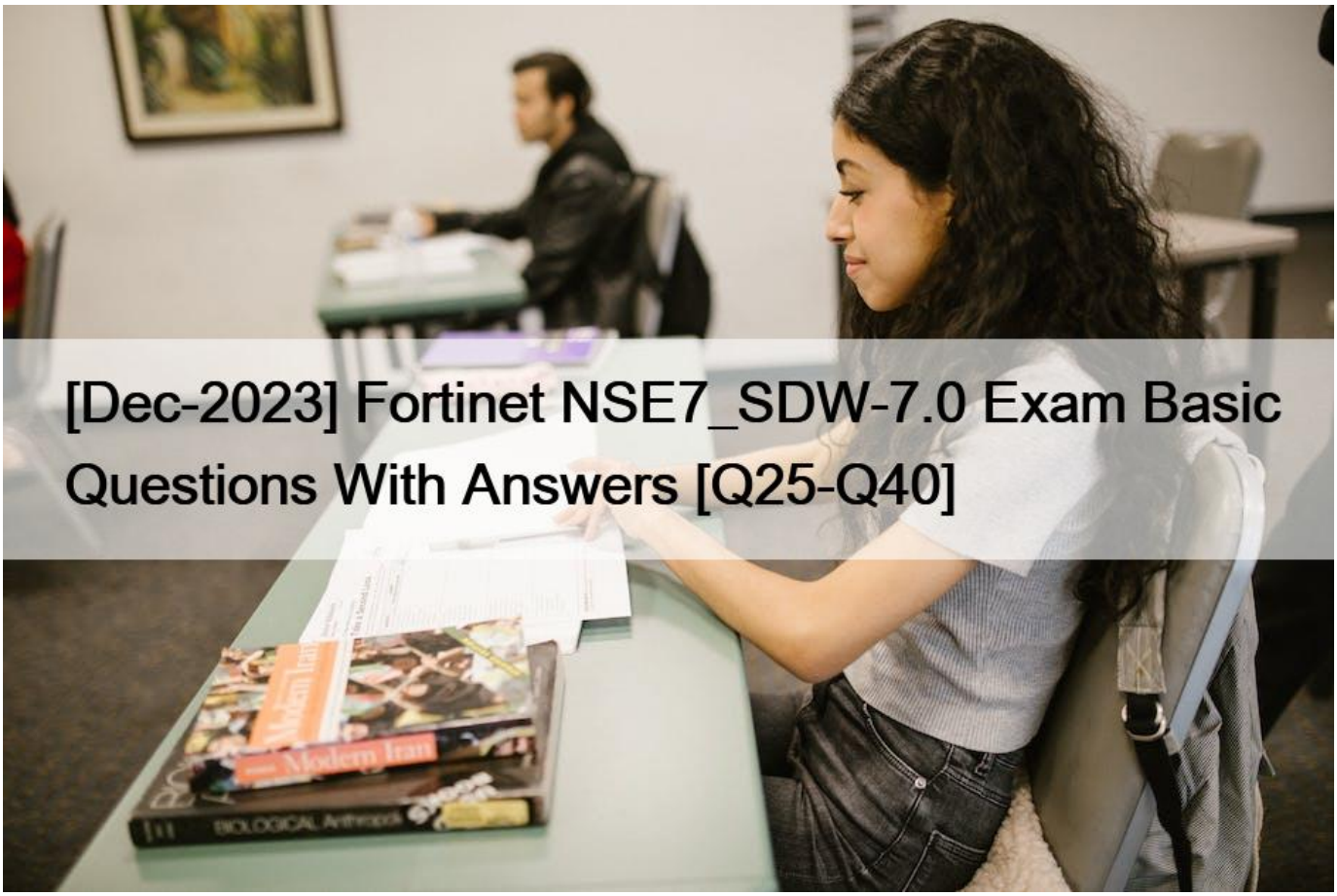
[Dec-2023 Fortinet NSE7_SDW-7.0 Exam Basic Questions With Answers [Q25-Q40



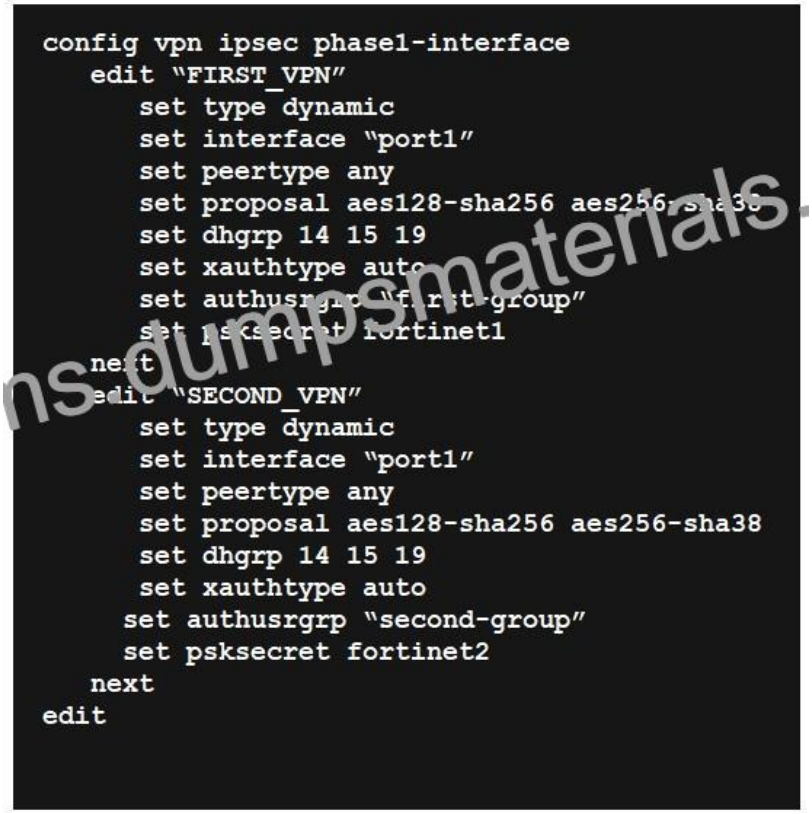
[Dec-2023] Fortinet NSE7_SDW-7.0 Exam: Basic Questions With Answers
New 2023 Realistic Free Fortinet NSE7_SDW-7.0 Exam Dump Questions and Answer

NO.25 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.)
* On the hubs, auto-discovery-sender must be enabled on the IPsec VPNs to spokes.
* On the spokes, auto-discovery-receiver must be enabled on the IPsec VPN to the hub.
* auto-discovery-forwarder must be enabled on all IPsec VPNs.
* On the hubs, net-device must be enabled on all IPsec VPNs.

NO.26 Refer to the exhibit.



FortiGate has multiple dial-up VPN interfaces incoming on port1 that match only FIRST_VPN.

Which two configuration changes must be made to both IPsec VPN interfaces to allow incoming connections to match all possible IPsec dial-up interfaces? (Choose two.)
* Specify a unique peer ID for each dial-up VPN interface.
* Use different proposals are used between the interfaces.
* Configure the IKE mode to be aggressive mode.
* Use unique Diffie Hellman groups on each VPN interface.

NO.27 What are two reasons why FortiGate would be unable to complete the zero-touch provisioning process?

(Choose two.)
* The FortiGate cloud key has not been added to the FortiGate cloud portal.

* FortiDeploy has connected with FortiGate and provided the initial configuration to contact FortiManager
* The zero-touch provisioning process has completed internally, behind FortiGate.
* FortiGate has obtained a configuration from the platform template in FortiGate cloud.
* A factory reset performed on FortiGate.

NO.28 What are two benefits of using forward error correction (FEC) in IPsec VPNs? (Choose two.)
* FEC supports hardware offloading.
* FEC improves reliability of noisy links.
* FEC transmits parity packets that can be used to reconstruct packet loss.
* FEC can leverage multiple IPsec tunnels for parity packets transmission.

NO.29 Exhibit.

```
id=20010 trace_id=1402 func=print_pkt_detail line=5588 msg="vd-root:0 received a
packet(proto=6, 10.1.10.1:52490->42.44.50.10:443) from port3. flag [.], seq 1213725680,
ack 1169005655, win 65535"
id=20010 trace_id=1402 func=resolve_ip_tuple_fast line=5669 msg="Find an existing
session, id-00001ca4, original direction"
id=20010 trace_id=1402 func=fw_forward_dirty_handler line=447 msg="Denied by quota
check"
```

Which conclusion about the packet debug flow output is correct?
* The total number of daily sessions for 10.1.10.1 exceeded the maximum number of concurrent sessions configured in the traffic shaper, and the packet was dropped.
* The packet size exceeded the outgoing interface MTU.
* The number of concurrent sessions for 10.1.10.1 exceeded the maximum number of concurrent sessions configured in the traffic shaper, and the packet was dropped.
* The number of concurrent sessions for 10.1.10.1 exceeded the maximum number of concurrent sessions configured in the firewall policy, and the packet was dropped.

NO.30 Which two interfaces are considered overlay links? (Choose two.)
* LAG
* IPsec
* Physical
* GRE

NO.31 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.)
* Each BGP route is three hops away from the destination.
* ibgp-multipath is disabled.
* additional-path is enabled.
* You can run the get router info routing-table database command to display the additional paths.

NO.32 Refer to the exhibits.

```
id=20010 trace_id=1402 func=print_pkt_detail line=5588 msg="vd-root:0 received a
packet(proto=6, 10.1.10.1:52490->42.44.50.10:443) from port3. flag [.], seq 1213725680,
ack 1169005655, win 65535"
id=20010 trace_id=1402 func=resolve_ip_tuple_fast line=5669 msg="Find an existing
session, id-00001ca4, original direction"
id=20010 trace_id=1402 func=fw_forward_dirty_handler line=447 msg="Denied by quota
check"
```

Which conclusion about the packet debug flow output is correct?
* The total number of daily sessions for 10.1.10.1 exceeded the maximum number of concurrent sessions configured in the traffic shaper, and the packet was dropped.
* The packet size exceeded the outgoing interface MTU.
* The number of concurrent sessions for 10.1.10.1 exceeded the maximum number of concurrent sessions configured in the traffic shaper, and the packet was dropped.
* The number of concurrent sessions for 10.1.10.1 exceeded the maximum number of concurrent sessions configured in the firewall policy, and the packet was dropped.
In a Per-IP shaper configuration, if an IP address exceeds the configured concurrent session limit, the message “Denied by quota check” appears. SD-WAN 7.0 Study Guide page 287

NO.33 In the default SD-WAN minimum configuration, which two statements are correct when traffic matches the default implicit SD-WAN rule? (Choose two)
* Traffic has matched none of the FortiGate policy routes.
* Matched traffic failed RPF and was caught by the rule.
* The FIB lookup resolved interface was the SD-WAN interface.
* An absolute SD-WAN rule was defined and matched traffic.

NO.34 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 10.0.2.101->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?
* This is a spoke that has received a query from a remote hub and has forwarded the response to its hub.
* Two hubs, 10.0.1.101 and 10.0.2.101, are receiving and forwarding queries between each other.
* This is a hub that has received a query from a spoke and has forwarded it to another spoke.
* Two spokes, 192.2.0.1 and 10.0.2.101, forward their queries to their hubs.

NO.35 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.)
* FortiGate flags the sessions as dirty.
* FortiGate continues routing the sessions with no SNAT, over port2.
* FortiGate performs a route lookup for the original traffic only.
* FortiGate updates the gateway information of the sessions with SNAT so that they use port1 instead of port2.

NO.36 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?

* When all three members have the same packet loss.
* When T_INET_0_0 has 4% packet loss.
* When T_INET_0_0 has 12% packet loss.
* When T_INET_1_0 has 4% packet loss.

NO.37 Which two performance SLA protocols enable you to verify that the server response contains a specific value?

(Choose two.)

* http
* icmp
* twamp
* dns

NO.38 Refer to the exhibits.

Exhibit A

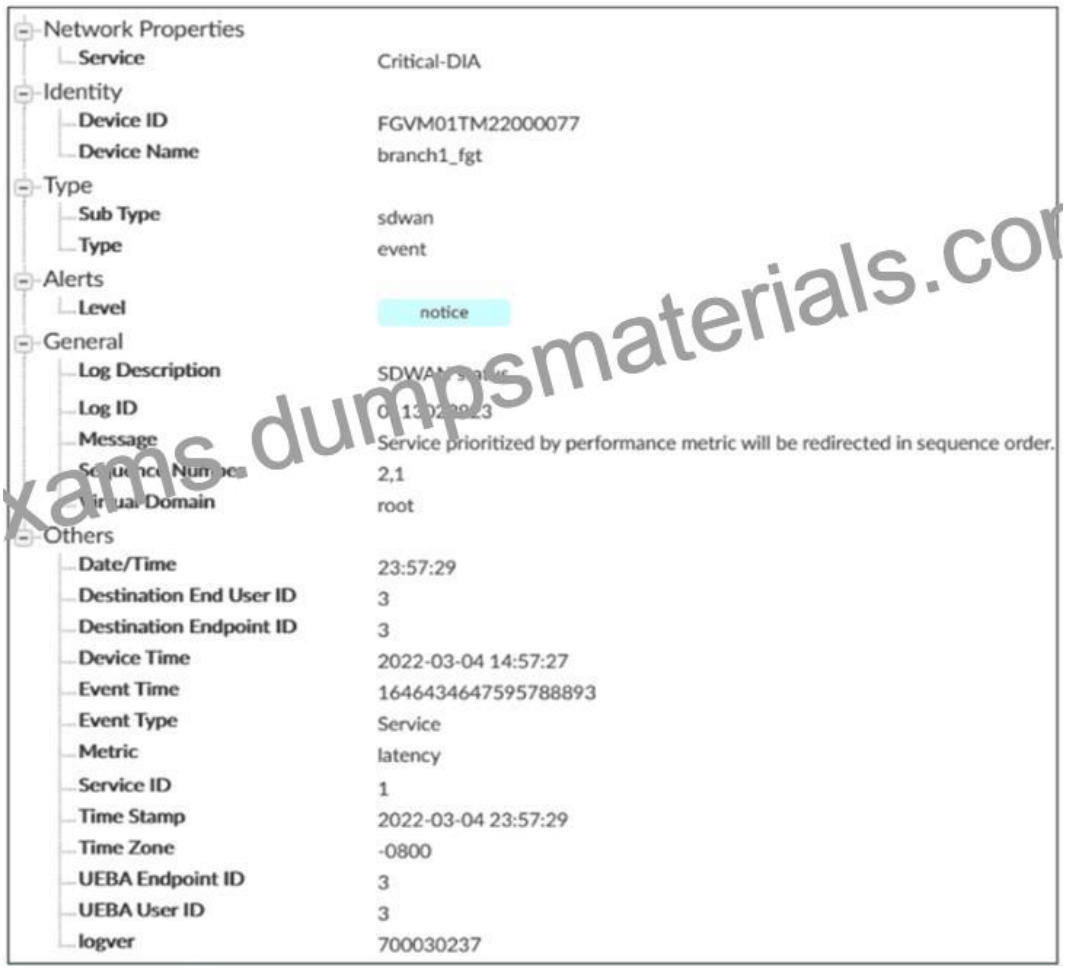


Exhibit B

```
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.

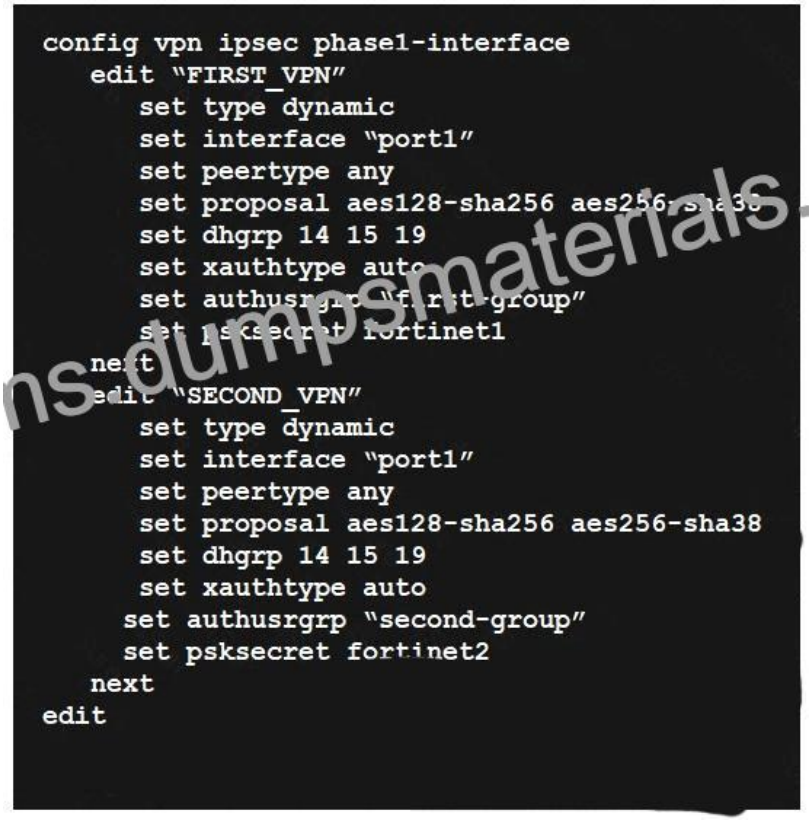
Based on the exhibits, which two statements are correct? (Choose two.)

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

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

NO.39 Which two statements about the SD-WAN zone configuration are true? (Choose two.)
* The service-sla-tie-break setting enables you to configure preferred member selection based on the best route to the destination.
* You can delete the default zones.
* The default zones are virtual-wan-link and SASE.
* An SD-WAN member can belong to two or more zones.

NO.40 Refer to the exhibit.



FortiGate has multiple dial-up VPN interfaces incoming on port1 that match only FIRST_VPN.

Which two configuration changes must be made to both IPsec VPN interfaces to allow incoming connections to match all possible IPsec dial-up interfaces? (Choose two.)
* Specify a unique peer ID for each dial-up VPN interface.
* Use different proposals are used between the interfaces.
* Configure the IKE mode to be aggressive mode.
* Use unique Diffie Hellman groups on each VPN interface.

Guaranteed Success in NSE 7 Network Security Architect NSE7_SDW-7.0 Exam Dumps:
https://www.dumpsmaterials.com/NSE7_SDW-7.0-real-torrent.html]