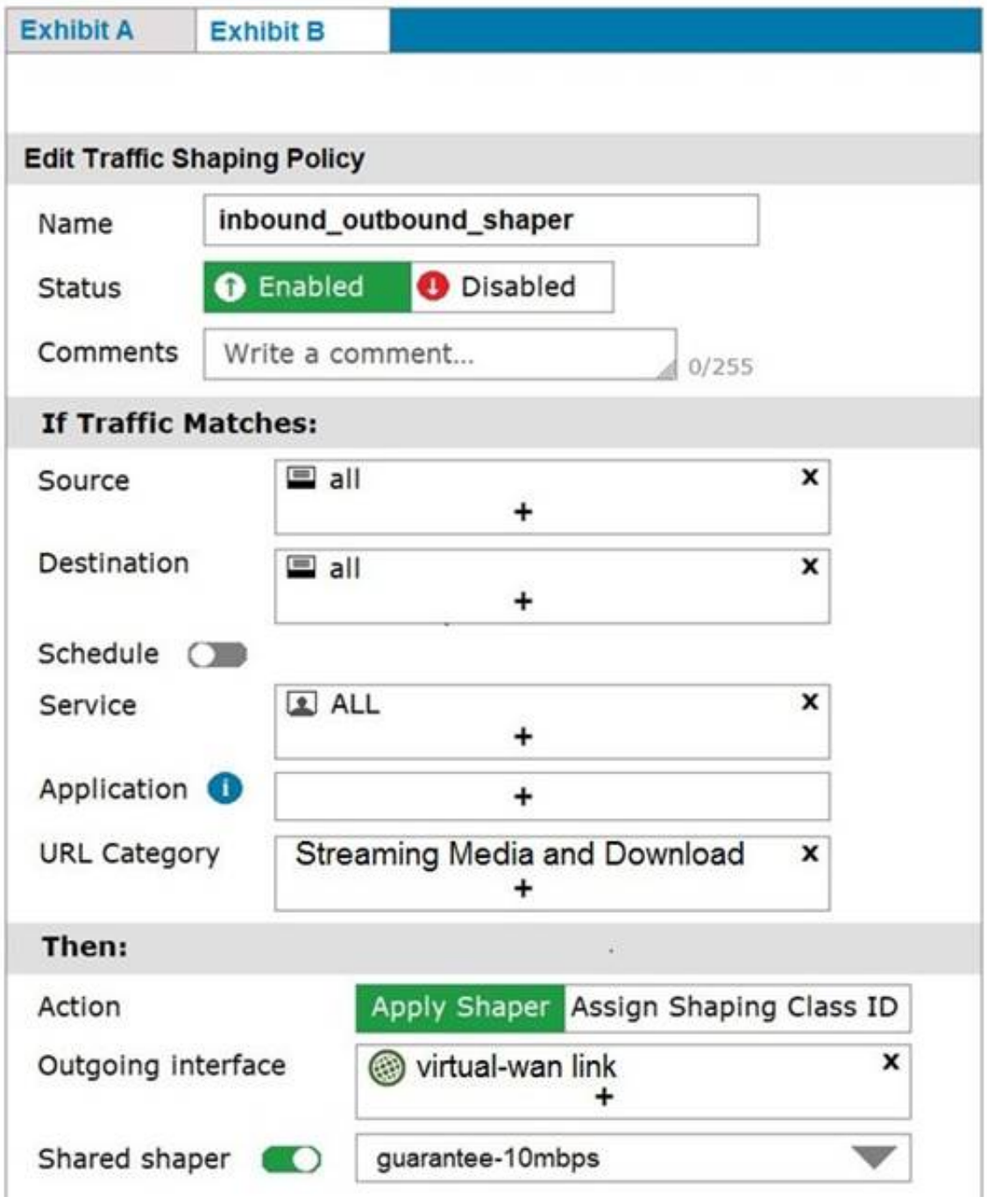
NEW QUESTION 35
What is the route-tag setting in an SD-WAN rule used for?

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 38
Exhibit A shows the firewall policy and exhibit B shows the traffic shaping policy.



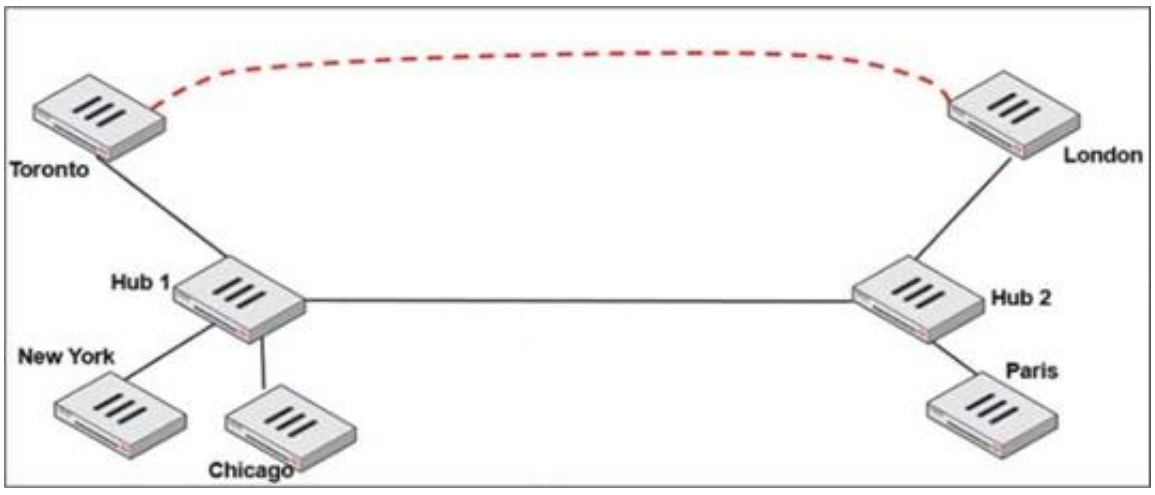


The traffic shaping policy is being applied to all outbound traffic; however, inbound traffic is not being evaluated by the shaping policy.
Based on the exhibits, what configuration change must be made in which policy so that traffic shaping can be applied to inbound traffic?

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.

Answer: D

NEW QUESTION 41
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 46
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?

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

NEW QUESTION 48
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 49
Which two interfaces are considered overlay links? (Choose two.)

A. LAG
B. IPsec
C. Physical
D. GRE

Answer: BD

NEW QUESTION 50
Which are three key routing principles in SD-WAN? (Choose three.)

A. FortiGate performs route lookups for new sessions only.
B. Regular policy routes have precedence over SD-WAN rules.
C. SD-WAN rules have precedence over ISDB routes.
D. By default, SD-WAN members are skipped if they do not have a valid route to thedestination.
E. By default, SD-WAN rules are skipped if the best route to the destination is not an SD- WAN member.

Answer: BDE

Explanation:
Study Guide 7.2, pages 125, 129, 151

NEW QUESTION 54
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 58

.....

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-7.2 Practice Exam Features:

* NSE7_SDW-7.2 Questions and Answers Updated Frequently

* NSE7_SDW-7.2 Practice Questions Verified by Expert Senior Certified Staff

* NSE7_SDW-7.2 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* NSE7_SDW-7.2 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year