NSE7_SDW-7.0 Q&As

Fortinet NSE 7 - SD-WAN 7.0

Pass Fortinet NSE7_SDW-7.0 Exam with 100% Guarantee

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

https://www.pass4itsure.com/nse7_sdw-7-0.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Refer to exhibits.

Exhibit A

Name	Detect Server	Packet Loss	Latency	Jitter	Failure Threshold	Recovery Threshold
DC_PBX_SLA	4.2.2.2	port1: 0.00%	port1: 32.80ms	port1: 8.58ms	5	5
	4.2.2.1	port2: 0.00%	port2: 55.36ms	port2: 8.37ms		

Exhibit B

```
NGFW-1 # diagnose sys virtual-wan-link health-check
Health Check(DC_PBX_SLA):
Seq(1 port1): state(dead), packet-loss(75.000%) sla_map=0x0
Seq(2 port2): state(alive), packet-loss(0.000%) latency(50.477), jitter(3.699)
sla_map=0x1

NGFW -1 # diagnose sys virtual-wan-link service

Service(1): Address Mode(IPV4) flags=0x0
  Gen(3), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(priority), link-cost-
factor(latency), link-cost-threshold(10), heath-check(DC_PBX_SLA)
  Members:
    1: Seq_num(2 port2), alive, latency: 50.233, selected
    2: Seq_num(1 port1), dead
  Internet Service: Microsoft-Skype_Teams(327781,0,0,0)
  Src address:
      0.0.0.0-255.255.255.255
```

Exhibit A shows the performance SLA exhibit B shows the SD-WAN diagnostics output. Based on the exhibits, which statement is correct?

A. Both SD-WAN member interfaces have used separate SLA targets.

B. The SLA state of port1 is dead after five unanswered requests by the SLA servers.

C. Port1 became dead 1ecause no traffic was offload through the egress of port1.

D. SD-WAN member interfaces are affected by the SLA state of the inactive interface

Correct Answer: B

SD-WAN_6.4_Study_Guide page 57

QUESTION 2

Refer to the exhibit.

What must you configure to enable ADVPN?

A. On the hub VPN, only the device needs additional phase one sett

B. ADVPN should only be enabled on unmanaged FortiGate devices.

C. Each VPN device has a unique pre-shared key configured separately on phase one

D. The protected subnets should be set to address object to all (0.0.0.0/0)..

Correct Answer: D

SD-WAN 6.4.5 Study Guide. pg 210

QUESTION 3

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

QUESTION 4

Which two statements describe how IPsec phase 1 aggressive mode is different from main mode when performing IKE negotiation? (Choose two)

A. A peer ID is included in the first packet from the initiator, along with suggested security policies.

B. XAuth is enabled as an additional level of authentication, which requires a username and password.

C. A total of six packets are exchanged between an initiator and a responder instead of three packets.

D. The use of Diffie Hellman keys is limited by the responder and needs initiator acceptance.

Correct Answer: AC

QUESTION 5

Why is it effective to use SD WAN rules when configuring application control?

A. Because traffic can be load balanced based on application type

B. Because SD-WAIM rules are independent from firewall policies to avoid controlling applications

C. Because you must use certificate full inspection on the firewall policy

D. Because the application database is manually maintained by administrators

Correct Answer: A

You can configure rules to steer traffic based on the application detected by Fortigate. This is know as application steering or application-aware routing