

# 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.Portals(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.

```
# get router info routing-table all
...
B      10.0.2.0/24 [200/0] via 10.201.1.2 [3] (recursive via VPN0 tunnel 100.64.1.1), 00:00:54
        [200/0] via 10.202.1.2 [3] (recursive via VPN1 tunnel 100.64.1.9), 00:00:54
        [200/0] via 10.203.1.1 [3] (recursive via VPN2 tunnel 172.16.1.5), 00:00:54
...
```

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. additional-path is enabled.
- D. You can run the get router info routing-table database command to display the additional paths.

**Answer:** CD**NEW QUESTION 3**

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.

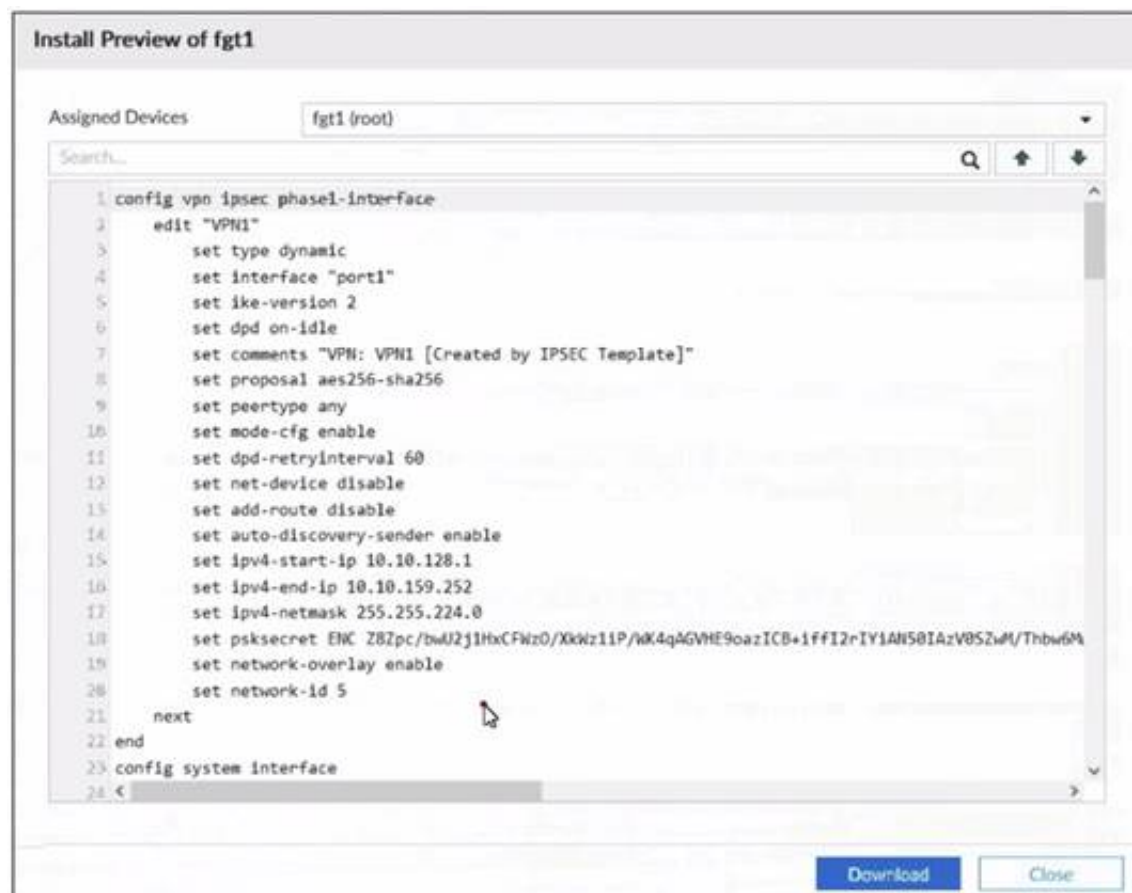
**Answer:** BD**NEW QUESTION 4**

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

- A. FEC supports hardware offloading.
- B. FEC improves reliability of noisy links.
- C. FEC transmits parity packets that can be used to reconstruct packet loss.
- D. FEC can leverage multiple IPsec tunnels for parity packets transmission.

**Answer:** BC**NEW QUESTION 5**

Refer to the exhibit.



An administrator used the SD-WAN overlay template to prepare an IPsec configuration for a hub-and-spoke SD-WAN topology. The exhibit shows the installation preview for one FortiGate device. In the exhibit, which statement best describes the configuration applied to the FortiGate device?

- A. It is a hub device
- B. It can send ADVPN shortcut offers.
- C. It is a spoke device that establishes dynamic IPsec tunnels to the hu
- D. The subnet range is 10.10.128.0/23.
- E. It is a spoke device that establishes dynamic IPsec tunnels to the hu
- F. It can send ADVPN shortcut requests.
- G. It is a hub device and will automatically discover the spoke devices that are in the SD- WAN topology.

**Answer: C**

**Explanation:**

According to the SD-WAN 7.2 Study Guide, the SD-WAN overlay template simplifies the configuration of IPsec tunnels in a hub-and-spoke topology. The template defines the following parameters:

- ? type: dynamic for spokes, static for hubs
  - ? interface: the WAN interface to use for the IPsec tunnel
  - ? network-overlay: enable for spokes, disable for hubs
  - ? network-id: a unique identifier for each spoke
  - ? auto-discovery-sender: enable for hubs, disable for spokes
  - ? auto-discovery-receiver: enable for spokes, disable for hubs
- Based on the exhibit, the FortiGate device has the following configuration:
- ? type: dynamic
  - ? interface: port1
  - ? network-overlay: enable
  - ? network-id: 5
  - ? auto-discovery-sender: disable
  - ? auto-discovery-receiver: enable

Therefore, the FortiGate device is a spoke that establishes dynamic IPsec tunnels to the hub. It also has the network-overlay and auto-discovery-receiver options enabled, which means it can send ADVPN shortcut requests to other spokes when it receives a shortcut offer from the hub

**NEW QUESTION 6**

Which best describes the SD-WAN traffic shaping mode that bases itself on a percentage of available bandwidth?

- A. Interface-based shaping mode
- B. Reverse-policy shaping mode
- C. Shared-policy shaping mode
- D. Per-IP shaping mode

**Answer: A**

**Explanation:**

Interface-based shaping goes further, enabling traffic controls based on percentage of the interface bandwidth.

**NEW QUESTION 7**

Refer to the exhibits.

**Exhibit A**

**Exhibit B**

Exhibit A shows two IPsec templates to define Branch\_IPsec\_1 and Branch\_IPsec\_2. Each template defines a VPN tunnel. Exhibit B shows the error message that FortiManager displayed when the administrator tried to assign the second template to the FortiGate device. Which statement best explain the cause for this issue?

- A. You can assign only one template with a tunnel of type static to each FortiGate device
- B. You can define only one IPsec tunnel from branch devices to HUB1.
- C. You can assign only one IPsec template to each FortiGate device.
- D. You should review the branch1\_fgt configuration for the already configured tunnel with the name HUB1-VPN2.

**Answer: C**

**Explanation:**

The error message in Exhibit B indicates a conflicting template assignment. This occurs because FortiManager does not allow the assignment of multiple IPsec templates that define VPN tunnels with the same name or settings to the same FortiGate device. The conflict arises from trying to assign a second IPsec template to a device that already has one assigned. References: This is based on Fortinet's best practices and administrative guidelines which state that each FortiGate device should be assigned a unique IPsec template to avoid configuration conflicts.

**NEW QUESTION 8**

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 9

What three characteristics apply to provisioning templates available on FortiManager? (Choose three.)

- A. You can apply a system template and a CLI template to the same FortiGate device.
- B. A CLI template can be of type CLI script or Perl script.
- C. A template group can include a system template and an SD-WAN template.
- D. A template group can contain CLI templates of both types.
- E. Templates are applied in order, from top to bottom.

**Answer:** BDE

#### Explanation:

According to the FortiManager Administration Guide, provisioning templates are used to configure FortiGate devices in a consistent and efficient way. There are different types of templates, such as system, IPsec, SD-WAN, certificate, and CLI templates. Some characteristics of provisioning templates are:

- ? You can apply a system template and a CLI template to the same FortiGate device, as long as they do not have conflicting settings<sup>1</sup>.
- ? A CLI template can be of type CLI script or Perl script. A CLI script template contains FortiOS CLI commands, while a Perl script template contains Perl code that can generate FortiOS CLI commands<sup>2</sup>.
- ? A template group can include a system template and an SD-WAN template, as well as other types of templates. A template group is a collection of templates that can be applied to multiple devices at once<sup>3</sup>.
- ? A template group can contain CLI templates of both types, as long as they do not have conflicting settings<sup>2</sup>.
- ? Templates are applied in order, from top to bottom. The order of the templates in a template group determines the order in which they are applied to the devices<sup>3</sup>.

### NEW QUESTION 10

Exhibit.

```
7: [...]logid="0101037141" type="event" subtype="vpn" level="notice" vd="root" logdesc="IPsec tunnel
statistics" msg="IPsec tunnel statistics" action="tunnel-stats" remip=100.64.1.9 locip=192.2.0.9
rempoort=500 locpoort=500 outintf="port2" cookies="773c72b40060051d/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
rempoort=500 locpoort=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
rempoort=500 locpoort=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=3560
sentbyte=388020 rcvdbyte=387994 nextstat=600 advpnsc=0
```

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

- A. There are no IPsec tunnel statistics log messages for ADVPN cuts.
- B. There is one shortcut tunnel built from master tunnel T\_MPLS\_0.
- C. The VPN tunnel T\_MPLS\_0 is a shortcut tunnel.
- D. The master tunnel T\_INET\_0 cannot accept the ADVPN shortcut.

**Answer:** B

#### Explanation:

VPN event logs record the status of VPN tunnels, such as the establishment, termination, or failure of a tunnel. The output includes the following information:

- ? logid: the log ID number
  - ? type: the log type, either traffic or event
  - ? subtype: the log subtype, either vpn or ipsec
  - ? level: the log level, either error, warning, or notice
  - ? vd: the virtual domain name
  - ? logdesc: the log description
  - ? msg: the log message
  - ? action: the log action, such as tunnel-up, tunnel-down, or tunnel-stats
  - ? remip: the remote IP address
  - ? locip: the local IP address
  - ? rempoort: the remote port number
  - ? locpoort: the local port number
  - ? outintf: the outgoing interface name
  - ? cookies: the IKE SA cookies
  - ? user: the user name
  - ? group: the user group name
  - ? useralt: the alternative user name
  - ? xauthuser: the XAuth user name
  - ? authgroup: the XAuth user group name
  - ? assignip: the assigned IP address
  - ? vpntunnel: the VPN tunnel name
  - ? tunnelip: the tunnel loopback IP address
  - ? tunnelid: the tunnel ID number
  - ? tunneltype: the tunnel type, either ipsec or ssl
  - ? duration: the tunnel duration in seconds
  - ? sentbyte: the number of bytes sent
  - ? rcvdbyte: the number of bytes received
  - ? nextstat: the next statistics interval in seconds
  - ? advpnsc: the ADVPN shortcut flag, either 0 or 1
- Based on the exhibit, the following statement is true:

? There is one shortcut tunnel built from master tunnel T\_MPLS\_0. This means that the VPN tunnel T\_MPLS\_0 is a master tunnel that can send ADVPN shortcut offers to other spokes, and the VPN tunnel T\_MPLS\_0\_0 is a shortcut tunnel that is built from the master tunnel T\_MPLS\_01. In the exhibit, the log action for T\_MPLS\_0 is tunnel-up, and the log action for T\_MPLS\_0\_0 is shortcut-up. The advpnsc flag for T\_MPLS\_0 is 0, indicating that it is not a shortcut tunnel, while the advpnsc flag for T\_MPLS\_0\_0 is 1, indicating that it is a shortcut tunnel.

#### NEW QUESTION 10

Refer to the exhibit.

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

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

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

**Answer:** AB

#### NEW QUESTION 14

Which two protocols in the IPsec suite are most used for authentication and encryption? (Choose two.)

- A. Encapsulating Security Payload (ESP)
- B. Secure Shell (SSH)
- C. Internet Key Exchange (IKE)
- D. Security Association (SA)

**Answer:** AC

#### NEW QUESTION 19

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 22

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 27

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



Exhibit A
Exhibit B

### Edit Policy

Name
Internet Access

Incoming interface
port3

Outgoing interface
virtual-wan link

Source
all
+
x

Destination
all
+
x

Schedule
always

Service
ALL
+
x

Action
ACCEPT
DENY

Inspection Mode
Flow-based
Proxy-based

### Firewall / Network Options

NAT
☒

IP Pool Configuration
Use Outgoing Interface Address
Use Dynamic

Preserve Source Port
☐

Protocol Options
PROT default

Exhibit A
Exhibit B

### Edit Traffic Shaping Policy

Name
inbound\_outbound\_shaper

Status
Enabled
Disabled

Comments
Write a comment...
0/255

### If Traffic Matches:

Source
all
+
x

Destination
all
+
x

Schedule
☐

Service
ALL
+
x

Application
+

URL Category
Streaming Media and Download
+
x

### Then:

Action
Apply Shaper
Assign Shaping Class ID

Outgoing interface
virtual-wan link
+
x

Shared shaper
☒
guarantee-10mbps

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

- Create a new firewall policy, and then select the SD-WAN zone as Incoming Interface.
- In the traffic shaping policy, select Assign Shaping Class ID as Action.
- In the firewall policy, select Proxy-based as Inspection Mode.
- In the traffic shaping policy, enable Reverse shaper, and then select the traffic shaper to use.



Answer: D

**NEW QUESTION 31**

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

- A. VPN monitor tool provides additional statistics for tunnels defined with an IPsec recommended template.
- B. FortiManager automatically installs IPsec tunnels to every spoke when they are added to the FortiManager ADOM.
- C. IPsec recommended template guides the administrator to use Fortinet recommended settings.
- D. IPsec recommended template ensures consistent settings between phase1 and phase2

Answer: BC

**Explanation:**

According to the SD-WAN 7.2 Study Guide, IPsec recommended templates are designed to simplify the configuration of IPsec tunnels in a hub-and-spoke topology. They have the following advantages:

? FortiManager automatically installs IPsec tunnels to every spoke when they are added to the FortiManager ADOM. This reduces the manual effort and ensures that all spokes have the same configuration.

? IPsec recommended template guides the administrator to use Fortinet recommended settings, such as encryption algorithms, key lifetimes, and dead peer detection. This ensures optimal performance and security of the IPsec tunnels.

**NEW QUESTION 36**

Refer to the exhibit.

```
ike 0:T_INET_0_0:214: received informational request
ike 0:T_INET_0_0:214: processing notify type SHORTCUT_QUERY
ike 0:T_INET_0_0: recv shortcut-query 9065761962601467474
07409008f7fbd17e/0000000000000000 192.2.0.1 10.0.1.101->10.0.2.101 psk 64 ppk 0 ttl 32
nat 0 ver 2 mode 0
ike 0:T_INET_0: iif 20 10.0.1.101->10.0.2.101 route lookup oif 20 T_INET_0 gwy
10.201.1.1
ike 0:T_INET_0_1: forward shortcut-query 9065761962601467474
07409008f7fbd17e/0000000000000000 192.2.0.1 10.0.1.101->10.0.2.101 psk 64 ppk 0 ttl 31
ver 2 mode 0, ext-mapping 192.2.0.1:500
```

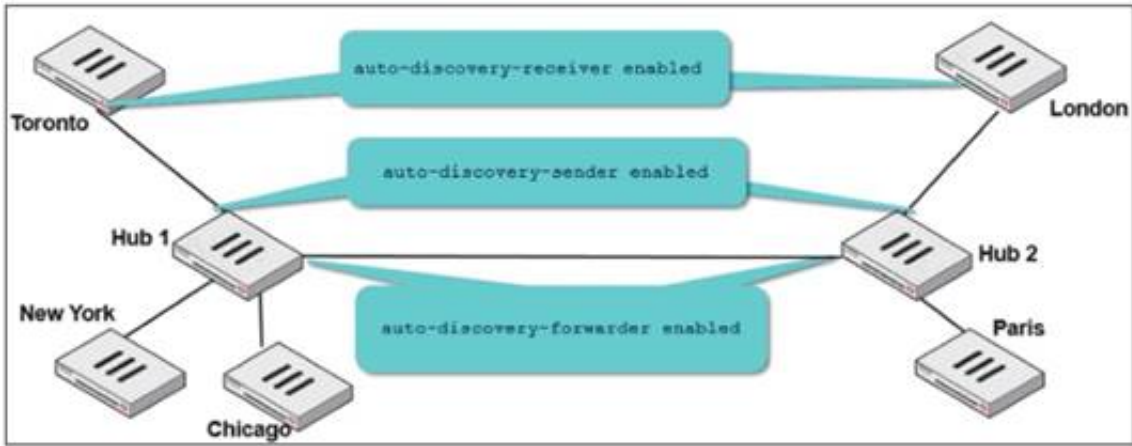
Which statement about the role of the ADVPN device in handling traffic is true?

- A. This is a spoke that has received a query from a remote hub and has forwarded the response to its hub.
- B. Two hubs, 10.0.1.101 and 10.0.2.101, are receiving and forwarding queries between each other.
- C. This is a hub that has received a query from a spoke and has forwarded it to another spoke.
- D. Two spokes, 192.2.0.1 and 10.0.2.101, forward their queries to their hubs.

Answer: C

**NEW QUESTION 38**

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 41**

.....

## 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 FirstTry
- \* NSE7\_SDW-7.2 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The NSE7\\_SDW-7.2 Practice Test Here](#)**