NSE7_SDW-6.4 Q&As

Fortinet NSE 7 - SD-WAN 6.4

Pass Fortinet NSE7_SDW-6.4 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/nse7_sdw-6-4.html

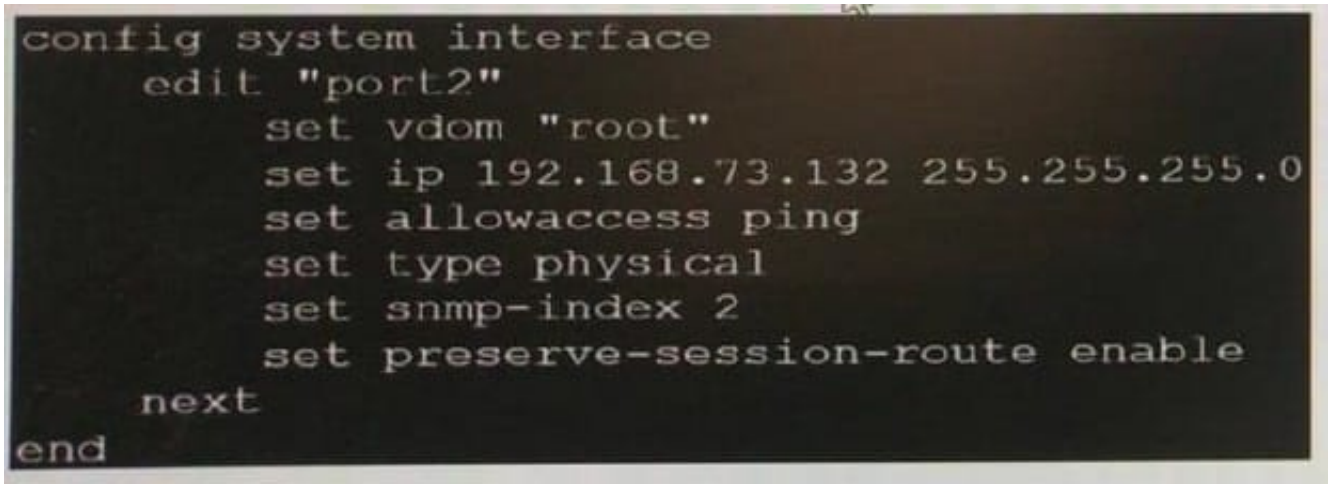
100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Refer to the exhibit.



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

A. FortiGate performs routing lookups for new sessions only after a route change.

B. FortiGate marks the routing information on existing sessions as persistent.

C. FortiGate flushes all routing information from the session table after a route change.

D. FortiGate always blocks all traffic after a route change.

Correct Answer: AB

QUESTION 2

Which two benefits from using forward error correction (FEC) in IPsec VPNs are true? (Choose two.)

A. FEC transmits the original payload in full to recover the error in transmission.

B. FEC reduces the stress on the remote device buffer to reconstruct packet loss.

C. FEC transmits additional packets as redundant data to the remote device.

D. FEC improves reliability, which overcomes adverse WAN conditions such as noisy links.

Correct Answer: CD

QUESTION 3

FortiGate is connected to the internet and is obtaining the IP address on its egress interlace from the DHCP server

Which statement is due when FortiGate restarts and receives preconfigured settings to install as part of a zero-touch provisioning process?

A. FortiDeploy connects with FortiGate and provides the initial configuration to contact FortiManager

B. The zero-touch provisioning process completes internally, behind FortiGate

C. FortiManager registers FortiGate after the restart and retrieves the existing configuration

D. The FortiGate cloud key added to the FortiGate cloud portal and FortiGate performs a factory reset before the restart

Correct Answer: A

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.

Correct Answer: AE

QUESTION 5

What are the two minimum configuration requirements for an outgoing interface to be selected once the SD-WAN logical interface is enabled? (Choose two)

A. Specify outgoing interface routing cost.

B. Configure SD-WAN rules interface preference.

C. Select SD-WAN balancing strategy.

D. Specify incoming interfaces in SD-WAN rules.

Correct Answer: AB

QUESTION 6

Which three protocols are available only on the command line to configure as performance SLA status check? (Choose three.)

A. smtp

B. tcp-echo

C. twamp

D. udp-echo

E. icmp

Correct Answer: BCD

QUESTION 7

Which three performance SLA protocols are available on the FortiGate CLI only? (Choose three.)

A. tcp-echo

B. icmp

C. twamp

D. udp-echo

E. smtp

Correct Answer: ACD

Command output from a fortigate:

FW-01 (test-health-check) # set protocol

ping Use PING to test the link with the server.

tcp-echo Use TCP echo to test the link with the server. udp-echo Use UDP echo to test the link with the server. http Use HTTP-GET to test the link with the server. twamp Use TWAMP to test the link with the server. dns Use DNS query to test

the link with the server. tcp-connect Use a full TCP connection to test the link with the server.

ftp Use FTP to test the link with the server.

QUESTION 8

In which two ways does FortiGate learn the FortiManager IP address or FQDN for zero-touch provisioning? (Choose two.)

A. From a FortiGuard definitions update

B. From the central management configuration configured in FortiDeploy

C. From a DHCP server configured with options 240 or 241

D. From another FortiGate device in the same local network

Correct Answer: BC

https://www.historiantech.com/zeroish-touch-provisioning-with-fortimanager-explained/

QUESTION 9

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.

Correct Answer: AC

QUESTION 10

Which statement reflects how BGP tags work with SD-WAN rules?

A. BGP tags match the SD-WAN rule based on the order that these rules were installed.

B. BGP tags require that the adding of static routes be enabled on all ADVPN interfaces

C. Route tags are used for a BGP community and the SD-WAN rules are assigned the same tag

D. VPN topologies are formed using only BGP dynamic routing with SD-WAN

Correct Answer: C

QUESTION 11

Refer to the exhibit.

```
config vpn ipsec phase1-interface
    edit Hub
        set add-route enable
        set net-device disable
        set tunnel-search nexthop
    next
end

diagnose vpn tunnel list name Hub
list ipsec tunnel by names in vd 0
------------------------------------------------------
name=Hub ver=1 serial=1 100.64.1.1:0->0.0.0.0:0 dst_mtu=0
bound_if=3 lgwy=static/1 tun=intf/0 mode=dialup/2 encap=none/512 options[0200]=search-
nexthop frag-rfc accept_traffic=1
proxyid_num=0 child_num=2 refcnt=20 ilast=176 olast=176 ad=/0
stat: rxp=22 txp=18 rxb=2992 txb=1752
dpd: mode=on-idle on=0 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
run_tally=2
ipv4 route tree:
100.64.3.1 1
100.64.5.1 0
172.16.1.2 1
172.16.1.3 0
```

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

A. FortiGate creates separate virtual interfaces for each dial-up client.

B. FortiGate creates a single IPsec virtual interface that is shared by all clients.

C. FortiGate maps the remote gateway 100.64.3.1 to tunnel index interface 1.

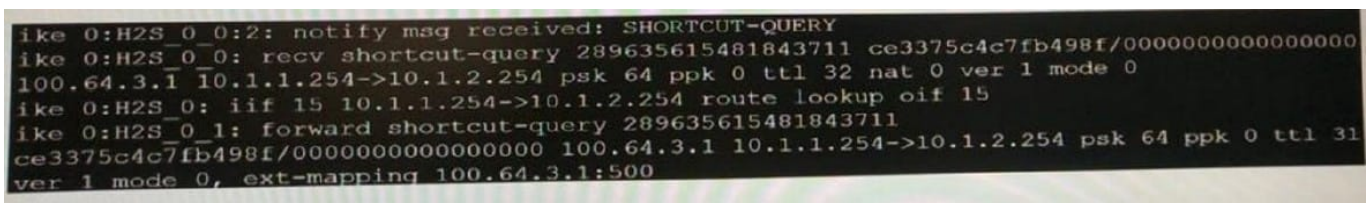
D. FortiGate does not install IPsec static routes for remote protected networks in the routing table.

Correct Answer: BC

If net-device is disabled, FortiGate creates a single IPSEC virtual interface that is shared by all IPSEC clients connecting to the same dialup VPN. In this case, the tunnel-search setting determines how FortiGate learns the network behind each remote client.

QUESTION 12

Refer to the exhibit



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

A. Two spokes 100.64.3.1 and 10.1.2. 254 forward their queries to their hubs

B. This is a hub that has received a query from a spoke and has forwarded it to another spoke

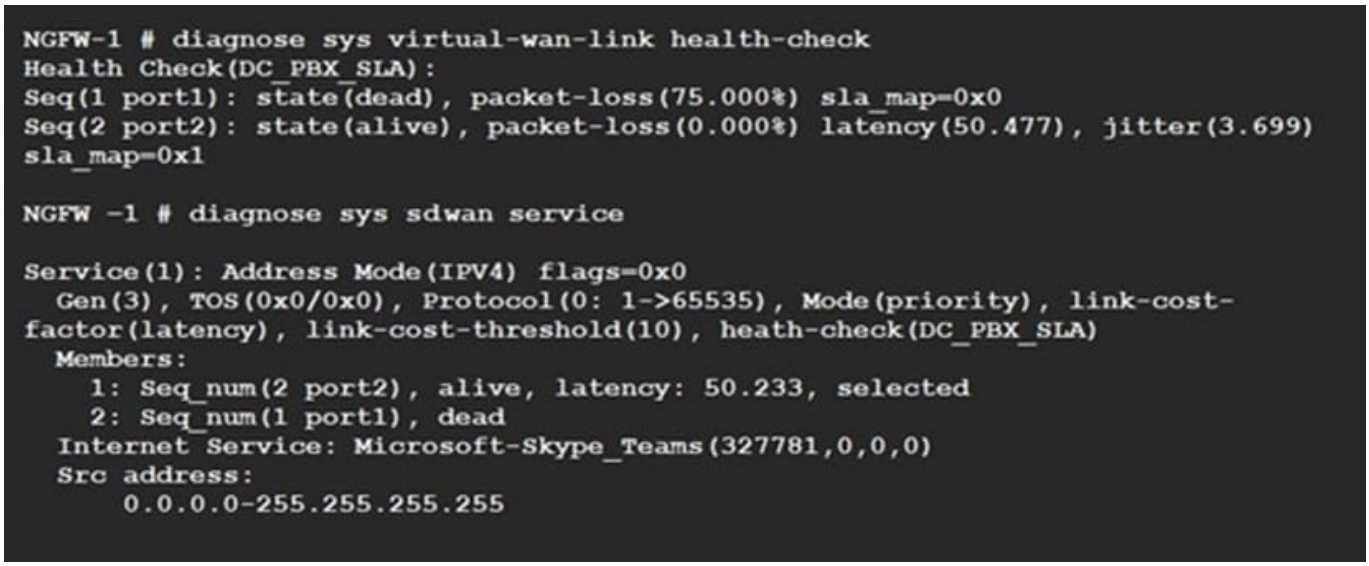
C. This is a spoke that has received a query from a remote hub and has forwarded the response to its hub

D. Two hubs. 10.1.1.254 and 10.1.2.254, are receiving and forwarding queries between each other

Correct Answer: B

QUESTION 13

Refer to the exhibit.



Based on the exhibit, which status description is correct?

A. Port1 is dead because it does not meet the SLA target.

B. Port2 is alive because its packet loss is lower than 10%.

C. The SD-WAN members are monitored by different performance SLAs.

D. Traffic matching the SD-WAN rule is steered through port2.

Correct Answer: D

QUESTION 14

Which diagnostic command can you use to show interface-specific SLA logs for the last 10 minutes?

A. diagnose sys sdwan log

B. diagnose sys sdwan health-check

C. diagnose sys sdwan intf-sla-log

D. diagnose sys sdwan sla-log

Correct Answer: D

diagnose sys sdwan intf-sla-log -> shows only bandwidth utilization diagnose sys sdwan sla-log -> shows packet-loss, latency, jitter, MOS

QUESTION 15

Refer to the exhibit.

```
config vpn ipsec phase1-interface
   edit "FIRST_VPN"
      set type dynamic
      set interface "port1"
      set peertype any
      set proposal aes128-sha256 aes256-sha38
      set dhgrp 14 15 19
      set xauthtype auto
      set authusrgrp "first-group"
      set psksecret fortinet1
   next
   edit "SECOND_VPN"
      set type dynamic
      set interface "port1"
      set peertype any
      set proposal aes128-sha256 aes256-sha38
      set dhgrp 14 15 19
      set xauthtype auto
     set authusrgrp "second-group"
     set psksecret fortinet2
   next
edit
```

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.)

A. Specify a unique peer ID for each dial-up VPN interface.

B. Use different proposals are used between the interfaces.

C. Configure the IKE mode to be aggressive mode.

D. Use unique Diffie Hellman groups on each VPN interface.

Correct Answer: AC

SD-WAN 6.4.5 Study Guide. pg 182