# NSE7_SDW-7.0 Dumps

Fortinet NSE 7 - SD-WAN 7.0

https://www.certleader.com/NSE7_SDW-7.0-dumps.html
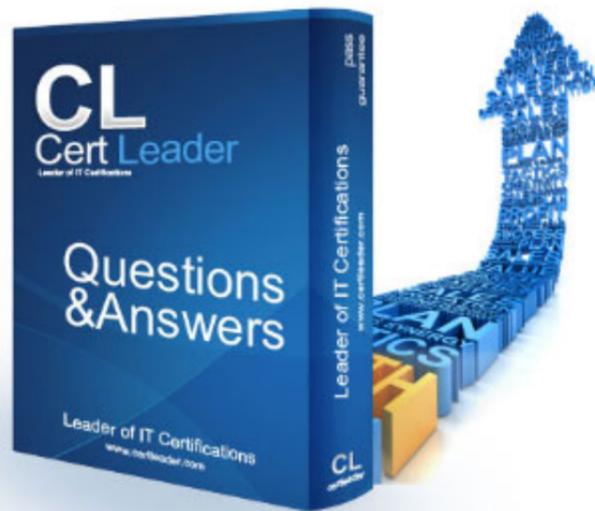
NEW QUESTION 1
Refer to the exhibit.
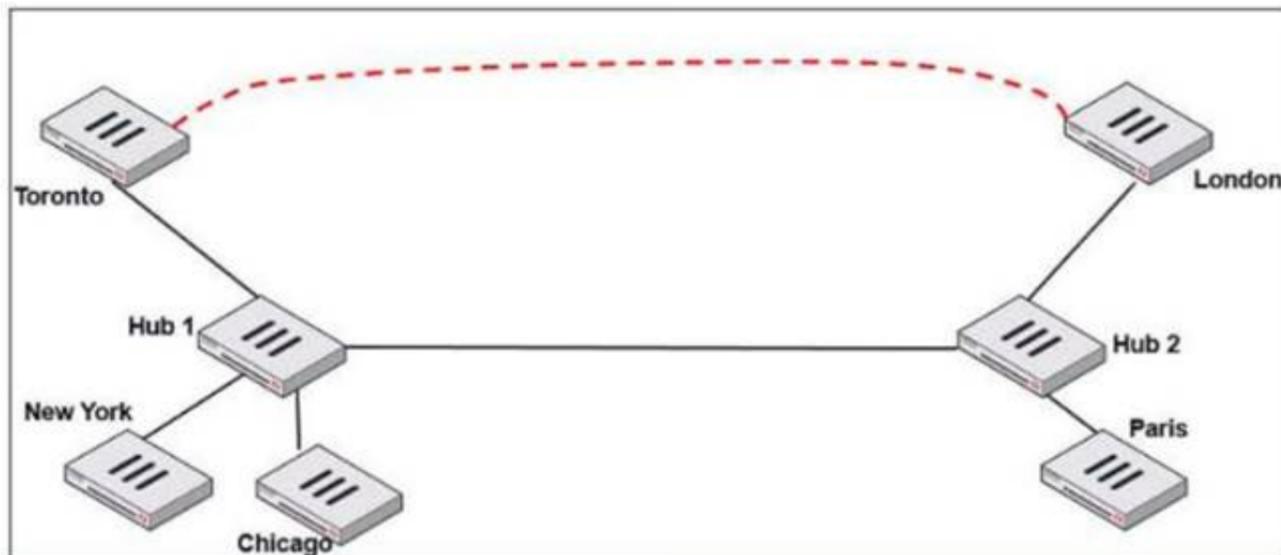
Two hub-and-spoke groups are connected through a site-to-site IPsec VPN between Hub 1 and Hub 2. Which two configuration settings are required for Toronto and London spokes to establish an ADVPN
shortcut? (Choose two.)

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 2
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 3
Which two statements about SLA targets and SD-WAN rules are true? (Choose two.)

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

Answer: BC

NEW QUESTION 4
What are two reasons for using FortiManager to organize and manage the network for a group of FortiGate devices? (Choose two)

A. It simplifies the deployment and administration of SD-WAN on managed FortiGate devices.
B. It improves SD-WAN performance on the managed FortiGate devices.
C. It sends probe signals as health checks to the beacon servers on behalf of FortiGate.
D. It acts as a policy compliance entity to review all managed FortiGate devices.
E. It reduces WAN usage on FortiGate devices by acting as a local FortiGuard server.

Answer: AE

NEW QUESTION 5
Refer to the exhibit.

```
branch1_fgt # diagnose sys sdwan service 3

Service(3): Address Mode(IPV4) flags=0x200 use-shortcut-sla
  Gen(2), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(priority), link-cost-factor(packet-
loss), link-cost-threshold(0), heath-check(VPN_PING)
  Members(3):
    1: Seq_num(3 T_INET_0_0), alive, packet loss: 2.000%, selected
    2: Seq_num(4 T_MPLS_0), alive, packet loss: 4.000%, selected
    3: Seq_num(5 T_INET_1_0), alive, packet loss: 12.000%, selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        10.0.0.0-10.255.255.255

branch1_fgt (3) # show
config service
    edit 3
        set name "Corp"
        set mode priority
        set dst "Corp-net"
        set src "LAN-net"
        set health-check "VPN_PING"
        set link-cost-factor packet-loss
        set link-cost-threshold 0
        set priority-members 5 3 4
    next
end
```

The exhibit shows the SD-WAN rule status and configuration.
Based on the exhibit, which change in the measured packet loss will make T_INET_1_0 the new preferred member?

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

Answer: A

NEW QUESTION 6
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 7
Refer to the exhibit.

```
FortiGate # diagnose sys session list

session info: proto=1 proto_state=00 duration=25 expire=34 timeout=0 flags=00000000
socktype=0 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=dirty may_dirty
statistic(bytes/packets/allow_err): org=84/1/1 reply=84/1/1 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=5->4/4->5 gwy=192.168.73.2/10.0.1.10
hook=post dir=org act=snat 10.0.1.10:2246->8.8.8.8:8(192.168.73.132:62662)
hook=pre dir=reply act=dnat 8.8.8.8:62662->192.168.73.132:0(10.0.1.10:2246)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00000a2c tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id= 80000000 rpdb_svc_id=0 ngfwid=n/a
npu_state=0x040000
total_session 1
```

Based on the exhibit, which statement about FortiGate re-evaluating traffic is true?

A. The type of traffic defined and allowed on firewall policy ID 1 is UDP.
B. FortiGate has terminated the session after a change on policy ID 1.
C. Changes have been made on firewall policy ID 1 on FortiGate.
D. Firewall policy ID 1 has source NAT disabled.

Answer: C

NEW QUESTION 8
What are two reasons why FortiGate would be unable to complete the zero-touch provisioning process? (Choose two.)

A. The FortiGate cloud key has not been added to the FortiGate cloud portal.
B. FortiDeploy has connected with FortiGate and provided the initial configuration to contact FortiManager
C. The zero-touch provisioning process has completed internally, behind FortiGate.
D. FortiGate has obtained a configuration from the platform template in FortiGate cloud.
E. A factory reset performed on FortiGate.

Answer: AC

NEW QUESTION 9
Refer to the exhibits.
Exhibit A

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

Exhibit B

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

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

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

A. FortiGate flags the sessions as dirty.
B. FortiGate continues routing the sessions with no SNAT, over port2.

C. FortiGate performs a route lookup for the original traffic only.
D. FortiGate updates the gateway information of the sessions with SNAT so that they use port1 instead of port2.

Answer: AD

NEW QUESTION 10
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

NEW QUESTION 10
Refer to the exhibits. Exhibit A

```
config system sdwan
    config health-check
        edit "Passive"
            set detect-mode passive
            set members 3 4
        next
    end
end

config system sdwan
    config service
        edit 1
            set name "Facebook-YouTube"
            set src "all"
            set internet-service enable
            set internet-service-app-ctrl 15832 31077
            set health-check "Passive"
            set priority-member 3 4
            set passive-measurement enable
        next
    end
end

branch1_fgt # get application name status | grep "id: 15832" -B1
app-name: "Facebook"
id: 15832

branch1_fgt # get application name status | grep "id: 31077" -B1
app-name: "YouTube"
id: 31077
```

Exhibit B

```
config firewall policy
    edit 1
        set name "DIA"
        set uuid b973e4ec-5f90-51ec-cadb-017c830d9418
        set srcintf "port5"
        set dstintf "underlay"
        set action accept
        set srcaddr "LAN-net"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set passive-wan-health-measurement enable
        set utm-status enable
        set ssl-ssh-profile "certificate-inspection"
        set application-list "default"
        set logtraffic all
        set auto-asic-offload disable
        set nat enable
    next
end

branch1_fgt # diagnose sys sdwan zone | grep underlay -A1
Zone underlay index=3
        members(2): 3(port1) 4(port2)
```

Exhibit A shows the SD-WAN performance SLA configuration, the SD-WAN rule configuration, and the application IDs of Facebook and YouTube. Exhibit B shows the firewall policy configuration and the underlay zone status.

Based on the exhibits, which two statements are correct about the health and performance of port1 and port2? (Choose two.)

A. The performance is an average of the metrics measured for Facebook and YouTube traffic passing through the member.
B. FortiGate is unable to measure jitter and packet loss on Facebook and YouTube traffic.
C. FortiGate identifies the member as dead when there is no Facebook and YouTube traffic passing through the member.
D. Non-TCP Facebook and YouTube traffic are not used for performance measurement.

Answer: AD

Explanation:
Study Guide 7.0, pages 88 - 89.
Study Guide 7.2, pages 103 - 104.
Another comment said "because without using application Control on the firewall policy, SDWAN can't work" but there is a app control "default" defined on config.

NEW QUESTION 13
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: B

NEW QUESTION 15
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
Which SD-WAN setting enables FortiGate to delay the recovery of ADVPN shortcuts?

A. hold-down-time
B. link-down-failover
C. auto-discovery-shortcuts
D. idle-timeout

Answer: A

NEW QUESTION 20
What are two benefits of using the Internet service database (ISDB) in an SD-WAN rule? (Choose two.)

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

Answer: AD

NEW QUESTION 25
Which two statements about SD-WAN central management are true? (Choose two.)

A. The objects are saved in the ADOM common object database.
B. It does not support meta fields.
C. It uses templates to configure SD-WAN on managed devices.
D. It supports normalized interfaces for SD-WAN member configuration.

Answer: AC

Explanation:
Normalized interfaces are not supported for SD-WAN templates. You can create multiple SD-WAN zones and add interface members to the SD-WAN zones. You must bind the interface members by name to physical interfaces or VPN interfaces.https://docs.fortinet.com/document/fortigate/7.0.0/sd-wan-new-features/794804/new-sd-wan-template

NEW QUESTION 28
Refer to the exhibit.

```
branch1_fgt # diagnose sys sdwan service 1

Service(3): Address Mode(IPV4) flags=0x200 use-shortcut-sla
  Gen(6), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(manual)
  Members(2):
    1: Seq_num(3 T_INET_0_0), alive, selected
    2: Seq_num(4 T_INET_1_0), alive, 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_0, flags=0x4 , gateway: 100.64.1.1, priority: 10 1024,
weight: 0
Member(4): interface: T_INET_1_0, flags=0x4 , gateway: 100.64.1.9, priority: 0 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_0 tunnel 100.64.1.9
```

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_0. However, the traffic is routed over T_INET_1_0.
Based on the output shown in the exhibit, which two reasons can cause the observed behavior? (Choose two.)

A. The traffic matches a regular policy route configured with T_INET_1_0 as the outgoing device.
B. T_INET_1_0 has a lower route priority value (higher priority) than T_INET_0_0.
C. T_INET_0_0 does not have a valid route to the destination.
D. T_INET_1_0 has a higher member configuration priority than T_INET_0_0.

Answer: AC

Explanation:
https://community.fortinet.com/t5/FortiGate/Technical-Tip-Assigning-Priority-to-SD-WAN-Members-for-Defau

NEW QUESTION 31
Which statement about using BGP for ADVPN is true?

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

Answer: A

NEW QUESTION 36
Refer to the exhibits.
Exhibit A
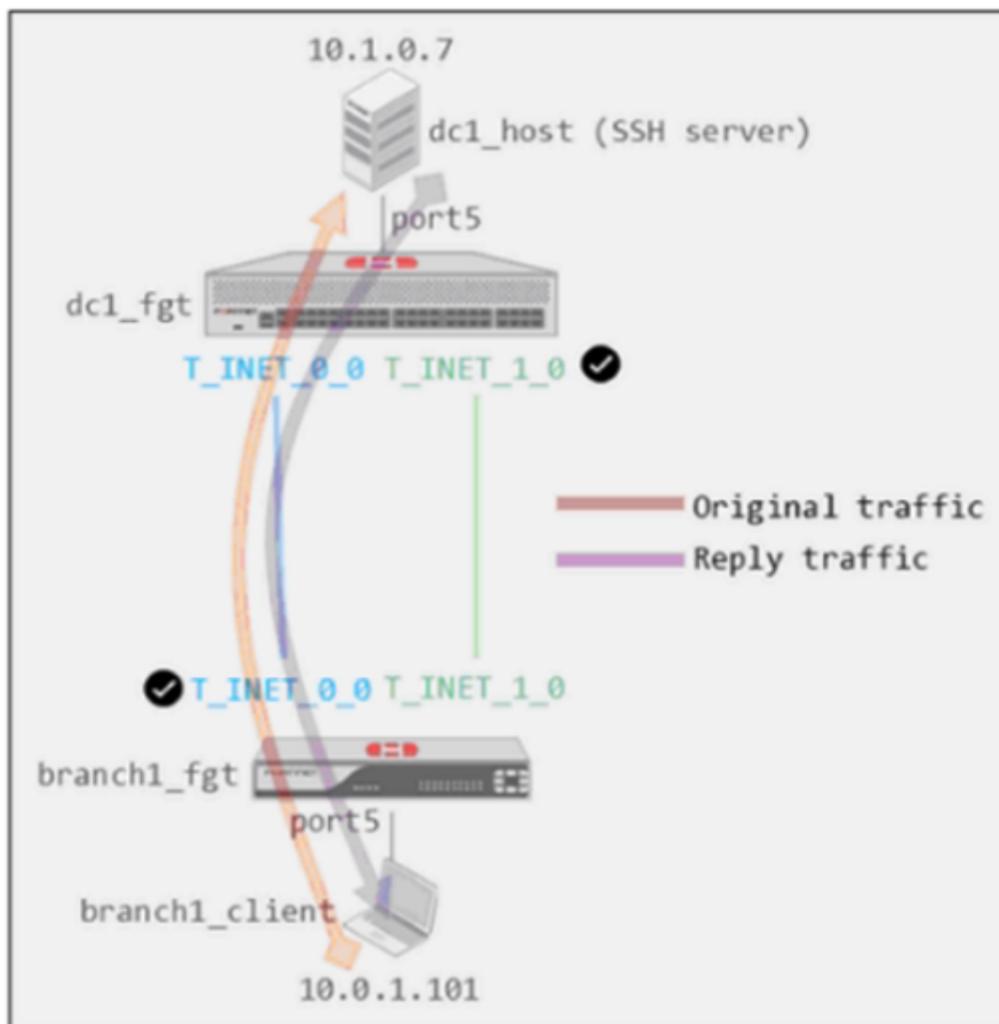
Exhibit B

```
dc1_fgt # show system global
config system global
    set admin-https-redirect disable
    set admintimeout 480
    set alias "FortiGate-VM64"
    set hostname "dc1_fgt"
    set timezone 04
end

dc1_fgt # show system settings
config system settings
    set tcp-session-without-syn enable
    set allow-subnet-overlap enable
    set gui-allow-unnamed-policy enable
    set gui-multiple-interface-policy enable
end
```

Exhibit A shows a site-to-site topology between two FortiGate devices: branch1_fgt and dc1_fgt. Exhibit B shows the system global and system settings configuration on dc1_fgt.

When branch1_client establishes a connection to dc1_host, the administrator observes that, on dc1_fgt, the reply traffic is routed over T_INET_0_0, even though T_INET_1_0 is the preferred member in the matching SD-WAN rule.

Based on the information shown in the exhibits, what configuration change must be made on dc1_fgt so dc1_fgt routes the reply traffic over T_INET_1_0?

A. Enable auxiliary-session under config system settings.
B. Disable tp-session-without-syn under config system settings.
C. Enable snat-route-change under config system global.
D. Disable allow-subnet-overlap under config system settings.

Answer: A

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

NEW QUESTION 38
......

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-7.0 Exam with Our Prep Materials Via below:

https://www.certleader.com/NSE7_SDW-7.0-dumps.html