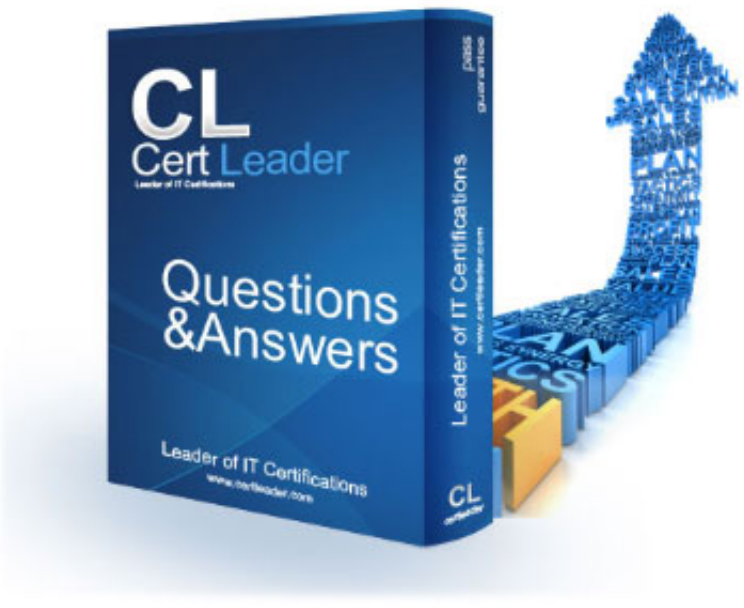
NSE7_SDW-7.2 Dumps

Fortinet NSE 7 - SD-WAN 7.2

https://www.certleader.com/NSE7_SDW-7.2-dumps.html



NEW QUESTION 1
Refer to the exhibits.
Exhibit A

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

Exhibit B

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

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

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

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

Answer: BD

NEW QUESTION 2
Which action fortigate performs on the traffic that is subject to a per-IP traffic shaper of 10 Mbps?

A. FortiGate applies traffic shaping to the original traffic direction only.
B. FortiGate shares 10 Mbps of bandwidth equally among all source IP addresse
C. RIAS
D. Fortigate limits each source ip address to a maximum bandwidth of 10 Mbps.
E. FortiGate guarantees a minimum of 10 Mbps of bandwidth to each source IP address.

Answer: C

NEW QUESTION 3
What is a benefit of using application steering in SD-WAN?

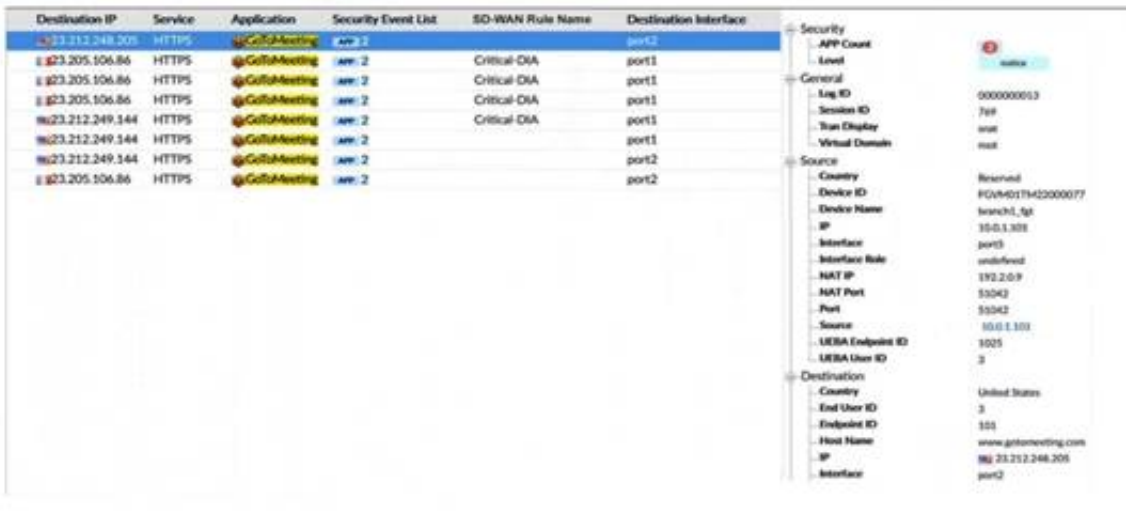
A. The traffic always skips the regular policy routes.
B. You steer traffic based on the detected application.
C. You do not need to enable SSL inspection.
D. You do not need to configure firewall policies that accept the SD-WAN traffic.

Answer: B

NEW QUESTION 4
Refer to the exhibits.
Exhibit A

```
branch1_fgt # diagnose sys sdwan service

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


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

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

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

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

Exhibit B



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

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

Answer: BC

Explanation:
Study guide 7.2 Page 191

NEW QUESTION 5
Refer to the exhibits.
Exhibit A

Exhibit B

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

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

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

A. FortiGate updated the outgoing interface list on the rule so it prefers port2.
B. Port2 has the highest member priority.

C. Port2 has a lower latency than port1.
D. SD-WAN rule ID 1 is set to lowest cost (SLA) mode.

Answer: AC

NEW QUESTION 6
Refer to the exhibits.

Exhibit A

```
branch1_fgt # diagnose sys sdwan service 1

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

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

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

Total number of prefixes 1
```

Exhibit B

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

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

Exhibit A shows the SD-WAN rule status and the learned BGP routes with community 65000:10.
Exhibit B shows the SD-WAN rule configuration, the BGP neighbor configuration, and the route map configuration.
The administrator wants to steer corporate traffic using routes tags in the SD-WAN rule ID 1.
However, the administrator observes that the corporate traffic does not match the SD-WAN rule ID 1.
Based on the exhibits, which configuration change is required to fix issue?

A. In the dcl-lab-rm route map configuration, set set-route-tag to 10.
B. In SD-WAN rule ID 1, change the destination to use ISDB entries.
C. In the BGP neighbor configuration, apply the route map dcl-lab-rm in the outbound direction.
D. In the dcl-lab-rm route map configuration, unset match-community.

Answer: C

NEW QUESTION 7
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 8
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 reply direction of the asymmetric traffic flows from port2 to port3.
B. The auxiliary session can be offloaded to hardware.
C. The original direction of the symmetric traffic flows from port3 to port2.
D. The main session cannot be offloaded to hardware.

Answer: AB

NEW QUESTION 9
Exhibit A –

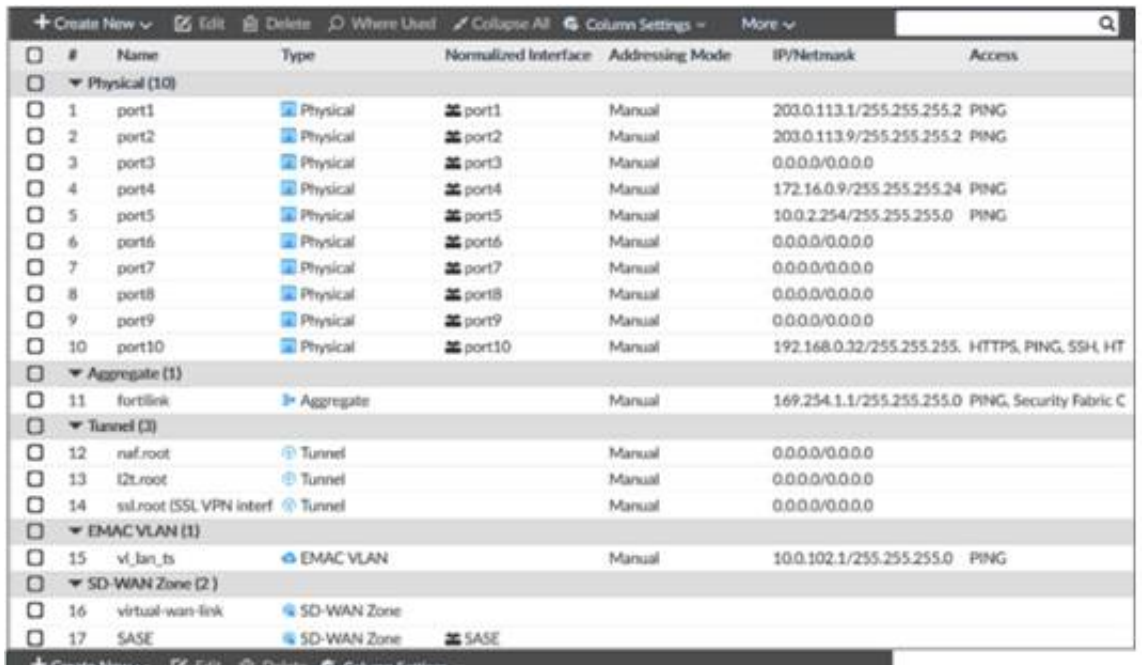


Exhibit B –

Exhibit A shows the system interface with the static routes and exhibit B shows the firewall policies on the managed FortiGate.
Based on the FortiGate configuration shown in the exhibits, what issue might you encounter when creating an SD-WAN zone for port1 and port2?

A. port1 is assigned a manual IP address.
B. port1 is referenced in a firewall policy.
C. port2 is referenced in a static route.
D. port1 and port2 are not administratively down.

Answer: B

NEW QUESTION 10
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 10
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 settings1.
? 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 commands2.
? 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 once3.
? A template group can contain CLI templates of both types, as long as they do not have conflicting settings2.
? 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 devices3.

NEW QUESTION 13
Which two performance SLA protocols enable you to verify that the server response contains a specific value? (Choose two.)

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

Answer: AD

Explanation:
Performance SLA (Service Level Agreement) protocols are used in SD-WAN to monitor the quality and performance of various network services. The two protocols that specifically allow for verifying a specific value in the server response are:
? HTTP (Hypertext Transfer Protocol): HTTP is the foundation of data communication on the World Wide Web. It allows for fetching resources, such as HTML documents. You can configure an HTTP performance SLA to send specific requests (e.g., GET or POST) and then check if the response body contains a particular string or value. This is useful for validating web server functionality and content delivery.
? DNS (Domain Name System): DNS is responsible for translating domain names into IP addresses. A DNS performance SLA can be set up to query a specific domain and verify that the returned IP address or other DNS record values match what is expected. This helps ensure proper name resolution and accessibility of

resources.

NEW QUESTION 14
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 16
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 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_N1PLS_0 has a latency of 80 ms.

Answer: D

NEW QUESTION 21
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 26
Which two statements are correct when traffic matches the implicit SD-WAN rule? (Choose two.)

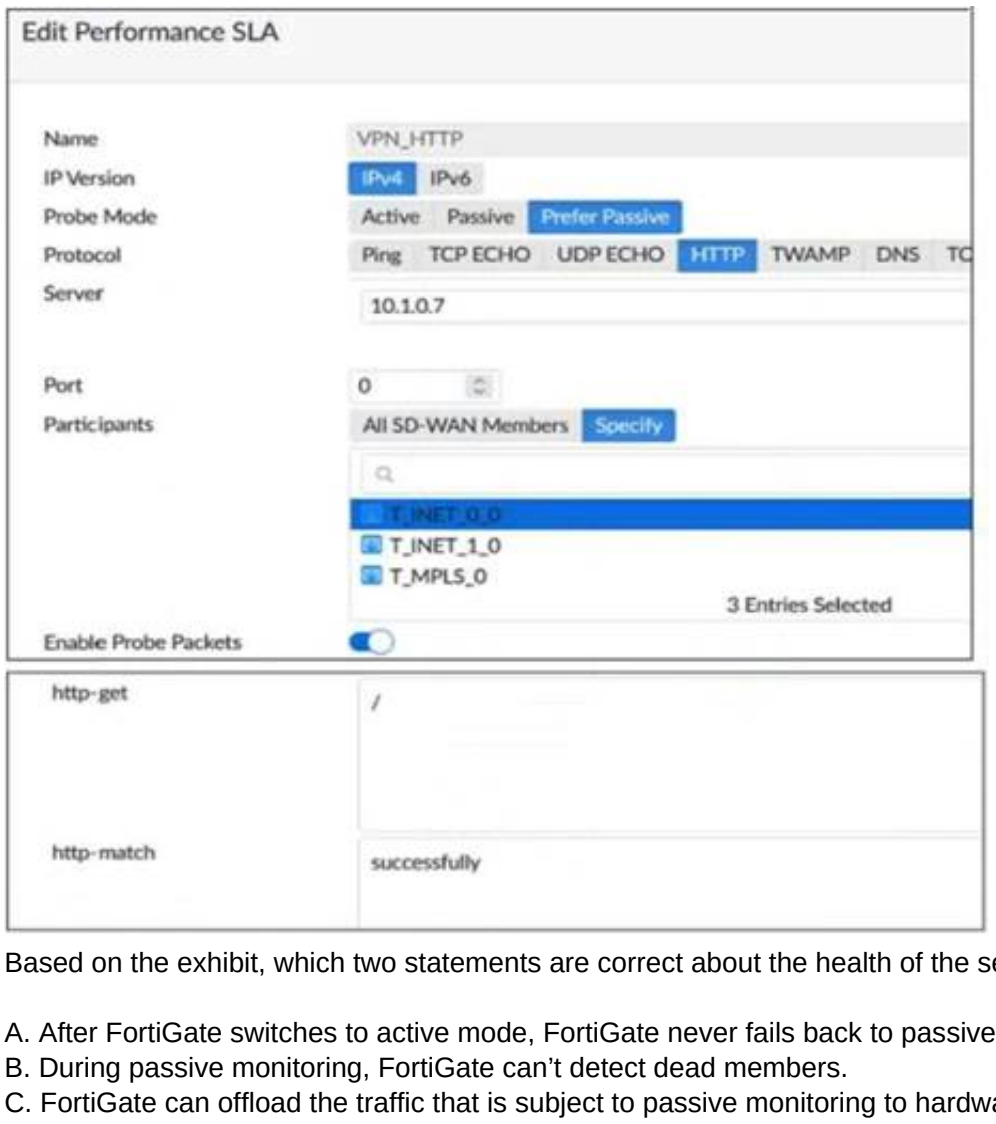
A. The sdwan_service_id flag in the session information is 0.
B. All SD-WAN rules have the default setting enabled.
C. Traffic does not match any of the entries in the policy route table.
D. Traffic is load balanced using the algorithm set for the v4-ecmp-mode setting.

Answer: AC

Explanation:
sdwan_service_id is 0 = match SD-WAN implicit rule, study guide 7.0 page 120, 7.2 page 149 SD-WAN rules internally are interpreted as a Policy route, so when the traffic doesn't match with any policy route, it will be flowing by implict policy.

NEW QUESTION 30

Refer to the exhibit.



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

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

Answer: BD

NEW QUESTION 34
Refer to the exhibits. Exhibit A -

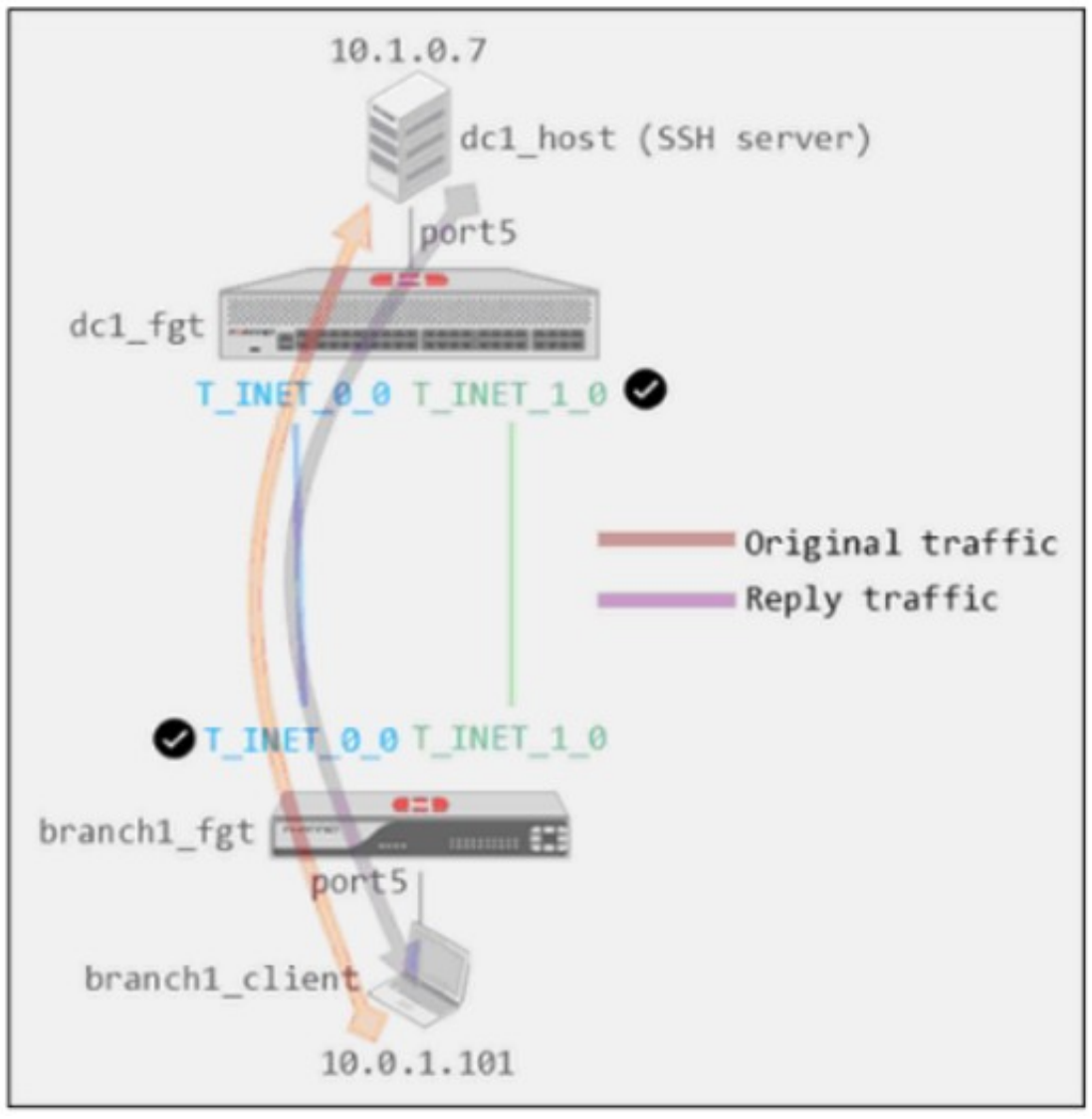


Exhibit B -

```
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 38
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 39
Which CLI command do you use to perform real-time troubleshooting for ADVPN negotiation?

A. get router info routing-table all
B. diagnose debug application ike
C. diagnose vpn tunnel list
D. get ipsec tunnel list

Answer: B

Explanation:
IKE real-time debug - useful when debugging ADVPN shortcut messages and spoke-to- spoke negotiations.
• diagnose debug console timestamp enable
• diagnose vpn ike log filter clear
• diagnose vpn ike log filter mdst-addr4 <ip.of.hub> <ip.of.spoke>
• diagnose debug application ike -1
• diagnose debug enable

NEW QUESTION 44
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 49
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 51
Which two interfaces are considered overlay links? (Choose two.)

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

Answer: BD

NEW QUESTION 53
Which are three key routing principles in SD-WAN? (Choose three.)

A. FortiGate performs route lookups for new sessions only.
B. Regular policy routes have precedence over SD-WAN rules.
C. SD-WAN rules have precedence over ISDB routes.
D. By default, SD-WAN members are skipped if they do not have a valid route to thedestination.
E. By default, SD-WAN rules are skipped if the best route to the destination is not an SD- WAN member.

Answer: BDE

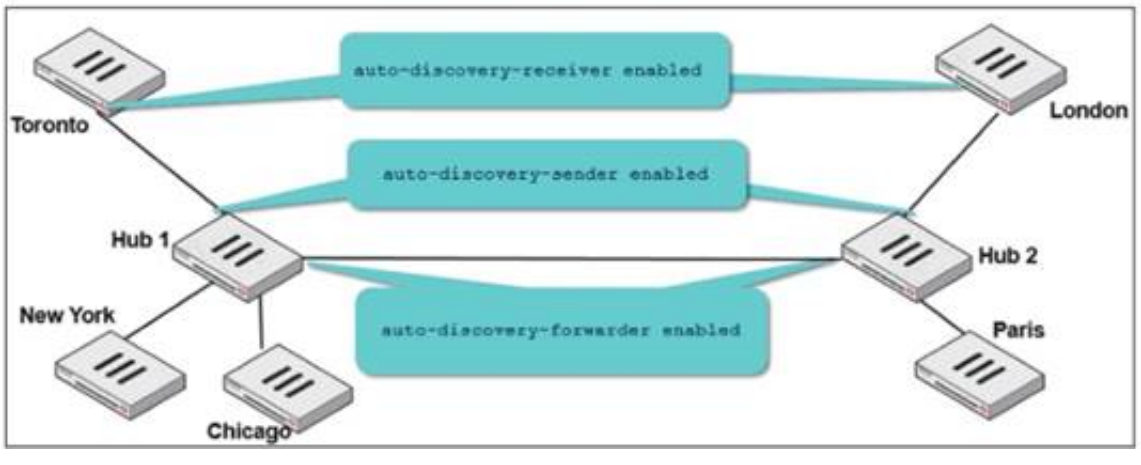
Explanation:
Study Guide 7.2, pages 125, 129, 151

NEW QUESTION 57
Which statement about using BGP routes in SD-WAN is true?

A. Learned routes can be used as dynamic destinations in SD-WAN rules.
B. You must use BGP to route traffic for both overlay and underlay links.
C. You must configure AS path prepending.
D. You must use external BGP.

Answer: A

NEW QUESTION 61
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 63
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 65
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your NSE7_SDW-7.2 Exam with Our Prep Materials Via below:

https://www.certleader.com/NSE7_SDW-7.2-dumps.html