

Fortinet

Exam Questions NSE7_SDW-7.2

Fortinet NSE 7 - SD-WAN 7.2



NEW QUESTION 1

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

Answer: AD

NEW QUESTION 2

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

```
config vpn ipsec phase1-interface
edit "T_INET_0_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 "[created by FMG VPN Manager]"
set idle-timeout enable
set idle-timeoutinterval 5
set auto-discovery-receiver enable
set remote-gw 100.64.1.1
set psksecret ENC
6D5rVsaKlMeAyVYt1z95BS24Psew761wY023hnFVviwb6deItSc5ltCa+iNYhujT8gycfD4+Wuszpmlv8rRzrVh
7DFkHaW2auAAprQ0dHUfaCzjOhME7mPw+8he2xB7Edb9ku/nZEhb0cKLkKYJc/p9J9IMweV2lZUgFjvIpxNxBxpH
LReOFShoH01SPFRz5IYCVa==
next
end
```

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

- A. You must set ike-version to 1.
- B. You must enable net-device.
- C. You must enable auto-discovery-sender.
- D. You must disable idle-timeout.

Answer: B

NEW QUESTION 3

Which are two benefits of using CLI templates in FortiManager? (Choose two.)

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

Answer: AD

NEW QUESTION 4

Which two statements 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 5

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

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

Answer: BD

NEW QUESTION 6

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?

- A. All traffic from a source IP to a destination IP is sent to the same interface.
- B. All traffic from a source IP is sent to the same interface.
- C. All traffic from a source IP is sent to the most used interface.
- D. All traffic from a source IP to a destination IP is sent to the least used interface.

Answer: A

Explanation:

Study Guide 7.2, page 176.

NEW QUESTION 7

Which statement about SD-WAN zones is true?

- A. An SD-WAN zone can contain only one type of interface.
- B. An SD-WAN zone can contain between 0 and 512 members.
- C. You cannot use an SD-WAN zone in static route definitions.
- D. You can configure up to 32 SD-WAN zones per VDOM.

Answer: D

Explanation:

SD-WAN zones are a group of interfaces that share the same SD-WAN settings, such as health check, SLA, and load balancing. Some characteristics of SD-WAN zones are:

- ? An SD-WAN zone can contain different types of interfaces, such as physical, VLAN, aggregate, and tunnel interfaces1.
- ? An SD-WAN zone can contain up to 512 members1.
- ? You can use an SD-WAN zone in static route definitions, as long as the destination interface is also an SD-WAN zone1.
- ? You can configure up to 32 SD-WAN zones per VDOM1.

NEW QUESTION 8

Refer to the exhibit.

Exhibit A

```
fgt # show vpn ipsec phase1-interface T_INET_1
config vpn ipsec phase1-interface
  edit "T_INET_1"
    set type dynamic
    set interface "port2"
    set ike-version 2
    set keylife 28800
    set peertype any
    set net-device disable
    set proposal aes128-sha256
    set add-route disable
    set auto-discovery-sender enable
    set paksecret ENC MXtFGROxLV+x4p3e9Xq2HGJoU+QOgg5YMqiXb2T73f2pSXS/
    jy9oahWeQ1NEj0JEtUqqD8mAw7G22LT1sR3/ihAaAY4tvjveS+9CuTn00J2tuddoM9
    uz4vaBTNbnRh3/KhbJytsCag==
  next
end
```

Exhibit B

```
fgt # diag vpn tunnel list name T_INET_1_0
list ipsec tunnel by names in vd 0
-----
name=T_INET_1_0 ver=2 serial=a 100.64.1.9:0->192.2.0.9:0 tun_id=192.2.0.9 tun_id6=:10.0.0.10
dst_mtu=0 dpd-link=on weight=1
bound_if=4 igwy=static/1 tun=intf mode=dial_inst/3 encap=none/74408 options=[122a8]=npu rgwy-chg
frag-rfc run_state=0 role=primary acc
ept_traffic=1 overlay_id=0
parent=T_INET_1 index=0
proxyid_num=1 child_num=0 refcnt=6 ilast=0 olast=42955943 ad=/0
stat: rkp=32 txp=0 rxh=1280 txh=0
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
fec: egress=0 ingress=0
proxyid=T_INET_1_0 proto=0 sa=1 ref=2 serial=1
src: 0:0.0.0.0-255.255.255.255:0
dst: 0:10.0.1.0-10.0.1.255:0
SA: ref=3 options=20603 type=00 soft=0 mtu=1280 expire=1774/08 replaywin=2048
seqno=1 esn=0 replaywin_lastseq=00000021 qat=0 rekey=0 hash_search_len=1
life: type=01 bytes=0/0 timeout=1791/1800
dec: spi=7c176e24 esp=aes key=16 8547efb42d148c6692fb2af0d01ff12d
ah=shal key=20 f0d3ac8192d2e79fbbe29162f9ccf406f1a161b5
enc: spi=809f9d49 esp=aes key=16 cb67f6d5f6alf9fe3ab38b953dd4782f
ah=shal key=20 d0182dfe827a4785d9493d46e3907d49465391fb
dec:pkts/bytes=64/2560, enc:pkts/bytes=0/0
npu_flag=00 npu_rgwy=192.2.0.9 npu_igwy=100.64.1.9 npu_selid=6 dec_npuid=0 enc_npuid=0
```

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

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

Answer: AC

NEW QUESTION 9

Refer to the exhibit.

```
config system interface
  edit "port2"
    set vdom "root"
    set ip 192.2.0.9 255.255.255.248
    set allowaccess ping
    set type physical
    set role wan
    set snmp-index 2
    set preserve-session-route enable
  next
end
```

Based on the exhibit, which two actions does FortiGate perform on traffic passing through port2? (Choose two.)

- A. FortiGate does not change the routing information on existing sessions that use a valid gateway, after a route change.
- B. FortiGate performs routing lookups for new sessions only, after a route change.
- C. FortiGate always blocks all traffic, after a route change.
- D. FortiGate flushes all routing information from the session table, after a route change.

Answer: AB

NEW QUESTION 10

Refer to the exhibit.

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

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

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

Answer: B

NEW QUESTION 10

Which two statements about SLA targets and SD-WAN rules are true? (Choose two.)

- A. SD-WAN rules use SLA targets to check if the preferred members meet the SLA requirements
- B. Member metrics are measured only if an SLA target is configured
- C. When configuring an SD-WAN rule you can select multiple SLA targets of the same performance SLA
- D. SLA targets are used only by SD-WAN rules that are configured with Lowest Cost (SLA) or Maximize Bandwidth (SLA) as strategy

Answer: AD

NEW QUESTION 15

Which statement about using BGP for ADVPN is true?

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

Answer: D

Explanation:

ADVPN is a technology that allows dynamic creation of IPsec tunnels between branch sites without requiring pre-configured policies or keys. BGP is a routing protocol that can be used to exchange routes between ADVPN peers. IBGP is a type of BGP that runs between routers in the same autonomous system (AS), while EBGP is a type of BGP that runs between routers in different ASes. IBGP is preferred over EBGP for ADVPN, because IBGP preserves the next hop information of the routes, which is needed to establish the IPsec tunnels. EBGP changes the next hop information to the EBGP peer address, which may not be reachable by the ADVPN peers. Therefore, using IBGP for ADVPN avoids the need to configure additional static routes or redistribute routes between BGP and another routing protocol. References = ADVPN with BGP as the routing protocol, ADVPN, SD-WAN self-healing with BGP, Technical Tip: ADVPN with BGP as the routing protocol

The statement that IBGP is preferred over EBGP for ADVPN because IBGP preserves next hop information (D) is true. In a typical ADVPN deployment, it's beneficial to maintain next hop information across the network to ensure proper routing and optimal path selection. References: This understanding comes from my knowledge of Fortinet's SD-WAN and ADVPN configurations, where BGP's behavior in terms of next hop preservation is a key consideration.

NEW QUESTION 16

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: C

NEW QUESTION 19

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

Explanation:

* B. Provide internet access through the hub: This involves routing branch or remote office internet traffic through a central hub, ensuring consistent security policies and possibly better management of network resources.

* C. Centralize security inspection on the hub: With this approach, all internet-bound traffic from various spokes is inspected at the hub, leveraging centralized security mechanisms for thorough inspection and policy enforcement.

NEW QUESTION 20

Refer to the exhibits. Exhibit A -

Edit Traffic Shaping Policy

IP Version: IPv4 IPv6

Name: Limit_YouTube

Status: Enable Disable

Comments: 0/255

If Traffic Matches:

Source Internet Service:

Source Address: LAN-net

Source User: +

Source User Group: +

Destination Internet Service:

Destination Address: all

Schedule: +

Service: ALL

Application: YouTube

Application Category: +

Application Group: +

URL Category: +

Type Of Service: 0x00

Type Of Service Mask: 0x00

Then:

Action: Apply Shaper Assign Group

Outgoing Interface: underlay

Shared Shaper: low-priority

Reverse Shaper: low-priority

Per-IP Shaper: +

Differentiated Services:

Differentiated Services Reverse:

Exhibit B -

Edit Firewall Policy

ID: 1

Name: DIA

ZTNA: Disable Full ZTNA IP/MAC filtering

Incoming Interface: LAN

Outgoing Interface: underlay

Source Internet Service:

IPv4 Source Address: LAN-net

IPv6 Source Address: +

Source User: +

Source User Group: +

FSSO Groups: +

Destination Internet Service:

IPv4 Destination Address: all

IPv6 Destination Address: +

Service: ALL

Schedule: always

Action: Deny Accept IPSEC

Inspection Mode: Flow-based Proxy-based

Firewall/Network Options

NAT: NAT NAT46 NAT64

IP Pool Configuration: Use Outgoing Interface Address Use Dynamic IP Pool

Preserve Source Port:

Protocol Options: default

Disclaimer Options

Display Disclaimer:

Security Profiles:

SSL/SSH Inspection: deep-inspection

Decrypted Traffic Mirror: +

Traffic Shaping Options

Shared Shaper: +

Reverse Shaper: +

Per-IP Shaper: +

Logging Options

Log Allowed Traffic: No Log Log Security Events Log All Sessions

Capture Packets

Generate Logs when Session Starts

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

The administrator wants FortiGate to limit the bandwidth used by YouTube. When testing, the administrator determines that FortiGate does not apply traffic shaping on YouTube traffic.

Based on the policies shown in the exhibits, what configuration change must be made so FortiGate performs traffic shaping on YouTube traffic?

- A. Destination internet service must be enabled on the traffic shaping policy.
- B. Application control must be enabled on the firewall policy.
- C. Web filtering must be enabled on the firewall policy.
- D. Individual SD-WAN members must be selected as the outgoing interface on the traffic shaping policy.

Answer: C

NEW QUESTION 21

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), health-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 and T_MPLS_0 have the same latency.
- B. When T_MPLS_0 has a latency of 100 ms.
- C. When T_INET_0_0 has a latency of 250 ms.
- D. When T_MPLS_0 has a latency of 80 ms.

Answer: D

NEW QUESTION 25

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. It automatically install IPsec tunnels to every spoke when they are added to the FortiManager ADOM.
- D. The VPN monitor tool provides additional statistics for tunnels defined with an IPsec recommended template.

Answer: AB

Explanation:

The use of an IPsec recommended template offers the advantage of ensuring consistent settings between phase1 and phase2 (A), which is essential for the stability and security of the IPsec tunnel. Additionally, it guides the administrator to use Fortinet's recommended settings (B), which are designed to optimize performance and security based on Fortinet's best practices. References: The benefits of using IPsec recommended templates are outlined in Fortinet's SD-WAN documentation, which emphasizes the importance of consistency and adherence to recommended configurations.

NEW QUESTION 29

Refer to the exhibit.

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

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

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

Answer: AB

NEW QUESTION 34

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 35

In a hub-and-spoke topology, what are two advantages of enabling ADVPN on the IPsec overlays? (Choose two.)

- A. It provides the benefits of a full-mesh topology in a hub-and-spoke network.
- B. It provides direct connectivity between spokes by creating shortcuts.
- C. It enables spokes to bypass the hub during shortcut negotiation.
- D. It enables spokes to establish shortcuts to third-party gateways.

Answer: AB

NEW QUESTION 38

Refer to the exhibits. Exhibit A -

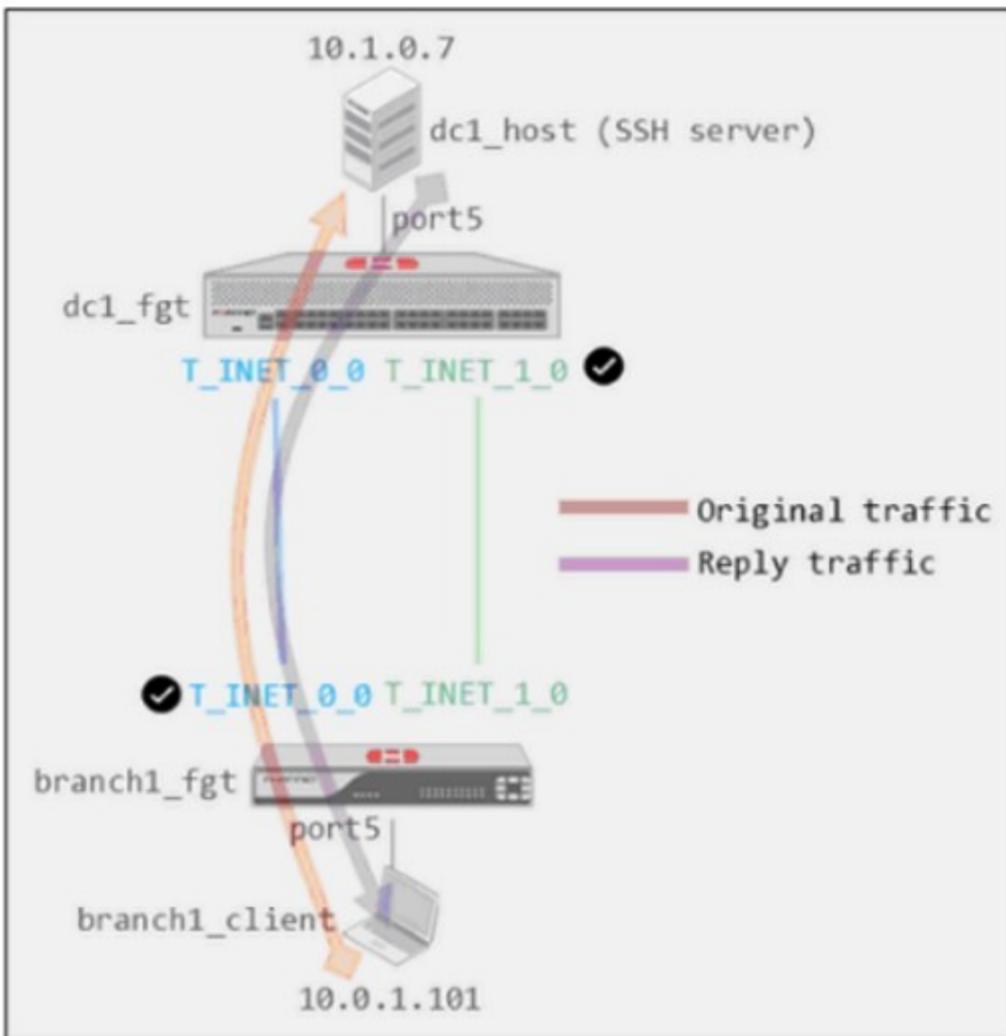


Exhibit B -

```

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

NEW QUESTION 39

In the default SD-WAN minimum configuration, which two statements are correct when traffic matches the default implicit SD-WAN rule? (Choose two)

- A. Traffic has matched none of the FortiGate policy routes.
- B. Matched traffic failed RPF and was caught by the rule.
- C. The FIB lookup resolved interface was the SD-WAN interface.
- D. An absolute SD-WAN rule was defined and matched traffic.

Answer: AC

NEW QUESTION 44

Refer to the exhibit.

```

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

Based on the exhibit, which action does FortiGate take?

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

Answer: A

NEW QUESTION 47

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. Create policy packages for branch devices.
- B. Assign an sdwan_id metadata variable to each device (branch and hub).
- C. Configure routing through overlay tunnels created by the SD-WAN overlay template.
- D. Assign a branch_id metadata variable to each branch device.
- E. Configure SD-WAN rules.

Answer: ABC

NEW QUESTION 52

Refer to the exhibits. Exhibit A -

Edit Performance SLA

Name: Level3_DNS

IP Version: **IPv4** IPv6

Probe Mode: **Active** Passive Prefer Passive

Protocol: **Ping** TCP ECHO UDP ECHO HTTP TW

Server: 4.2.2.1
4.2.2.2

Participants: All SD-WAN Members **Specify**

port1
port2
2 Entries

Enable Probe Packets:

SLA Targets: **+ Add Target**

Link Status

Interval: 500 Milliseconds

Failure Before Inactive: 3 (max 3600)

Restore Link After: 2 (max 3600)

Action When Inactive

Update Static Route:

Cascade Interfaces:

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.

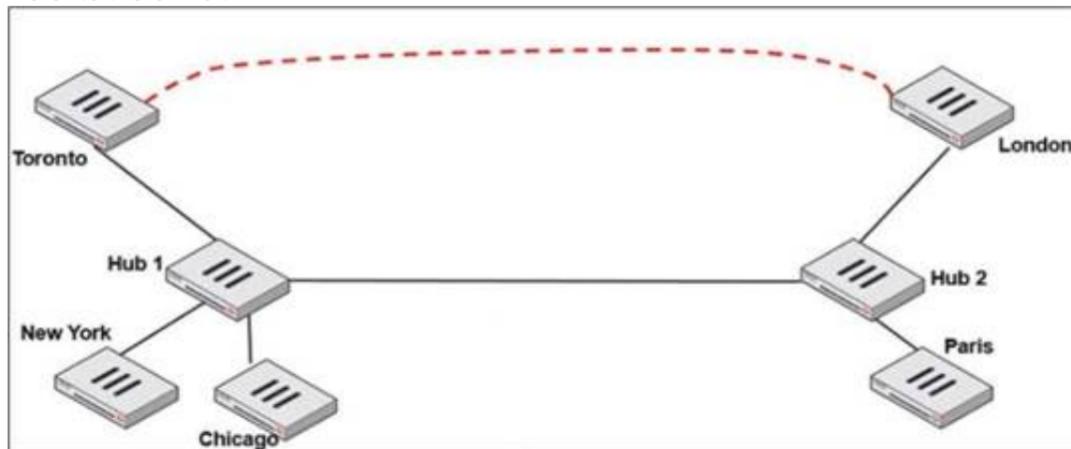
Answer: B

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 53

Refer to the exhibit.



Two hub-and-spoke groups are connected through a site-to-site IPsec VPN between Hub 1 and Hub 2. Which two configuration settings are required for Toronto and London spokes to establish an ADVPN shortcut? (Choose two.)

- A. On the hubs, auto-discovery-sender must be enabled on the IPsec VPNs to spokes.
- B. On the spokes, auto-discovery-receiver must be enabled on the IPsec VPN to the hub.
- C. auto-discovery-forwarder must be enabled on all IPsec VPNs.
- D. On the hubs, net-device must be enabled on all IPsec VPNs.

Answer: AB

NEW QUESTION 57

What are two benefits of choosing packet duplication over FEC for data loss correction on noisy links? (Choose two.)

- A. Packet duplication can leverage multiple IPsec overlays for sending additional data.
- B. Packet duplication does not require a route to the destination.
- C. Packet duplication supports hardware offloading.
- D. Packet duplication uses smaller parity packets which results in less bandwidth consumption.

Answer: AC

NEW QUESTION 60

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

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

Answer: BD

NEW QUESTION 62

Which statement is correct about SD-WAN and ADVPN?

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

Answer: B

NEW QUESTION 67

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 68

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

NSE7_SDW-7.2 Practice Exam Features:

- * NSE7_SDW-7.2 Questions and Answers Updated Frequently
- * NSE7_SDW-7.2 Practice Questions Verified by Expert Senior Certified Staff
- * NSE7_SDW-7.2 Most Realistic Questions that Guarantee you a Pass on Your First Try
- * NSE7_SDW-7.2 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The NSE7_SDW-7.2 Practice Test Here](#)