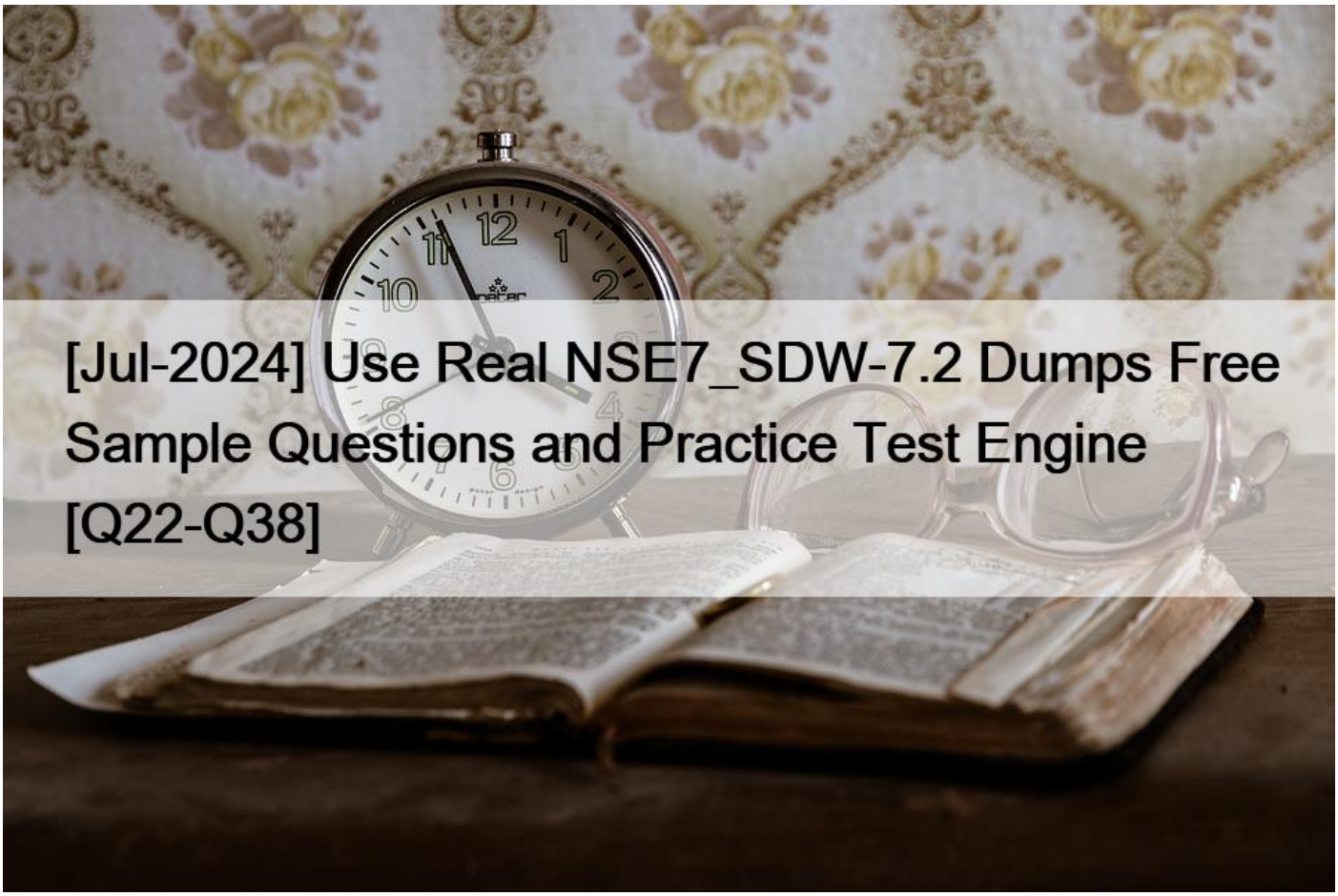
[Jul-2024 Use Real NSE7_SDW-7.2 Dumps Free Sample Questions and Practice Test Engine [Q22-Q38



[Jul-2024] Use Real NSE7_SDW-7.2 Dumps Free Sample Questions and Practice Test Engine
Pass Fortinet NSE7_SDW-7.2 exam - questions - convert Tets Engine to PDF

NO.22 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)
```

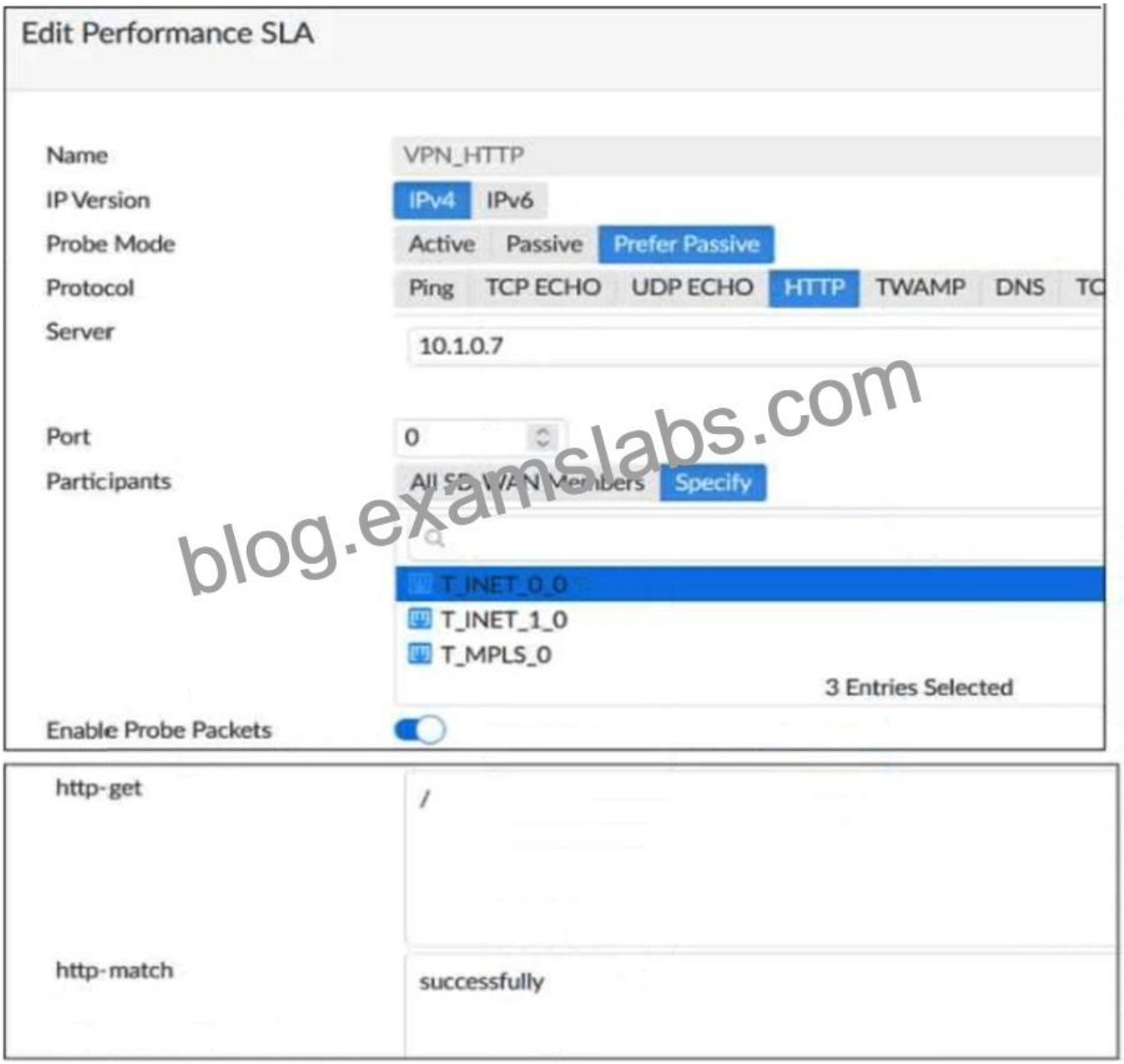
Exhibit A shows the SD-WAN performance SLA configuration, the SD-WAN rule configuration, and the application IDs of Facebook and YouTube. Exhibit B shows the firewall policy configuration and the underlay zone status.

Based on the exhibits, which two statements are correct about the health and performance of port1 and port2? (Choose two.)
* The performance is an average of the metrics measured for Facebook and YouTube traffic passing through the member.
* FortiGate is unable to measure jitter and packet loss on Facebook and YouTube traffic.
* FortiGate identifies the member as dead when there is no Facebook and YouTube traffic passing through the member.
* Non-TCP Facebook and YouTube traffic are not used for performance measurement.

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.

NO.23 Which two statements describe how IPsec phase 1 main mode is different from aggressive mode when performing IKE negotiation? (Choose two)
* A peer ID is included in the first packet from the initiator, along with suggested security policies.
* XAuth is enabled as an additional level of authentication, which requires a username and password.
* A total of six packets are exchanged between an initiator and a responder instead of three packets.
* The use of Diffie Hellman keys is limited by the responder and needs initiator acceptance.

NO.24 Refer to the exhibit.



Based on the exhibit, which two statements are correct about the health of the selected members? (Choose two.)

* After FortiGate switches to active mode, FortiGate never fails back to passive monitoring.
* During passive monitoring, FortiGate can’t detect dead members.
* FortiGate can offload the traffic that is subject to passive monitoring to hardware.
* FortiGate passively monitors the member if TCP traffic is passing through the member.

NO.25 Refer to the exhibits.

Exhibit A

```
branch1_fgt # diagnose sys sdwan service 1

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
  Gen(8), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(manual)
  Service disabled caused by no destination.
  Members(2):
    1: Seq_num(4 T_INET_1_0), alive, selected
    2: Seq_num(5 T_MPLS_0), alive, selected
  Src address(1):
        10.0.1.0-10.0.1.255

branch1_fgt # get router info bgp community 65000:10
VRF 0 BGP table version is 3, local router ID is 10.0.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight RouteTag Path
*>i10.1.0.0/24      10.202.1.254             0    100      0        1 i <-/1>
* i                 10.203.1.254             0    100      0        1 i <-/->

Total number of prefixes 1
```

Exhibit B

```
branch1_fgt (1) # show
config service
    edit 1
        set name "Corp"
        set route-tag 10
        set src "LAN-net"
        set priority-zone "overlay"
    next
end

config router bgp
...
    config neighbor
        edit "10.202.1.254"
            set soft-reconfiguration enable
            set interface "T_INET_1_0"
            set remote-as 65000
            set route-map-in "dc1-lan-rm"
            set update-source "T_INET_1_0"
        next
        edit "10.203.1.254"
            set soft-reconfiguration enable
            set interface "T_MPLS_0"
            set remote-as 65000
            set route-map-in "dc1-lan-rm"
            set update-source "T_MPLS_0"
        next
    end
...
config router route-map
    edit "dc1-lan-rm"
        config rule
            edit 1
                set match-community "dc1-lan-c1"
                set set-route-tag 1
            next
        end
    next
end
```

Exhibit A shows the SD-WAN rule status and the learned BGP routes with community 65000:10.

Exhibit B shows the SD-WAN rule configuration, the BGP neighbor configuration, and the route map

configuration.

The administrator wants to steer corporate traffic using routes tags in the SD-WAN rule ID 1.

However, the administrator observes that the corporate traffic does not match the SD-WAN rule ID 1.

Based on the exhibits, which configuration change is required to fix issue?
* In the dcl-lab-rm route map configuration, set set-route-tag to 10.
* In SD-WAN rule ID 1, change the destination to use ISDB entries.
* In the BGP neighbor configuration, apply the route map dcl-lab-rm in the outbound direction.
* In the dcl-lab-rm route map configuration, unset match-community.

NO.26 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?
* FortiGate bounces port5 after it detects all SD-WAN members as dead.
* FortiGate fails over to the secondary device after it detects all SD-WAN members as dead.
* FortiGate brings up port5 after it detects all SD-WAN members as alive.
* FortiGate brings down port5 after it detects all SD-WAN members as dead.

NO.27 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.)
* Setadditional-pathtosend
* Enableroute-reflector-client
* Setadvertisement-intervalto the number of additional paths to advertise
* Setadv-additional-pathto the number of additional paths to advertise
* Enablesoft-reconfiguration

NO.28 Which are three key routing principles in SD-WAN? (Choose three.)
* FortiGate performs route lookups for new sessions only.
* Regular policy routes have precedence over SD-WAN rules.
* SD-WAN rules have precedence over ISDB routes.
* By default, SD-WAN members are skipped if they do not have a valid route to the destination.
* By default, SD-WAN rules are skipped if the best route to the destination is not an SD-WAN member.

Explanation

Study Guide 7.2, pages 125, 129, 151

NO.29 Which two statements are true about using SD-WAN to steer local-out traffic? (Choose two.)
* FortiGate does not consider the source address of the packet when matching an SD-WAN rule for local-out traffic.
* By default, local-out traffic does not use SD-WAN.
* By default, FortiGate does not check if the selected member has a valid route to the destination.
* You must configure each local-out feature individually, to use SD-WAN.

NO.30 Refer to the exhibit.

```
config system sdwan
    set status enable
    set load-balance source-dest-ip-based
    config zone
        edit "virtual-wan-link"
        next
        edit "SASE"
        next
        edit "underlay"
        next
    end
    config members
        edit 1
            set interface "port1"
            set zone "underlay"
            set gateway 192.2.0.2
        next
        edit 2
            set interface "port2"
            set zone "underlay"
            set gateway 192.2.0.10
        next
    end
...
end
```


Which algorithm does SD-WAN use to distribute traffic that does not match any of the SD-WAN rules?

* All traffic from a source IP to a destination IP is sent to the same interface.
* All traffic from a source IP is sent to the same interface.
* All traffic from a source IP is sent to the most used interface.
* All traffic from a source IP to a destination IP is sent to the least used interface.

Explanation

Study Guide 7.2, page 176.

NO.31 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.)

* Specify a unique peer ID for each dial-up VPN interface.
* Use different proposals are used between the interfaces.
* Configure the IKE mode to be aggressive mode.
* Use unique Diffie Hellman groups on each VPN interface.

NO.32 Refer to the exhibit.

```
id=20085 trace_id=847 func=print_pkt_detail line=5428 msg="vd-root:0 received a
packet(proto=6, 10.1.10.1:33920->74.125.195.93:443) from port3. flag [.], seq
2018554516, ack 4141536963, win 2238"
id=20085 trace_id=847 func=resolve_ip_tuple_fast line=5508 msg="Find an existing
session, id-000008c1, original direction"
id=20085 trace_id=847 func=shaper_handler line=821 msg="exceeded shaper limit, drop"
```

Which conclusion about the packet debug flow output is correct?
* The original traffic exceeded the maximum packets per second of the outgoing interface, and the packet

was dropped.
* The reply traffic exceeded the maximum bandwidth configured in the traffic shaper, and the packet was

dropped.
* The original traffic exceeded the maximum bandwidth of the outgoing interface, and the packet was

dropped.
* The original traffic exceeded the maximum bandwidth configured in the traffic shaper, and the packet

was dropped.

NO.33 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.)
* FortiGate does not change the routing information on existing sessions that use a valid gateway, after a

route change.
* FortiGate performs routing lookups for new sessions only, after a route change.
* FortiGate always blocks all traffic, after a route change.
* FortiGate flushes all routing information from the session table, after a route change.

NO.34

```
# 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.)

* The traffic shaper drops packets if the bandwidth is less than 2500 KBps.
* The measured bandwidth is less than 100 KBps.
* The traffic shaper drops packets if the bandwidth exceeds 6250 KBps.
* The traffic shaper limits the bandwidth of each source IP to a maximum of 6250 KBps.

NO.35 Refer to the exhibit.

```
branch1_fgt # diagnose sys sdwan service 3

Service(3): Address Mode(IPV4) flags=0x200 use-shortcut-sla
  Gen(2), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(priority), link-cost-factor(packet-
loss), link-cost-threshold(0), heath-check(VPN_PING)
  Members(3):
    1: Seq_num(3 T_INET_0_0), alive, packet loss: 2.000%, selected
    2: Seq_num(4 T_MPLS_0), alive, packet loss: 4.000%, selected
    3: Seq_num(5 T_INET_1_0), alive, packet loss: 12.000%, 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 link-cost-factor packet-loss
        set link-cost-threshold 0
        set priority-members 5 3 4
    next
end
```

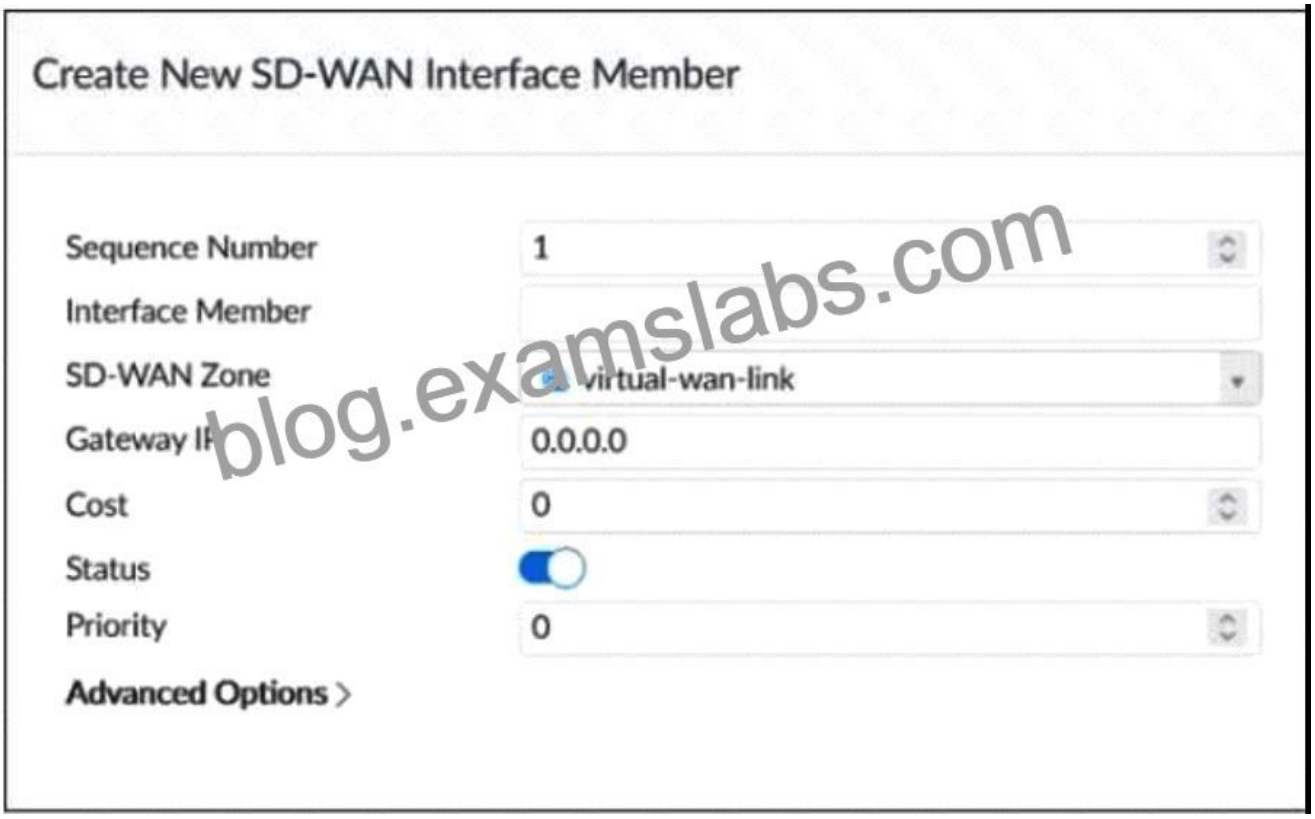

The exhibit shows the SD-WAN rule status and configuration.

Based on the exhibit, which change in the measured packet loss will make T_INET_1_0 the new preferred member?

* When all three members have the same packet loss.

* When T_INET_0_0 has 4% packet loss.
* When T_INET_0_0 has 12% packet loss.
* When T_INET_1_0 has 4% packet loss.

NO.36 Refer to the exhibit.



Which two SD-WAN template member settings support the use of FortiManager meta fields? (Choose two.)
* Cost
* Interface member
* Priority
* Gateway IP

NO.37 Refer to the exhibit.

```
branch1_fgt # diagnose firewall proute list
list route policy info(vf=root):

id=1 dscp_tag=0xff 0xff flags=0x0 tos=0x00 tos_mask=0x00 protocol=17 sport=0-65535 iif=7
dport=53 path(1) oif=3(port1)
source wildcard(1): 0.0.0.0/0.0.0.0
destination wildcard(1): 4.2.2.1/255.255.255.255
hit_count=0 last_used=2022-03-25 10:53:26

id=2131165185(0x7f070001) vwl_service=1(Critical-DIA) vwl_mbr_seq=1 dscp_tag=0xff 0xff
flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 sport=0-65535 iif=0 dport=1-65535 path(2)
oif=3(port1) oif=4(port2)
source(1): 10.0.1.0-10.0.1.255
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(3): GoToMeeting(4294836966,0,0,0, 16354)
Microsoft.Office.365.Portal(4294837474,0,0,0, 41468) Salesforce(4294837976,0,0,0, 16920)
hit_count=0 last_used=2022-03-24 12:18:16

id=2131165186(0x7f070002) vwl_service=2(Non-Critical-DIA) vwl_mbr_seq=2 dscp_tag=0xff
0xff flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 sport=0-65535 iif=0 dport=1-65535
path(1) oif=4(port2)
source(1): 10.0.1.0-10.0.1.255
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(2): Facebook(4294836806,0,0,0, 15832) Twitter(4294838278,0,0,0, 16001)
hit_count=0 last_used=2022-03-24 12:18:16

id=2131165187(0x7f070003) vwl_service=3(all_rules) vwl_mbr_seq=1 dscp_tag=0xff 0xff
flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 sport=0-65535 iif=0 dport=1-65535 path(1)
oif=3(port1)
source(1): 0.0.0.0-255.255.255.255
destination(1): 0.0.0.0-255.255.255.255
hit_count=0 last_used=2022-03-25 10:58:12
```

Based on the output, which two conclusions are true? (Choose two.)

* There is more than one SD-WAN rule configured.
* The SD-WAN rules take precedence over regular policy routes.
* The all_rules rule represents the implicit SD-WAN rule.
* Entry 1(id=1) is a regular policy route.

NO.38 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="port1" 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?

* There are no IPsec tunnel statistics log messages for ADVPN cuts.

* There is one shortcut tunnel built from master tunnel T_MPLS_0.
* The VPN tunnel T_MPLS_0 is a shortcut tunnel.
* The master tunnel T_INET_0 cannot accept the ADVPN shortcut.

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.