Actual exam question from Fortinet's NSE7_SDW-7.2

Question #: 1

Topic #: 1

[All NSE7_SDW-7.2 Questions]

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"
           set remote-as 65000
           set update-source "T_INET_0"
        next
        edit "Branches_INET_1"
           set interface "T_INET_1"
           set remote-as 65000
           set update-source "T_INET_1"
        next
        edit "Branches_MPLS"
           set interface "T_MPLS"
           set remote-as 65000
           set update-source "T_MPLS"
        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. Enable soft-reconfiguration

B. Enable route-reflector-client

C. Set additional-path to send

D. Set adv-additional-path to the number of additional paths to advertise

E. Set advertisement-interval to the number of additional paths to advertise

Show Suggested Answer

Actual exam question from Fortinet's NSE7_SDW-7.2

Question #: 2

Topic #: 1

[All NSE7_SDW-7.2 Questions]

What are two advantages of using an IPsec recommended template to configure an IPsec tunnel in an hub-and-spoke topology? (Choose two.)

A. It ensures consistent settings between phase1 and phase2.

B. It guides the administrator to use Fortinet recommended settings.

C. The VPN monitor tool provides additional statistics for tunnels defined with an IPsec recommended template.

D. It automatically install IPsec tunnels to every spoke when they are added to the FortiManager ADOM.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_SDW-7.2

Question #: 3

Topic #: 1

[All NSE7_SDW-7.2 Questions]

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
```

A. FortiGate does not change the routing information on existing sessions that use a valid gateway, after a route change.

B. FortiGate always blocks all traffic, after a route change.

C. FortiGate performs routing lookups for new sessions only, after a route change.

D. FortiGate flushes all routing information from the session table, after a route change.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_SDW-7.2

Question #: 4

Topic #: 1

[All NSE7_SDW-7.2 Questions]

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 enables spokes to establish shortcuts to third-party gateways.

C. It provides direct connectivity between spokes by creating shortcuts.

D. It enables spokes to bypass the hub during shortcut negotiation.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_SDW-7.2

Question #: 5

Topic #: 1

[All NSE7_SDW-7.2 Questions]

Refer to the exhibit.

```
fgt_1 # diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
  Tie break: cfg
   Gen(7), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(priority), link-cost-factor(latency), link-cost-
threshold(10), heath-check(HQ_Servers)

   Members(2):
     1: Seq_num(1 port1), alive, latency: 2.672, selected
     2: Seq_num(2 port2), alive, latency: 2.570, selected
   Internet Service(2): Facebook(4294836714,0,0,0,0 15832) Twitter(4294838045,0,0,0,0 16001)
   Src address(1):
         10.0.1.0-10.0.1.255

Service(2): Address Mode(IPV4) flags=0x200 use-shortcut-sla
  Tie break: cfg
   Gen(6), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(manual)
   Members(1):
    1: Seq_num(2 port2), alive, selected
   Internet Service(2): Business(0,29,0,0,0) Industrial(0,26,0,0,0)
   Src address(1):
         10.0.1.0-10.0.1.255

Service(3): Address Mode(IPV4) flags=0x200 use-shortcut-sla
  Tie break: cfg
   Gen(7), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(sla), sla-compare-order
   Members(3):
     1: Seq_num(3 T_HQ1), alive, alive, sla(0x3), gid(0), cfg_order(0), local cost(0), selected
     2: Seq_num(4 T_HQ2), alive, alive, sla(0x2), gid(0), cfg_order(1), local cost(0), selected
     3: Seq_num(5 T_HQ3), alive, alive, sla(0x1), gid(0), cfg_order(2), local 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
```

The exhibit shows output of the command diagnose sys sdwan service collected on a FortiGate device.

The administrator wants to know through which interface FortiGate will steer the traffic from local users on subnet 10.0.1.0/255.255.255.192 and with a destination of the business application Salesforce located on HQ servers 10.0.0.1.

Based on the exhibits, which two statements are correct? (Choose two.)

A. There is no service defined for the Salesforce application, so FortiGate will use the service rule 3 and steer the traffic through interface T_HQ1.

B. FortiGate steers traffic to HQ servers according to service rule 1 and it uses port1 or port2 because both interfaces are selected.

C. When FortiGate cannot recognize the application of the flow it steers the traffic destined to server 10.0.0.1 according to service rule 3.

D. FortiGate steers traffic for business application according to service rule 2 and steers traffic through port2.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_SDW-7.2

Question #: 6

Topic #: 1

[All NSE7_SDW-7.2 Questions]

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

A. By default. SD-WAN members are skipped if they do not have a valid route to the destination.

B. By default. SD-WAN rules are skipped if the best route to the destination is not an SD-WAN member.

C. FortiGate performs route lookups for new sessions only.

D. SD-WAN rules have precedence over ISDB routes.

E. Regular policy routes have precedence over SD-WAN rules.

Show Suggested Answer

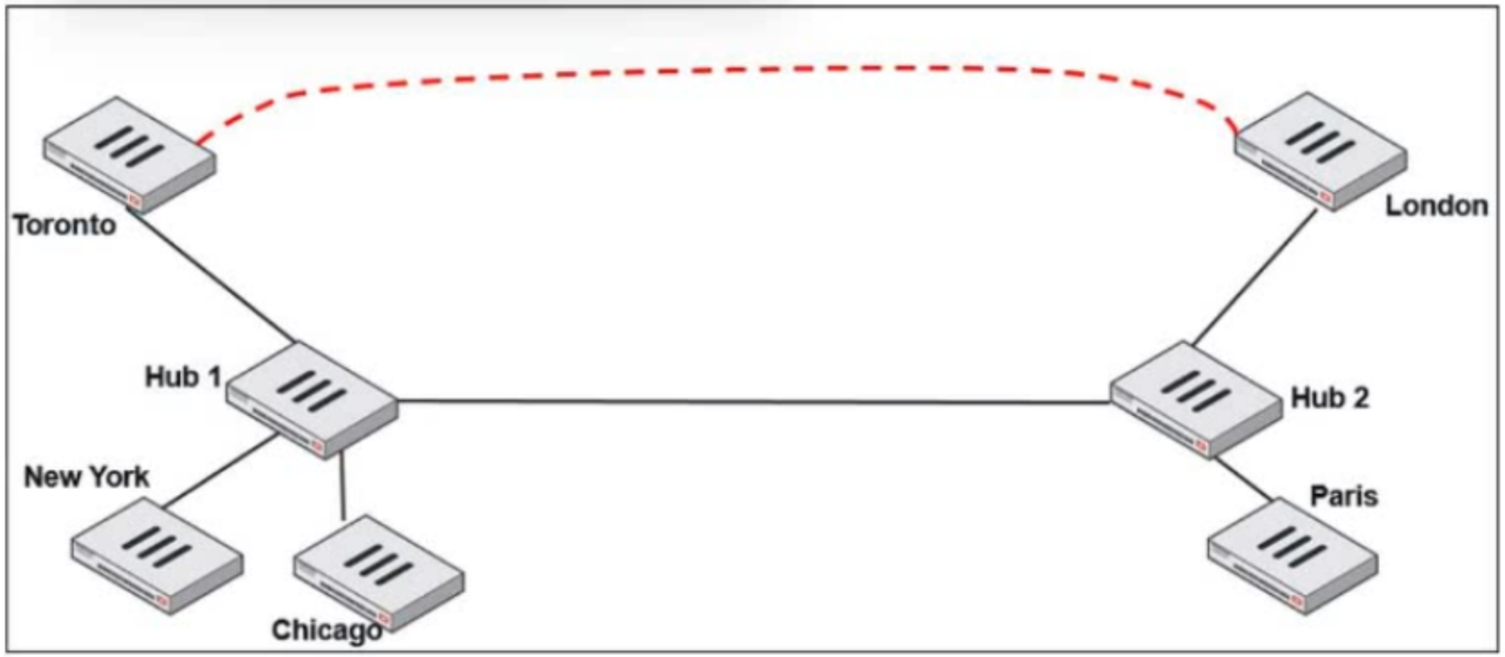
Actual exam question from Fortinet's NSE7_SDW-7.2

Question #: 7

Topic #: 1

[All NSE7_SDW-7.2 Questions]

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, net-device must be enabled on all IPsec VPNs.

B. auto-discovery-forwarder must be enabled on all IPsec VPNs.

C. On the spokes, auto-discovery-receiver must be enabled on the IPsec VPN to the hub.

D. On the hubs, auto-discovery-sender must be enabled on the IPsec VPNs to spokes.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_SDW-7.2

Question #: 8

Topic #: 1

[All NSE7_SDW-7.2 Questions]

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

A. get router info routing-table all

B. get ipsec tunnel list

C. diagnose vpn tunnel list

D. diagnose debug application ike

Show Suggested Answer

Actual exam question from Fortinet's NSE7_SDW-7.2

Question #: 9

Topic #: 1

[All NSE7_SDW-7.2 Questions]

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

A. Provide internet access through the hub.

B. Centralize security inspection on the hub.

C. Provide thorough inspection on spokes.

D. Provide direct internet access on spokes.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_SDW-7.2

Question #: 10

Topic #: 1

[All NSE7_SDW-7.2 Questions]

Refer to the exhibits.

Exhibit A.

```
branch1_fgt # diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
 Tie break: cfg
  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(4294836841,0,0,0,0 16354)
  Microsoft.Office.365.Portal(4294837312,0,0,0,0 41468) Salesforce(42948377 84,0,0,0,0 16920)
  Src address(1):
        10.0.1.0-10.0.1.255

Service(2): Address Mode(IPV4) flags=0x200 use-shortcut-sla
 Tie break: cfg
  Gen(7), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(manual)
  Members(1):
        1: Seq_num(2 port2), alive, selected
  Internet Service(2): Facebook(4294836714,0,0,0,0 15832) Twitter(4294838045,0,0,0,0 16001)
  Src address(1):
        10.0.1.0-10.0.1.255

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

Facebook(15832 4294836714): 157.240.229.35 6 443 Wed Apr 26 07:49:30 2023
GoToMeeting(16354 4294836841): 23.205.106.86 6 443 Wed Apr 26 07:49:30 2023
GoToMeeting(16354 4294836841): 23.212.249.144 6 443 Wed Apr 26 07:49:31 2023
Salesforce(16920 4294837784): 23.212.249.11 6 443 Wed Apr 26 07:49:30 2023

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

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	Critical-DIA	port1
23.212.249.144	HTTPS	GoToMeeting	APP 2		port2
23.205.106.86	HTTPS	GoToMeeting	APP 2		port2

- Security
  - APP Count: 2
  - Level: notice
- General
  - Log ID: 0000000013
  - Session ID: 769
  - Tran Display: snat
  - Virtual Domain: root
- Source
  - Country: Reserved
  - Device ID: FGVM01TM22000077
  - Device Name: branch1_fgt

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 some log messages show that the traffic matched the implicit SD-WAN rule? (Choose two.)

A. Port1 and port2 do not have a valid route to the destination.

B. The session 3-tuple did not match any of the existing entries in the ISDB application cache.

C. Full SSL inspection is not enabled on the matching firewall policy.

D. FortiGate did not refresh the routing information on the session after the application was detected.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_SDW-7.2

Question #: 11

Topic #: 1

[All NSE7_SDW-7.2 Questions]

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

A. diagnose sys sdwan member

B. diagnose sys sdwan interface

C. diagnose sys sdwan zone

D. diagnose sys sdwan service

Show Suggested Answer

Actual exam question from Fortinet's NSE7_SDW-7.2

Question #: 12

Topic #: 1

[All NSE7_SDW-7.2 Questions]

Which statement is correct about SD-WAN and ADVPN?

A. SD-WAN can steer traffic to ADVPN shortcuts only for rules defined with strategy manual or best quality.

B. SD-WAN does not monitor the health and performance of ADVPN shortcuts.

C. SD-WAN cannot steer traffic to ADVPN shortcuts established over IPSec overlays if the zone contains physical interfaces.

D. SD-WAN can steer traffic to ADVPN shortcuts established over IPsec overlays configured as SD-WAN members.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_SDW-7.2

Question #: 13

Topic #: 1

[All NSE7_SDW-7.2 Questions]

Refer to the exhibit.

```
branch1_fgt # diagnose sys sdwan service 3

Service(3): Address Mode(IPV4) flags=0x200 use-shortcut-sla
  Gen(5), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(priority), link-cost-
factor(latency), link-cost-threshold(10), heath-check(VPN_PING)
  Members(3):
    1: Seq_num(3 T_INET_0_0), alive, latency: 101.349, selected
    2: Seq_num(4 T_INET_1_0), alive, latency: 151.278, selected
    3: Seq_num(5 T_MPLS_0), alive, latency: 200.984, selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        10.0.0.0-10.255.255.255


branch1_fgt (3) # show
config service
    edit 3
        set name "Corp"
        set mode priority
        set dst "Corp-net"
        set src "LAN-net"
        set health-check "VPN_PING"
        set priority-members 3 4 5
    next
end
```

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

Based on the exhibit, which change in the measured latency will make T_MPLS_0 the new preferred member?

A. When T_INET_0_0 has a latency of 250 ms.

B. When T_MPLS_0 has a latency of 80 ms.

C. When T_INET_0_0 and T_MPLS_0 have the same latency.

D. When T_MPLS_0 has a latency of 100 ms.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_SDW-7.2

Question #: 14

Topic #: 1

[All NSE7_SDW-7.2 Questions]

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

A. The traffic always skips the regular policy routes.

B. You do not need to configure firewall policies that accept the SD-WAN traffic.

C. You steer traffic based on the detected application.

D. You do not need to enable SSL inspection.

Show Suggested Answer

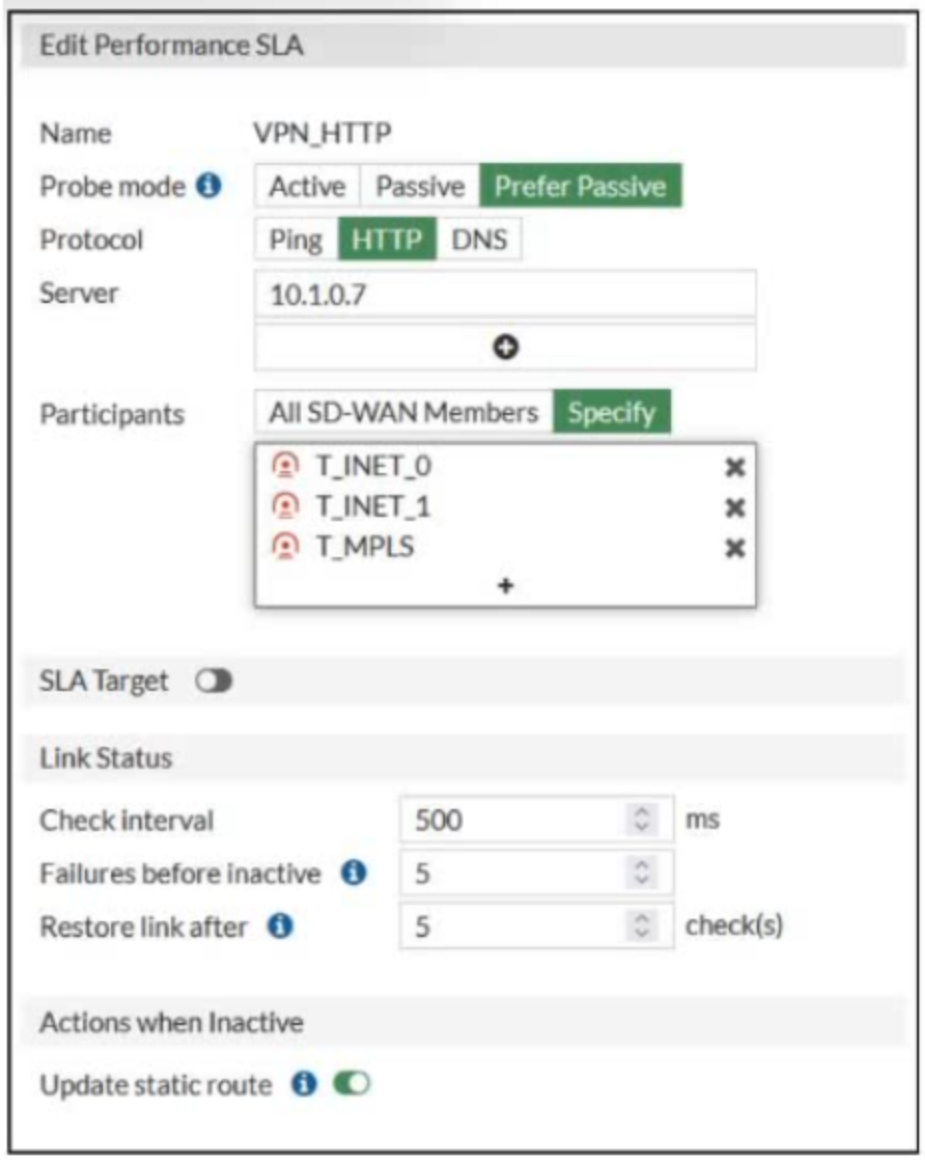
Actual exam question from Fortinet's NSE7_SDW-7.2

Question #: 15

Topic #: 1

[All NSE7_SDW-7.2 Questions]

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, the SLA performance rule never fallsback to passive monitoring.

B. FortiGate passively monitors the member if TCP traffic is passing through the member.

C. FortiGate can offload the traffic that is subject to passive monitoring to hardware.

D. During passive monitoring, the SLA performance rule cannot detect dead members.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_SDW-7.2

Question #: 16

Topic #: 1

[All NSE7_SDW-7.2 Questions]

Which two statements about the SD-WAN members are true? (Choose two.)

A. Interfaces of type virtual wire pair can be used as SD-WAN members.

B. You can manually define the SD-WAN members sequence number.

C. An SD-WAN member can belong to two or more SD-WAN zones.

D. Interfaces of type VLAN can be used as SD-WAN members.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_SDW-7.2

Question #: 17

Topic #: 1

[All NSE7_SDW-7.2 Questions]

Refer to the exhibit.

```
branch1_fgt # diag sys sdwan service 1

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
  Tie break: cfg
   Gen(14), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(sla), sla-compare-order
   Members(4):
      1: Seq_num(3 T_INET_0), alive, sla(0x1), gid(0), cfg_order(0), local cost(0), selected
      2: Seq_num(4 T_INET_1), alive, sla(0x1), gid(0), cfg_order(1), local 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 # diagnose sys sdwan member | grep T_INET_
Member(3): interface: T_INET_0, flags=0xd may_child, gateway: 100.64.1.1, peer: 10.201.1.254, priority:
10 1024, weight: 0
Member(4): interface: T_INET_1, flags=0xd may_child, gateway: 100.64.1.9, peer: 10.202.1.254, priority:
1 1024, weight: 0

branch1_fgt # get router info routing-table all | grep T_INET_
S       10.0.0.0/8 [1/0] via T_INET_1 tunnel 100.64.1.9, [1/0]
```

An administrator is troubleshooting SD-WAN on FortiGate. A device behind branch1_fgt generates traffic to the 10.0.0.0/8 network. The administrator expects the traffic to match SD-WAN rule ID 1 and be routed over T_INET_0. However, the traffic is routed over T_INET_1.

Based on the output shown in the exhibit, which two reasons can cause the observed behavior? (Choose two.)

A. T_INET_1 has a lower route priority value (higher priority) than T_INET_0.

B. The traffic matches a regular policy route configured with T_INET_1 as the outgoing device.

C. T_INET_1 has a higher member configuration priority than T_INET_0.

D. T_INET_0 does not have a valid route to the destination.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_SDW-7.2

Question #: 18

Topic #: 1

[All NSE7_SDW-7.2 Questions]

Within IPsec tunnel templates available on FortiManager, which template will you use to configure static tunnels for a hub and spoke topology?

A. Hub_IPsec_Recommended

B. Static_IPsec_Recommended

C. IPsec Fortinet Recommended

D. Branch IPsec Recommended

Show Suggested Answer

Actual exam question from Fortinet's NSE7_SDW-7.2
Question #: 19
Topic #: 1
[All NSE7_SDW-7.2 Questions]

The administrator uses the FortiManager SD-WAN overlay template to prepare an SD-WAN deployment. With information provided through the SD-WAN overlay template wizard, FortiManager creates templates ready to install on spoke and hub devices.
Select three templates created by the SD-WAN overlay template for a spoke device. (Choose three.)

A. IPsec tunnel template

B. BGP template

C. Overlay template

D. System template

E. CLI template

Show Suggested Answer

Actual exam question from Fortinet's NSE7_SDW-7.2

Question #: 20

Topic #: 1

[All NSE7_SDW-7.2 Questions]

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 2 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.)

A. Entry 1 (id=1) is a regular policy route.

B. There is more than one SD-WAN rule configured.

C. The SD-WAN rules take precedence over regular policy routes.

D. The all_rules rule represents the implicit SD-WAN rule.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_SDW-7.2

Question #: 21

Topic #: 1

[All NSE7_SDW-7.2 Questions]

What are two benefits of using forward error correction (FEC) in IPsec VPNs? (Choose two.)

A. FEC can leverage multiple IPsec tunnels for parity packets transmission.

B. FEC transmits parity packets that can be used to reconstruct packet loss.

C. FEC improves reliability of noisy links.

D. FEC supports hardware offloading.

Show Suggested Answer

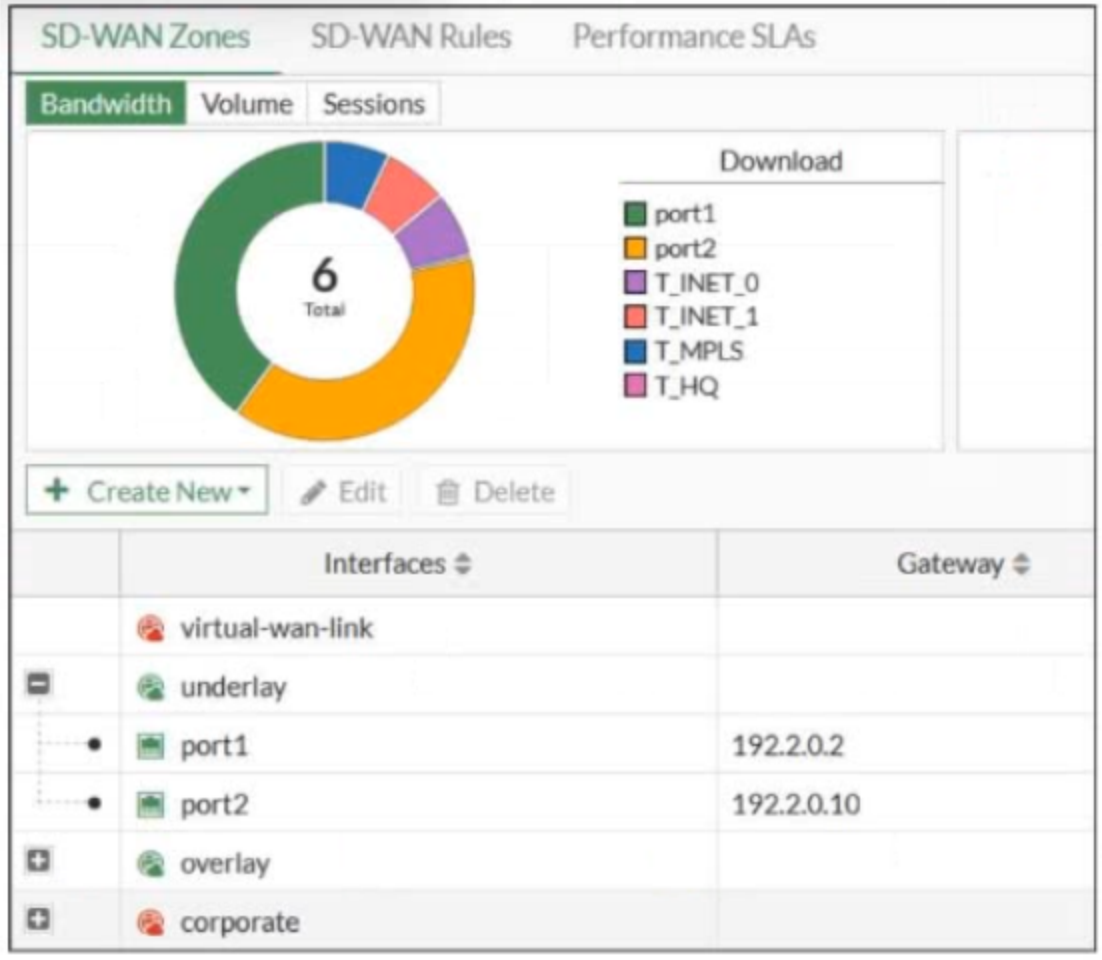
Actual exam question from Fortinet's NSE7_SDW-7.2

Question #: 22

Topic #: 1

[All NSE7_SDW-7.2 Questions]

Refer to the exhibit, which shows an SD-WAN zone configuration on the FortiGate GUI.



Based on the exhibit, which statement is true?

A. You can move port1 from the underlay zone to the overlay zone.

B. You can delete the virtual-wan-link zone because it contains no member.

C. The corporate zone contains no member.

D. The overlay zone contains four members.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_SDW-7.2

Question #: 23

Topic #: 1

[All NSE7_SDW-7.2 Questions]

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 terminates the old sessions.

B. FortiGate evaluates new sessions.

C. FortiGate does not change existing sessions.

D. FortiGate flushes all sessions.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_SDW-7.2

Question #: 24

Topic #: 1

[All NSE7_SDW-7.2 Questions]

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 main session cannot be offloaded to hardware.

B. The original direction of the symmetric traffic flows from port3 to port2.

C. The reply direction of the asymmetric traffic flows from port2 to port3.

D. The auxiliary session can be offloaded to hardware.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_SDW-7.2
Question #: 25
Topic #: 1
[All NSE7_SDW-7.2 Questions]

The SD-WAN overlay template helps to prepare SD-WAN deployments. To complete the tasks performed by the SD-WAN overlay template, the administrator must perform some post-run tasks.
What are three mandatory post-run tasks that must be performed? (Choose three.)

A. Assign an sdwan_id metadata variable to each device (branch and hub).

B. Assign a branch_id metadata variable to each branch device.

C. Create policy packages for branch devices.

D. Configure SD-WAN rules.

E. Configure routing through overlay tunnels created by the SD-WAN overlay template.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_SDW-7.2

Question #: 26

Topic #: 1

[All NSE7_SDW-7.2 Questions]

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 skip content inspection on TCP traffic, to improve performance.

B. It instructs the hub to not check the ESP sequence numbers on IPsec traffic, to improve performance.

C. 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.

D. It instructs the hub to disable the reordering of TCP packets on behalf of the receiver, to improve performance.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_SDW-7.2

Question #: 27

Topic #: 1

[All NSE7_SDW-7.2 Questions]

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

A. The session information output displays no SD-WAN-specific details.

B. All SD-WAN rules have the default and gateway setting enabled.

C. Traffic does not match any of the entries in the policy route table.

D. Traffic is load balanced using the algorithm set for the v4-ecmp-mode setting.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_SDW-7.2

Question #: 28

Topic #: 1

[All NSE7_SDW-7.2 Questions]

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 # diag sys sdwan zone
Zone overlay index=3
     members(3): 19(T_INET_0) 20(T_INET_1) 21(T_MPLS)
Zone underlay index=2
     members(2): 3(port1) 4(port2)
Zone virtual-wan-link index=1
     members(0):
```

```
17.779659 port5 in 10.0.1.101 -> 10.1.0.7: icmp: echo request
17.779717 T_INET_0 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
17.779795 T_INET_1 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
17.779821 T_MPLS out 10.0.1.101 -> 10.1.0.7: icmp: echo request
17.781852 T_INET_1 in 10.1.0.7 -> 10.0.1.101: icmp: echo reply
17.781874 port5 out 10.1.0.7 -> 10.0.1.101: icmp: echo reply
```

Exhibit B -

```
3.679621 T_INET_1 in 10.0.1.101 -> 10.1.0.7: icmp: echo request
3.679735 port5 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
3.679798 T_INET_0 in 10.0.1.101 -> 10.1.0.7: icmp: echo request
3.679835 T_MPLS in 10.0.1.101 -> 10.1.0.7: icmp: echo request
3.681827 port5 in 10.1.0.7 -> 10.0.1.101: icmp: echo reply
3.681853 T_INET_1 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 a FortiGate device acting as the sender. Exhibit B shows the sniffer output on a FortiGate device 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.

Based on the output shown in the exhibits, which two reasons can cause the observed behavior?

(Choose two.)

A. The ICMP echo request packets sent over T_INET_0 and T_MPLS were dropped along the way.

B. On the receiver FortiGate, packet-de-duplication is enabled.

C. On the sender FortiGate, duplication-max-num is set to 3.

D. The sender FortiGate has anti-replay enabled to block duplicate ICMP replies.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_SDW-7.2

Question #: 29

Topic #: 1

[All NSE7_SDW-7.2 Questions]

Refer to the exhibit.

```
ike 0:T_INET_0:4: received informational request
ike 0:T_INET_0:4: processing notify type SHORTCUT_OFFER
ike 0:T_INET_0: shortcut-offer 10.0.1.101->10.0.2.101 0 psk 64 ppk 0 ver 2
mode 0, peer-addr 203.0.113.1:500
ike 0 looking up shortcut by addr 10.0.2.101, name T_INET_0, peer-addr
203.0.113.1:500
ike 0:T_INET_0: send shortcut-query 8212421445716741 85
e7132541b71ac3ea/0000000000000000 192.2.0.1 10.0.1.101->10.0.2.101 0 psk 64
```

Which statement about the role of the ADVPN device in handling traffic is true?

A. This is a spoke that has received an offer from a remote hub.

B. Two spokes, 192.2.0.1 and 10.0.2.101, establish a shortcut.

C. This is a hub that has received an offer from a spoke and has forwarded it to another spoke.

D. An IKE session is established between 10.0.1.101 and 10.0.2.101 in the process of forming a shortcut tunnel.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_SDW-7.2

Question #: 30

Topic #: 1

[All NSE7_SDW-7.2 Questions]

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

A. By default, FortiGate does not check if the selected member has a valid route to the destination.

B. You must configure each local-out feature individually, to use SD-WAN.

C. By default, local-out traffic does not use SD-WAN.

D. FortiGate does not consider the source address of the packet when matching an SD-WAN rule for local-out traffic.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_SDW-7.2

Question #: 31

Topic #: 1

[All NSE7_SDW-7.2 Questions]

Refer to the exhibits.

Exhibit A -

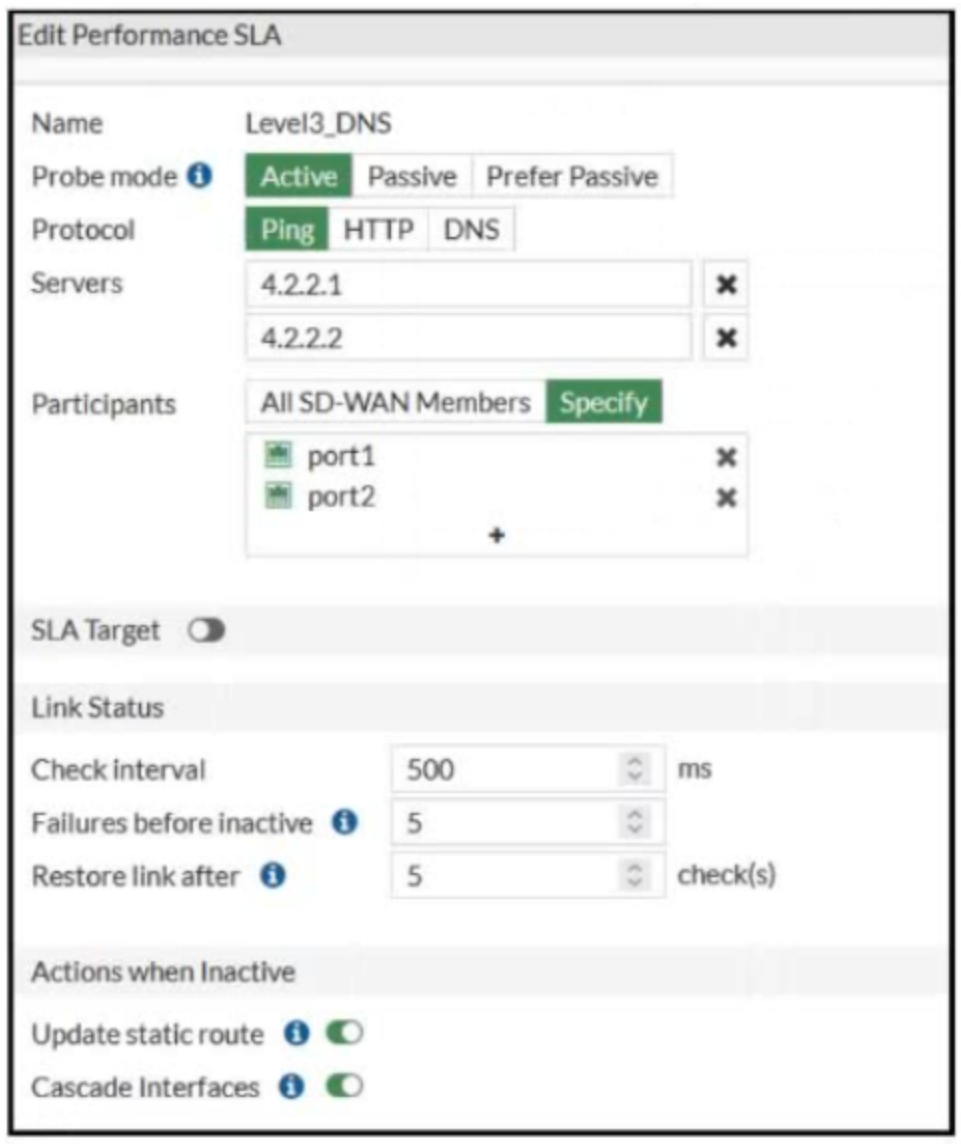


Exhibit B -

```
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. Host 8.3.8.8 is reachable through port1 and port2.

B. Port2 becomes alive after three successful probes are detected.

C. The administrator manually restores the static routes for port2, if port2 becomes alive.

D. FortiGate disables all static routes for port2.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_SDW-7.2

Question #: 32

Topic #: 1

[All NSE7_SDW-7.2 Questions]

In which SD-WAN template field can you use a metadata variable?

A. You can use metadata variables only to define interface members and the gateway IP.

B. Any field identified with a dollar sign (S) in a magnifying glass.

C. Any field identified with an "M" in a circle.

D. All SD-WAN template fields support metadata variables.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_SDW-7.2

Question #: 33

Topic #: 1

[All NSE7_SDW-7.2 Questions]

Refer to the exhibit.

```
# get router info routing-table all
...
B     10.0.2.0/24 [200/0] via 10.201.1.2 [3] (recursive is directly connected, VPN0), 00:26:48, [1/0]
                  [200/0] via 10.202.1.2 [3] (recursive is directly connected, VPN1), 00:26:48, [1/0]
                  [200/0] via 10.203.1.1 [3] (recursive is directly connected, VPN2), 00:26:48, [1/0]
...
```

The device exchanges routes using IBGP.

Which two statements are correct about the IBGP configuration and routing information on the device? (Choose two.)

A. Each BGP route is three hops away from the destination.

B. ibgp-multipath is disabled.

C. You can run the get router info routing-table database command to display the additional paths.

D. additional-path is enabled.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_SDW-7.2

Question #: 34

Topic #: 1

[All NSE7_SDW-7.2 Questions]

Refer to the exhibit, which shows output of the command diagnose sys sdwan health-check status collected on a FortiGate device.

```
# diagnose sys sdwan health-check status

Health Check(Level3_DNS):
Seq(1 port1): state(alive), packet-loss(0.000%) latency(22.129), jitter(0.201), mos(4.393),
bandwidth-up(10235), bandwidth-dw(10235), bandwidth-bi(20470) sla_map=0x0
Seq(2 port2): state(alive), packet-loss(7.000%) latency(42.394), jitter(0.912), mos(4.378),
bandwidth-up(10236), bandwidth-dw(10237), bandwidth-bi(20473) sla_map=0x0
Health Check(VPN_PING):
Seq(5 T_MPLS): state(alive), packet-loss(0.000%) latency(131.336), jitter(0.199), mos(4.330),
bandwidth-up(9999999), bandwidth-dw(9999999), bandwidth-bi(19999998) sla_map=0x2
Seq(4 T_INET_1): state(alive), packet-loss(11.000%) latency(1.465), jitter(0.226), mos(4.398),
bandwidth-up(10239), bandwidth-dw(10239), bandwidth-bi(20478) sla_map=0x1
Seq(3 T_INET_0): state(alive), packet-loss(0.000%) latency(1.440), jitter(0.245), mos(4.403),
bandwidth-up(10239), bandwidth-dw(10239), bandwidth-bi(20478) sla_map=0x3
```

Which two statements are correct about the health check status on this FortiGate device? (Choose two.)

A. The interface T_INET_0 missed three SLA targets.

B. The interface T_INET_1 missed one SLA target.

C. There is no SLA criteria configured for the health-check Level3_DNS.

D. The health-check VPN_PING orders the members according to the measured jitter.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_SDW-7.2

Question #: 35

Topic #: 1

[All NSE7_SDW-7.2 Questions]

Refer to the exhibits.

Exhibit A -

	#	Name	From	To	Source	Destination
☑	1	DIA	D-LAN LAN	underlay	LAN-net	all
☐	Implicit (2/2 Total:1)					
☐	2	Implicit Deny	any	any	all all	all all

Exhibit B -

View Install Log

```
Copy device global objects

validation error on firewall policy 1, by dynamic interface check

Vdom copy failed:
error 42 - entry not exist. detail: Dynamic interface "LAN" mapping undefined for device branch2_fgt

Copy objects for vdom root
```

Exhibit A shows a policy package definition. Exhibit B shows the install log that the administrator received when he tried to install the policy package on FortiGate devices. Based on the output shown in the exhibits, what can the administrator do to solve the issue?

A. Create dynamic mapping for the LAN interface for all devices in the installation target list.

B. Policies can refer to only one LAN source interface. Keep only the D-LAN, which is the dynamic LAN interface.

C. Dynamic mapping should be done automatically. Review the LAN interface configuration for branch2_fgt.

D. Use a metadata variable instead of a dynamic interface to define the firewall policy.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_SDW-7.2

Question #: 36

Topic #: 1

[All NSE7_SDW-7.2 Questions]

What is true about SD-WAN multiregion topologies?

A. It is not compatible with ADVPN.

B. Routing between the hub and spokes must be BGP.

C. Regions must correspond to geographical areas.

D. Each region has its own SD-WAN topology.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_SDW-7.2

Question #: 37

Topic #: 1

[All NSE7_SDW-7.2 Questions]

Refer to the exhibit, which shows the IPsec phase 1 configuration of a spoke.

```
config vpn ipsec phase1-interface
        edit "T_INET_0"
            set interface "port1"
            set ike-version 2
            set keylife 28800
            set peertype any
            set net-device disable
            set proposal aes128-sha256 aes256-sha256 aes128gcm-prfsha256 aes256gcm-
            prfsha384 chacha20poly1305-prfsha256
            set comments "VPN: T_INET_0 [Created by IPSEC Template]"
            set idle-timeout enable
            set idle-timeoutinterval 5
            set auto-discover-receiver enable
            set remote-gw 100.64.1.1
            set psksecret ENC
            lje09rV3LYnzg23vX2JgbzPPFAMaB/jWGQTt5qauJYXzVXsFMoIhS6BHw3lVkVBx+O434nvM0Y
            rKBCvpzMgOGq4Z0YDTvmn6PqkPMNj41IgHr8osKhUkJ54Cjp8N1jxh/zg8DpSw0bRDCwrUkCvC
            IA9jkP1vC+ijDx2yemCw7+HW1pXCgaToLKWvu7Mu5sfwnH09Zg==
        next
end
```

What must you configure on the IPsec phase 1 configuration for ADVPN to work with SD-WAN?

A. You must disable idle-timeout.

B. You must set ike-version to 1.

C. You must enable auto-discovery-sender.

D. You must enable net-device.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_SDW-7.2

Question #: 38

Topic #: 1

[All NSE7_SDW-7.2 Questions]

Which statement about using BGP for ADVPN is true?

A. IBGP is preferred over EBGP, because IBGP preserves next hop information.

B. You must configure AS path prepending.

C. You must configure BGP communities.

D. You must use BGP to route traffic for both overlay and underlay links.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_SDW-7.2

Question #: 39

Topic #: 1

[All NSE7_SDW-7.2 Questions]

Refer to the exhibit that shows VPN event logs on FortiGate.

```
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
```

Based on the output shown in the exhibit, which statement is true?

A. There is one shortcut tunnel built from master tunnel T_MPLS_0.

B. The master tunnel T_INET_0 cannot accept the ADVPN shortcut.

C. There are no IPsec tunnel statistics log messages for ADVPN shortcuts.

D. The VPN tunnel T_MPLS_0 is a shortcut tunnel.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_SDW-7.2

Question #: 40

Topic #: 1

[All NSE7_SDW-7.2 Questions]

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 brings down port5 after it detects all SD-WAN members as dead.

B. FortiGate brings up port5 after it detects all SD-WAN members as alive.

C. FortiGate bounces port5 after it detects all SD-WAN members as dead.

D. FortiGate fails over to the secondary device after it detects all SD-WAN members as dead.

Show Suggested Answer