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
Refer to the exhibits.

Exhibit A

```
config duplication
    edit 1
        set srcaddr "10.0.1.0/24"
        set dstaddr "10.1.0.0/24"
        set srcintf "port5"
        set dstintf "overlay"
        set service "ALL"
        set packet-duplication force
    next
end
```

```
branch1_fgt # diagnose sys sdwan zone
Zone SASE index=2
        members(0):
Zone overlay index=4
        members(3): 19(T_INET_0_0) 20(T_INET_1_0) 21(T_MPLS_0)
Zone underlay index=3
        members(2): 3(port1) 4(port2)
Zone virtual-wan-link index=1
        members(0):
```

```
1.274665 port5 in 10.0.1.101 -> 10.1.0.7: icmp: echo request
1.275788 T_INET_0_0 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
1.275790 T_INET_1_0 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
1.275801 T_MPLS_0 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
1.278365 T_INET_1_0 in 10.1.0.7 -> 10.0.1.101: icmp: echo reply
1.278553 port5 out 10.1.0.7 -> 10.0.1.101: icmp: echo reply
```

Exhibit B

```
3.874431 T_INET_1_0 in 10.0.1.101 -> 10.1.0.7: icmp: echo request
3.874630 port5 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
3.874895 T_INET_0_0 in 10.0.1.101 -> 10.1.0.7: icmp: echo request
3.875125 T_MPLS_0 in 10.0.1.101 -> 10.1.0.7: icmp: echo request
3.875054 port5 in 10.1.0.7 -> 10.0.1.101: icmp: echo reply
3.875308 T_INET_1_0 out 10.1.0.7 -> 10.0.1.101: icmp: echo reply
```

Exhibit A shows the packet duplication rule configuration, the SD-WAN zone status output, and the sniffer output on FortiGate acting as the sender. Exhibit B shows the sniffer output on a FortiGate acting as the receiver.
The administrator configured packet duplication on both FortiGate devices. The sniffer output on the sender FortiGate shows that FortiGate forwards an ICMP echo request packet over three overlays, but it only receives one reply packet through T_INET_1_0.
Based on the output shown in the exhibits, which two reasons can cause the observed behavior? (Choose two.)

A. On the receiver FortiGate, packet-de-duplication is enabled.
B. The ICMP echo request packets sent over T_INET_0_0 and T_MPLS_0 were dropped along the way.
C. The ICMP echo request packets received over T_INET_0_0 and T_MPLS_0 were offloaded to NPU.
D. On the sender FortiGate, duplication-max-num is set to 3.

Answer: AD

NEW QUESTION 2
Which diagnostic command can you use to show the member utilization statistics measured by performance SLAs for the last 10 minutes?

A. diagnose sys sdwan intf-sla-log
B. diagnose sys sdwan health-check
C. diagnose sys sdwan log
D. diagnose sys sdwan sla-log

Answer: D

Explanation:
SD-WAN 7.2 Study Guide page 321 You can view the stored member metrics by running the diagnose sys sdwan sla-log command. Note that you must include the name of the performance SLA followed by the member configuration index number. To display the SLA logs per interface, you run the diagnose sys sdwan intf-sla-log command.

NEW QUESTION 3
Refer to the exhibit.

```
# 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 are two expected behaviors of the traffic that matches the traffic shaper? (Choose two.)

A. The number of simultaneous connections among all source IP addresses cannot exceed five connections.
B. The traffic shaper limits the combined bandwidth of all connections to a maximum of 5 MB/sec.
C. The number of simultaneous connections allowed for each source IP address cannot exceed five connections.
D. The traffic shaper limits the bandwidth of each source IP address to a maximum of 625 KB/sec.

Answer: CD

NEW QUESTION 4
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 5
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 6
What does enabling the exchange-interface-ip setting enable FortiGate devices to exchange?

A. The gateway address of their IPsec interfaces
B. The tunnel ID of their IPsec interfaces
C. The IP address of their IPsec interfaces
D. The name of their IPsec interfaces

Answer: C

NEW QUESTION 7
Which two performance SLA protocols enable you to verify that the server response contains a specific value? (Choose two.)

A. http
B. icmp
C. twamp
D. dns

Answer: AD

Explanation:
Pages 85,86 in Study guide 7.0 Pages 100,101 in Study guide 7

NEW QUESTION 8
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 the destination.
E. By default, SD-WAN rules are skipped if the best route to the destination is not an SD-WAN member.

Answer: BDE

NEW QUESTION 9
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?

A. When all three members have the same packet loss.
B. When T_INET_0_0 has 4% packet loss.
C. When T_INET_0_0 has 12% packet loss.
D. When T_INET_1_0 has 4% packet loss.

Answer: A

NEW QUESTION 10
Which two settings can you configure to speed up routing convergence in BGP? (Choose two.)

A. update-source
B. set-route-tag
C. holdtime-timer
D. link-down-failover

Answer: CD

NEW QUESTION 10
What are two common use cases for remote internet access (RIA)? (Choose two.)

A. Provide direct internet access on spokes
B. Provide internet access through the hub
C. Centralize security inspection on the hub
D. Provide thorough inspection on spokes

Answer: BC

NEW QUESTION 15
Which components make up the secure SD-WAN solution?

A. Application, antivirus, and URL, and SSL inspection
B. Datacenter, branch offices, and public cloud
C. FortiGate, FortiManager, FortiAnalyzer, and FortiDeploy
D. Telephone, ISDN, and telecom network.

Answer: C

NEW QUESTION 17
Refer to the exhibits.
Exhibit A

Exhibit B

```
branch1_fgt # diagnose sys sdwan member
Member(1): interface: port1, flags=0x0 , gateway: 192.2.0.2, priority: 0 1024, weight: 0
Member(2): interface: port2, flags=0x0 , gateway: 192.2.0.10, priority: 0 1024, weight: 0
```

```
config service
    edit 1
        set name "Critical-DIA"
        set mode priority
        set src "LAN-net"
        set internet-service enable
        set internet-service-app-ctrl 16354 41468 16920
        set health-check "Level3_DNS"
        set priority-members 1 2
    next
end
```

Exhibit A shows an SD-WAN event log and exhibit B shows the member status and the SD-WAN rule configuration.
Based on the exhibits, which two statements are correct? (Choose two.)

A. FortiGate updated the outgoing interface list on the rule so it prefers port2.
B. Port2 has the highest member priority.
C. Port2 has a lower latency than port1.
D. SD-WAN rule ID 1 is set to lowest cost (SLA) mode.

Answer: AC

NEW QUESTION 18
Refer to the exhibits.
Exhibit A

```
config system global
    set snat-route-change enable
end
```

Exhibit B

```
branch1_fgt # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [1/0] via 192.2.0.2, port2, [1/0]
                  [1/0] via 192.2.0.10, port1 [10/0]
...
```

Exhibit A shows the source NAT (SNAT) global setting and exhibit B shows the routing table on FortiGate.
Based on the exhibits, which two actions does FortiGate perform on existing sessions established over port2, if the administrator increases the static route priority on port2 to 20? (Choose two.)

A. FortiGate flags the sessions as dirty.
B. FortiGate continues routing the sessions with no SNAT, over port2.
C. FortiGate performs a route lookup for the original traffic only.
D. FortiGate updates the gateway information of the sessions with SNAT so that they use port1 instead of port2.

Answer: AD

NEW QUESTION 19
Which diagnostic command can you use to show the configured SD-WAN zones and their assigned members?

A. diagnose sys sdwan zone
B. diagnose sys sdwan service
C. diagnose sys sdwan member
D. diagnose sys sdwan interface

Answer: A

NEW QUESTION 21
Refer to the exhibits.
Exhibit A

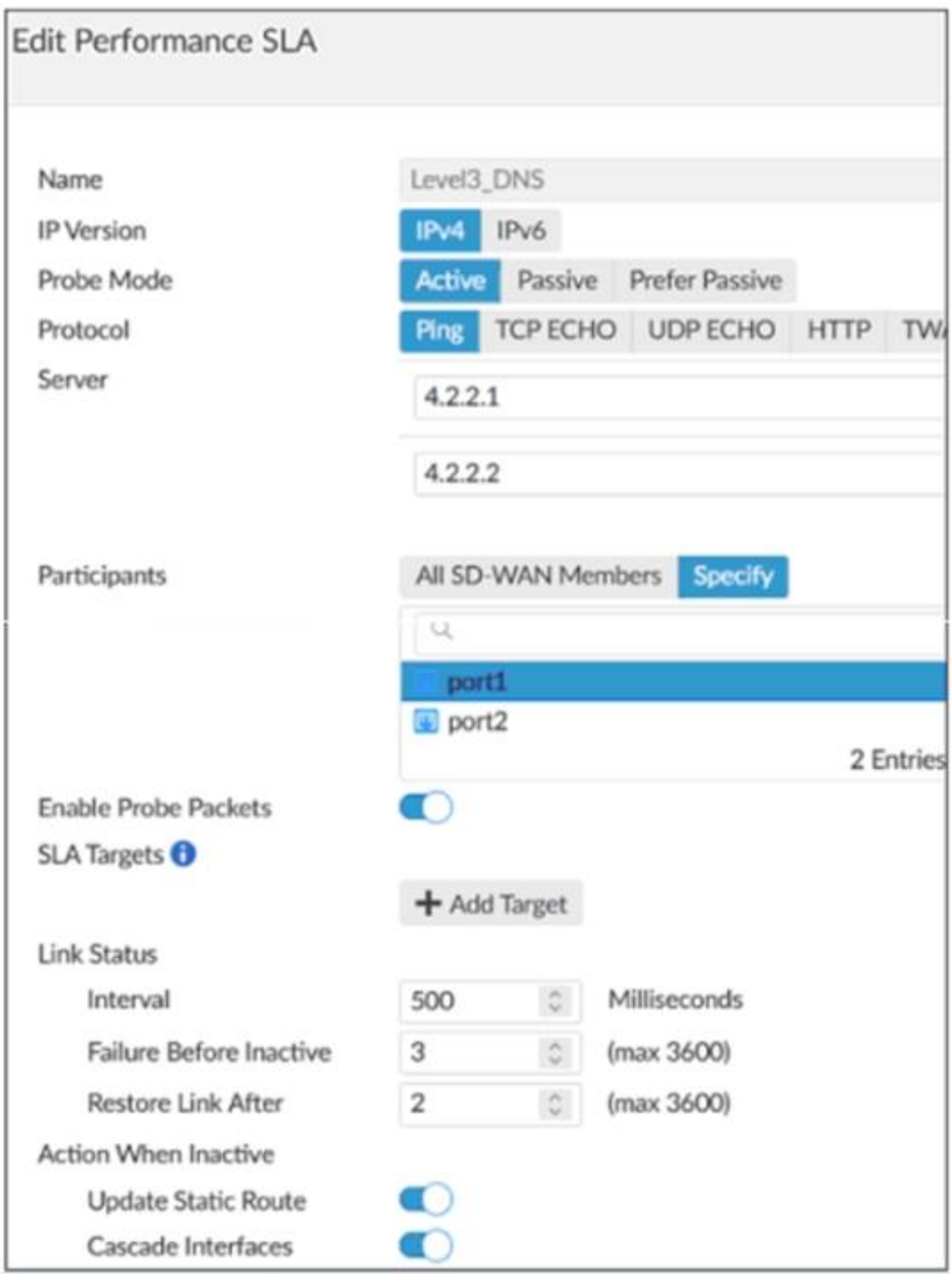


Exhibit B

```
branch1_fgt # diagnose sys sdwan member | grep port
Member(1): interface: port1, flags=0x0 , gateway: 192.2.0.2, priority: 0 1024, weight: 0
Member(2): interface: port2, flags=0x0 , gateway: 192.2.0.10, priority: 0 1024, weight: 0

branch1_fgt # get router info routing-table all | grep port
S*      0.0.0.0/0 [1/0] via 192.2.0.2, port1
                  [1/0] via 192.2.0.10, port2
S       8.8.8.8/32 [10/0] via 192.2.0.11, port2
C       10.0.1.0/24 is directly connected, port5
S       172.16.0.0/16 [10/0] via 172.16.0.2, port4
C       172.16.0.0/29 is directly connected, port4
C       192.2.0.0/29 is directly connected, port1
C       192.2.0.8/29 is directly connected, port2
C       192.168.0.0/24 is directly connected, port10

branch1_fgt # diagnose sys sdwan health-check status Level3_DNS
Health Check(Level3_DNS):
Seq(1 port1): state(alive), packet-loss(0.000%) latency(1.919), jitter(0.137), bandwidth-
up(10238), bandwidth-dw(10238), bandwidth-bi(20476) sla_map=0x0
Seq(2 port2): state(alive), packet-loss(0.000%) latency(1.509), jitter(0.101), bandwidth-
up(10238), bandwidth-dw(10238), bandwidth-bi(20476) sla_map=0x0
```

Exhibit A shows the SD-WAN performance SLA and exhibit B shows the SD-WAN member status, the routing table, and the performance SLA status.
If port2 is detected dead by FortiGate, what is the expected behavior?

A. Port2 becomes alive after three successful probes are detected.
B. FortiGate removes all static routes for port2.
C. The administrator manually restores the static routes for port2, if port2 becomes alive.
D. Host 8.8.8.8 is reachable through port1 and port2.

Answer: B

Explanation:
This is due to Update static route is enable which removes the static route entry referencing the interface if the interface is dead

NEW QUESTION 25
Refer to the exhibits.

Exhibit A

```
branch1_fgt # diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
  Gen(8), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(manual)
  Members(2):
    1: Seq_num(1 port1), alive, selected
    2: Seq_num(2 port2), alive, selected
  Internet Service(3): GoToMeeting(4294836966,0,0,0 16354)
Microsoft.Office.365.Portal(4294837474,0,0,0 41468) Salesforce(4294837976,0,0,0 16920)
  Src address(1):
        10.0.1.0-10.0.1.255


Service(2): Address Mode(IPV4) flags=0x200 use-shortcut-sla
  Gen(7), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(manual)
  Members(1):
    1: Seq_num(2 port2), alive, selected
  Internet Service(2): Facebook(4294836806,0,0,0 15832) Twitter(4294838278,0,0,0 16001)
  Src address(1):
        10.0.1.0-10.0.1.255

branch1_fgt # diagnose sys sdwan internet-service-app-ctrl-list

Facebook(15832 4294836806): 157.240.229.35 6 443 Tue Mar  8 12:24:04 2022
GoToMeeting(16354 4294836966): 23.205.106.86 6 443 Tue Mar  8 12:24:04 2022
GoToMeeting(16354 4294836966): 23.212.249.144 6 443 Tue Mar  8 12:24:39 2022
Salesforce(16920 4294837976): 23.212.249.11 6 443 Tue Mar  8 12:24:04 2022

branch1_fgt # get router info routing-table all
...
S*      0.0.0.0/0 [1/0] via 192.2.0.2, port1
                  [1/0] via 192.2.0.10, port2
...
```

Exhibit B

Destination IP	Service	Application	Security Event List	SD-WAN Rule Name	Destination Interface
23.212.248.205	HTTPS	GoToMeeting	APP 2		port2
23.205.106.86	HTTPS	GoToMeeting	APP 2	Critical-DIA	port1
23.205.106.86	HTTPS	GoToMeeting	APP 2	Critical-DIA	port1
23.205.106.86	HTTPS	GoToMeeting	APP 2	Critical-DIA	port1
23.212.249.144	HTTPS	GoToMeeting	APP 2	Critical-DIA	port1
23.212.249.144	HTTPS	GoToMeeting	APP 2		port1
23.212.249.144	HTTPS	GoToMeeting	APP 2		port2
23.205.106.86	HTTPS	GoToMeeting	APP 2		port2

An administrator is testing application steering in SD-WAN. Before generating test traffic, the administrator collected the information shown in exhibit A.
After generating GoToMeeting test traffic, the administrator examined the respective traffic log on FortiAnalyzer, which is shown in exhibit B. The administrator noticed that the traffic matched the implicit SD-WAN rule, but they expected the traffic to match rule ID 1.
Which two reasons explain why the traffic matched the implicit SD-WAN rule? (Choose two.)

A. FortiGate did not refresh the routing information on the session after the application was detected.
B. Port1 and port2 do not have a valid route to the destination.
C. Full SSL inspection is not enabled on the matching firewall policy.
D. The session 3-tuple did not match any of the existing entries in the ISDB application cache.

Answer: AC

NEW QUESTION 26
Refer to the exhibit.

```
config vpn ipsec phase1-interface
    edit "T_INET_0_0"
        set type dynamic
        set interface "port1"
        set keylife 28800
        set peertype any
        set net-device disable
        set proposal aes128-sha256
        set add-route enable
        set psksecret ENC
Zv9n4Urfk0W4jj8vWI+KywxBG4ZDT7jWHKd8YaL8j4+pRpYOx/N7mSgc7VL0BW2ZHQUXWJ6zvFxNKktiPYNtA8aP
i6ly7gDx2lP/OfKexTQQJzgCGRYzLM8eFTOnK7K6AuX0bFDCpBBhEIdf+03CYBMLwkFZmdU6RsT+qvybblVX+Ioy
HK5EXakpmz5RiltELgZ9Gg==
    next
end
```

Which configuration change is required if the responder FortiGate uses a dynamic routing protocol to exchange routes over IPsec?

A. type must be set to static.
B. mode-cfg must be enabled.
C. exchange-interface-ip must be enabled.
D. add-route must be disabled.

Answer: D

Explanation:
for using "non ike" routes (for example BGP/static and so on) you must do disable the add-route that inject automatically kernel route based on p2 selectors from the remote site from the SD-WAN_7.2_Study_Guide page 236

NEW QUESTION 29
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)
```

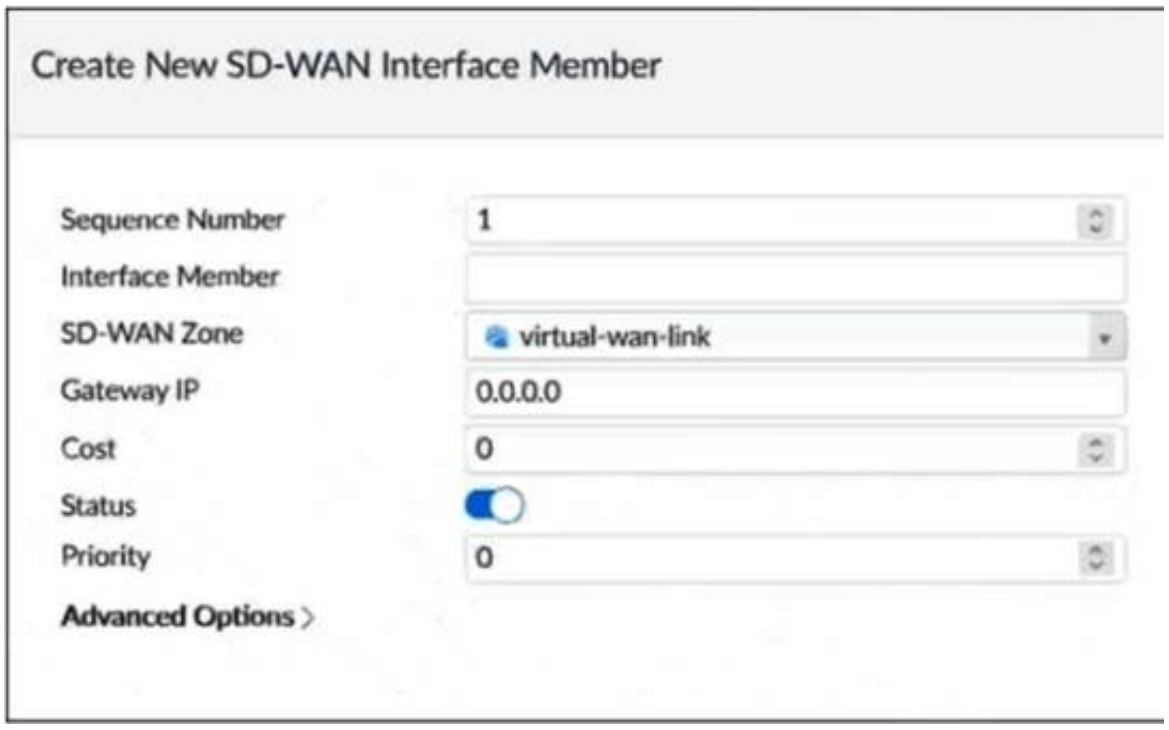
Exhibit A shows the SD-WAN performance SLA configuration, the SD-WAN rule configuration, and the application IDs of Facebook and YouTube. Exhibit B shows the firewall policy configuration and the underlay zone status.
Based on the exhibits, which two statements are correct about the health and performance 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 7.0, pages 88 - 89.
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 30
Refer to the exhibit.

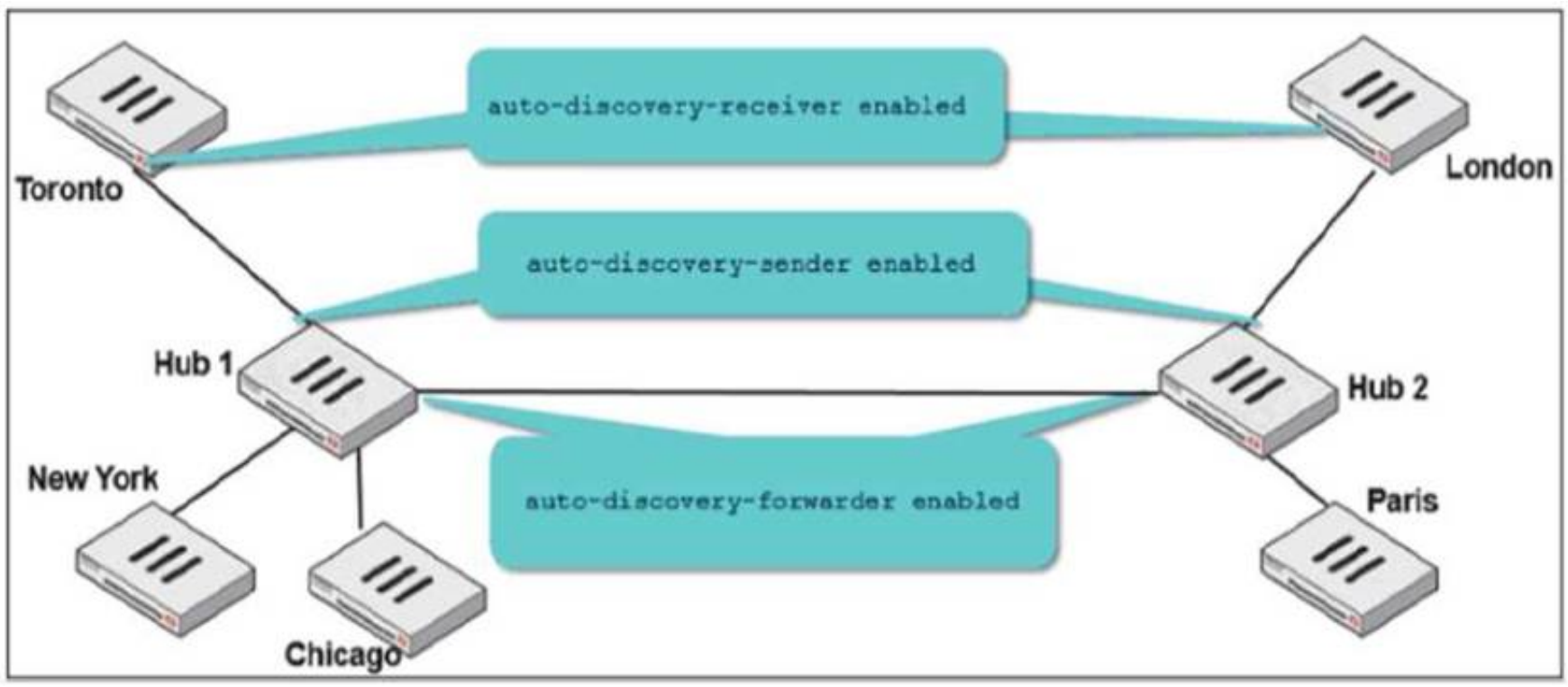


Which two SD-WAN template member settings support the use of FortiManager meta fields? (Choose two.)

A. Cost
B. Interface member
C. Priority
D. Gateway IP

Answer: BD

NEW QUESTION 33
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 38
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 41
What are two benefits of using the Internet service database (ISDB) in an SD-WAN rule? (Choose two.)

A. The ISDB is dynamically updated and reduces administrative overhead.
B. The ISDB requires application control to maintain signatures and perform load balancing.
C. The ISDB applies rules to traffic from specific sources, based on application type.
D. The ISDB contains the IP addresses and port ranges of well-known internet services.

Answer: AD

NEW QUESTION 44
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

NEW QUESTION 45
Refer to the exhibits. Exhibit A

```
branch1_fgt (3) # show
config service
    edit 3
        set name "Corp"
        set mode sla
        set dst "Corp-net"
        set src "LAN-net"
        config sla
            edit "VPN_PING"
                set id 1
            next
            edit "VPN_HTTP"
                set id 1
            next
        end
        set priority-members 3 4 5
        set gateway enable
    next
end
```

Exhibit B

```
branch1_fgt # diagnose sys sdwan service 3

Service(3): Address Mode(IPV4) flags=0x200 use-shortcut-sla
  Gen(1), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(sla), sla-compare-order
  Members(2):
    1: Seq_num(5 T_MPLS_0), alive, sla(0x3), gid(0), cfg_order(2), cost(0), selected
    2: Seq_num(4 T_INET_1_0), alive, sla(0x1), gid(0), cfg_order(1), cost(0), selected
    3: Seq_num(3 T_INET_0_0), alive, sla(0x0), gid(0), cfg_order(0), cost(0), 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 # get router info routing-table all | grep T_
S       10.0.0.0/8 [1/0] via T_INET_0_0 tunnel 100.64.1.1
                   [1/0] via T_INET_1_0 tunnel 100.64.1.9
S       10.201.1.254/32 [15/0] via T_INET_0_0 tunnel 100.64.1.1
S       10.202.1.254/32 [15/0] via T_INET_1_0 tunnel 100.64.1.9
S       10.203.1.254/32 [15/0] via T_MPLS_0 tunnel 172.16.1.5


branch1_fgt # diagnose sys sdwan member | grep T_
Member(3): interface: T_INET_0_0, flags=0x4 , gateway: 100.64.1.1,  peer: 10.201.1.254,
priority: 0 1024, weight: 0
Member(4): interface: T_INET_1_0, flags=0x4 , gateway: 100.64.1.9,  peer: 10.202.1.254,
priority: 0 1024, weight: 0
Member(5): interface: T_MPLS_0, flags=0x4 , gateway: 172.16.1.5,  peer: 10.203.1.254,
priority: 0 1024, weight: 0
```

Exhibit A shows the configuration for an SD-WAN rule and exhibit B shows the respective rule status, the routing table, and the member status.
The administrator wants to understand the expected behavior for traffic matching the SD-WAN rule. Based on the exhibits, what can the administrator expect for traffic matching the SD-WAN rule?

A. The traffic will be load balanced across all three overlays.
B. The traffic will be routed over T_INET_0_0.
C. The traffic will be routed over T_MPLS_0.
D. The traffic will be routed over T_INET_1_0.

Answer: D

NEW QUESTION 46
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?

A. The original traffic exceeded the maximum packets per second of the outgoing interface, and the packet was dropped.
B. The reply traffic exceeded the maximum bandwidth configured in the traffic shaper, and the packet was dropped.
C. The original traffic exceeded the maximum bandwidth of the outgoing interface, and the packet was dropped.
D. The original traffic exceeded the maximum bandwidth configured in the traffic shaper, and the packet was dropped.

Answer: D

NEW QUESTION 47
Refer to the exhibits.

```
dc1_fgt # show vpn ipsec phase1-interface T_INET_1_0
config vpn ipsec phase1-interface
    edit "T_INET_1_0"
        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 psksecret ENC
GayzHJ/UhxCc9FYtwas5o4rkNCMjjNUEj4Q4fZNS6I65RIVF9zum6sJALsU9Cg+1jsXz3ZtIM+WNkHLsXkHqydgS
G/Zx8Vp9Rcht6zKHPectOcFVbaG+UeO3Rw41pmGP/Z3rIz3tdXJxfYSzKjRqggqahsmDovkrKRHTVFUlzA07Zt6W
iPL9co/Zf3cX+Qpnmm38MQ==
    next
end
```

```
dc1_fgt # diagnose vpn tunnel list name T_INET_1_0_0
list ipsec tunnel by names in vd 0
------------------------------------------------------
name=T_INET_1_0_0 ver=2 serial=7 100.64.1.9:0->192.2.0.9:0 tun_id=192.2.0.9 dst_mtu=0
dpd-link=on weight=1
bound_if=4 lgwy=static/1 tun=tunnel/255 mode=dial_inst/3 encap=none/8832
options[2280]=rgwy-chg frag-rfc  run_state=0 accept_traffic=1 overlay_id=0
parent=T_INET_1_0 index=0
proxyid_num=1 child_num=0 refcnt=6 ilast=17 olast=23464 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=1
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=T_INET_1_0_0 proto=0 sa=1 ref=2 serial=1 add-route
  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=20683 type=00 soft=0 mtu=1280 expire=972/0B replaywin=2048
       seqno=1 esn=0 replaywin_lastseq=00000000 itn=0 qat=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=1790/1800
  dec: spi=02f9844e esp=aes key=16 7fb5011247248d3a45ac3d802d8c8d64
       ah=sha1 key=20 bb217ce87ae060f27823b005005233811993a303
  enc: spi=ffc6576a esp=aes key=16 825bddbc5c995feb70411a773867c2d0
       ah=sha1 key=20 02db4176f7f21fae7d141526099a707f639893f1
  dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
```

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 table.
B. The phase 1 configuration supports the network-overlay setting.
C. FortiGate facilitated the negotiation of the T_INET_1_0_0 ADVPN shortcut over T_INET_1_0.
D. Dead peer detection is disabled.

Answer: AB

NEW QUESTION 49
Which statement about using BGP for ADVPN is true?

A. IBGP is preferred over EBGP, because IBGP preserves next hop information.
B. You must use BGP to route traffic for both overlay and underlay links.
C. You must configure BGP communities.
D. You must configure AS path prepending.

Answer: A

NEW QUESTION 53
Refer to the exhibits.

Exhibit A

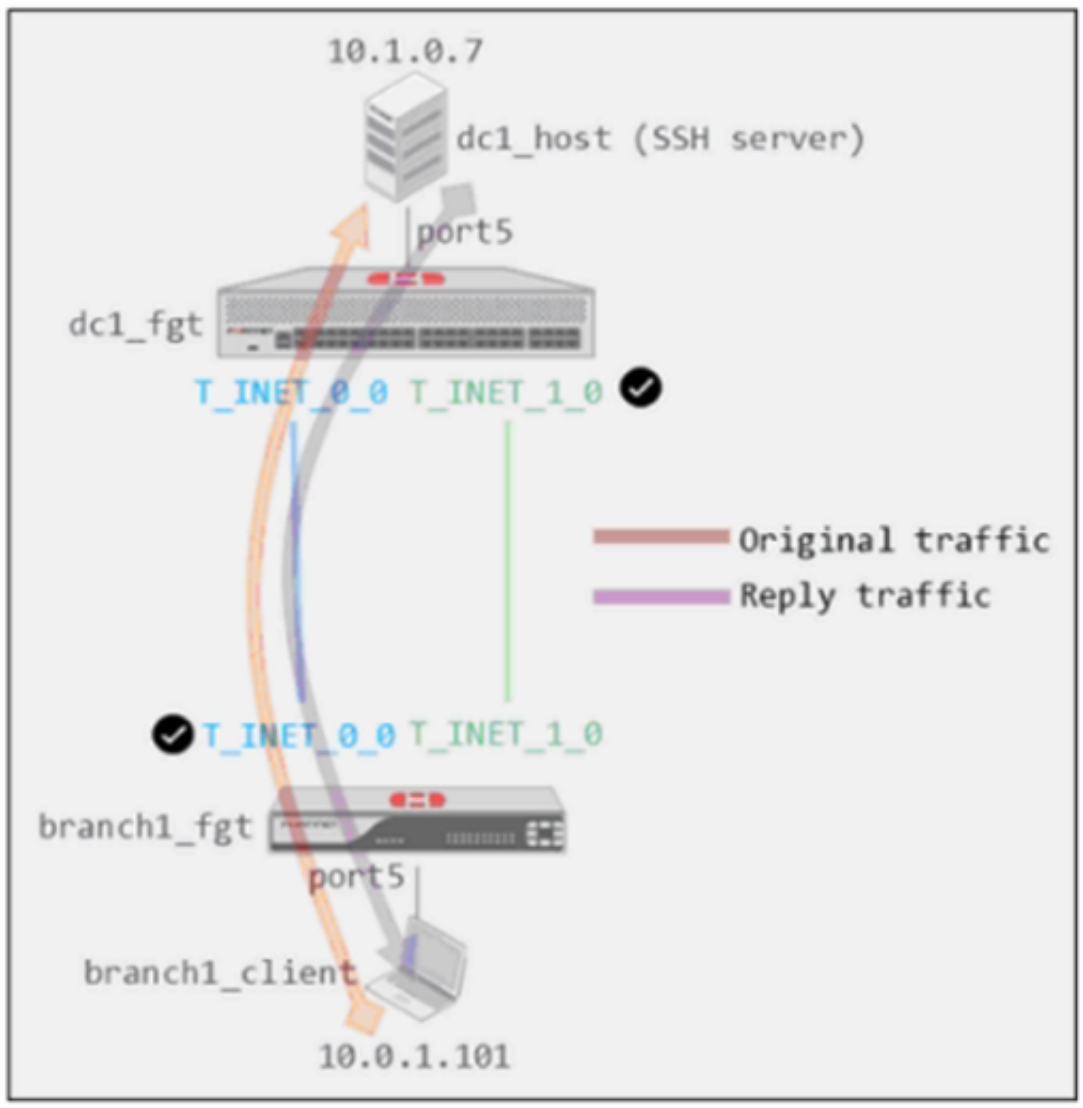


Exhibit B

```
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

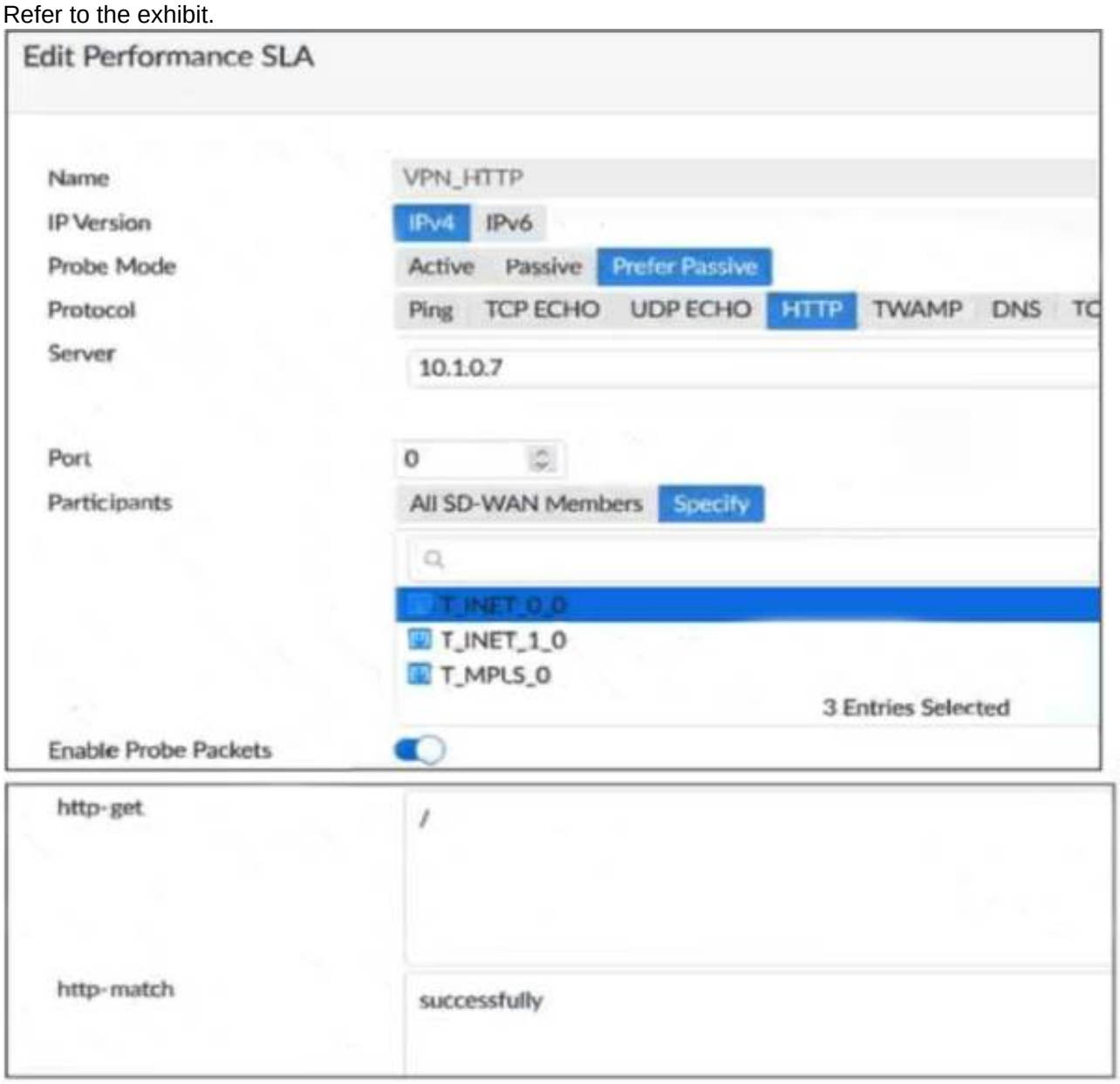
Explanation:
Controlling return path with auxiliary session When multiple incoming or outgoing interfaces are used in ECMP or for load balancing, changes to routing, incoming, or return traffic interfaces impacts how an existing sessions handles the traffic. Auxiliary sessions can be used to handle these changes to traffic patterns.https://docs.fortinet.com/document/fortigate/7.0.11/administration-guide/14295/controlling-return-path

NEW QUESTION 58
Which two statements are true about using SD-WAN to steer local-out traffic? (Choose two.)

A. FortiGate does not consider the source address of the packet when matching an SD-WAN rule for local-out traffic.
B. By default, local-out traffic does not use SD-WAN.
C. By default, FortiGate does not check if the selected member has a valid route to the destination.
D. You must configure each local-out feature individually, to use SD-WAN.

Answer: BD

NEW QUESTION 60
Refer to the exhibit.



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

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

Answer: BD

NEW QUESTION 61
Which two interfaces are considered overlay links? (Choose two.)

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

Answer: BD

NEW QUESTION 66
.....

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