

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.

```
config system virtual-wan-link
  set status enable
  set load-balance-mode source-ip-based
  config members
    edit 1
      set interface "port1"
      set gateway 100.64.1.254
      set source 100.64.1.1
      set cost 15
    next
    edit 2
      set interface "port2"
      set gateway 100.64.2.254
      set priority 10
    next
  end
end
```

Based on the output shown in the exhibit, which two criteria on the SD-WAN member configuration can be used to select an outgoing interface in an SD-WAN rule? (Choose two.)

- A. Set priority 10.
- B. Set cost 15.
- C. Set load-balance-mode source-ip-ip-based.
- D. Set source 100.64.1.1.

Answer: AB

NEW QUESTION 2

Exhibit A –

| # | Name | Type | Normalized Interface | Addressing Mode | IP/Netmask | Access |
|-----------------|--------------------------|-------------|----------------------|-----------------|---------------------------|-------------------------|
| Physical (10) | | | | | | |
| 1 | port1 | Physical | port1 | Manual | 203.0.113.1/255.255.255.2 | PING |
| 2 | port2 | Physical | port2 | Manual | 203.0.113.9/255.255.255.2 | PING |
| 3 | port3 | Physical | port3 | Manual | 0.0.0.0/0.0.0.0 | |
| 4 | port4 | Physical | port4 | Manual | 172.16.0.9/255.255.255.24 | PING |
| 5 | port5 | Physical | port5 | Manual | 10.0.2.254/255.255.255.0 | PING |
| 6 | port6 | Physical | port6 | Manual | 0.0.0.0/0.0.0.0 | |
| 7 | port7 | Physical | port7 | Manual | 0.0.0.0/0.0.0.0 | |
| 8 | port8 | Physical | port8 | Manual | 0.0.0.0/0.0.0.0 | |
| 9 | port9 | Physical | port9 | Manual | 0.0.0.0/0.0.0.0 | |
| 10 | port10 | Physical | port10 | Manual | 192.168.0.32/255.255.255. | HTTPS, PING, SSH, HT |
| Aggregate (1) | | | | | | |
| 11 | fortilink | Aggregate | | Manual | 169.254.1.1/255.255.255.0 | PING, Security Fabric C |
| Tunnel (3) | | | | | | |
| 12 | na1.root | Tunnel | | Manual | 0.0.0.0/0.0.0.0 | |
| 13 | l2t.root | Tunnel | | Manual | 0.0.0.0/0.0.0.0 | |
| 14 | ssl.root (SSL VPN interf | Tunnel | | Manual | 0.0.0.0/0.0.0.0 | |
| EMAC VLAN (1) | | | | | | |
| 15 | vl_lan_b1 | EMAC VLAN | | Manual | 10.0.102.1/255.255.255.0 | PING |
| SD-WAN Zone (2) | | | | | | |
| 16 | virtual-wan-link | SD-WAN Zone | | | | |
| 17 | SASE | SD-WAN Zone | SASE | | | |

| # | ID | Destination | Gateway | Interface | Distance | Priority | Status | Description |
|------------------|----|-----------------|--------------|-----------|----------|----------|--------|-------------|
| Static Route (2) | | | | | | | | |
| 1 | 1 | 0.0.0.0/0.0.0.0 | 203.0.113.2 | port1 | 10 | 0 | Enable | |
| 2 | 2 | 0.0.0.0/0.0.0.0 | 203.0.113.10 | port2 | 10 | 0 | Enable | |

Exhibit B –

| # | Name | From | To | Source | Destination | Schedule | Service |
|---------------------------|-----------------|-------|-------|--------|-------------|----------|---------|
| 1 | Internet_Access | port5 | port1 | all | all | always | ALL |
| Implicit (2-2 / Total: 1) | | | | | | | |
| 2 | Implicit Deny | any | any | all | all | always | ALL |

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 3

Refer to the exhibit, which shows the IPsec phase 1 configuration of a spoke.

```
config vpn ipsec phase1-interface
 edit "T_INET_0_0"
  set interface "port1"
  set ike-version 2
  set keylife 28800
  set peertype any
  set net-device disable
  set proposal aes128-sha256 aes256-sha256 aes128gcm-prfsha256 aes256gcm-prfsha384
  chacha20poly1305-prfsha256
  set comments "[created by FMG VPN Manager]"
  set idle-timeout enable
  set idle-timeoutinterval 5
  set auto-discovery-receiver enable
  set remote-gw 100.64.1.1
  set psksecret ENC
  6D5rVsaKlMeAyVYt1z95BS24Psew761wY023hnFVviwb6deIt8c5ltCa+iNYhuJ78gycfD4+WuszpmuIv8rRzrVh
  7DFkHaW2auAAprQ0dHUfaCzjOhME7mPw+8he2xB7Edb9ku/nZEHb0cKLkKYJc/p9J9IMweV21ZUgFjvIpXNxHxpH
  LReOFShoH01SPFKz5IYCVA==
  next
end
```

What must you configure on the IPsec phase 1 configuration for ADVPN to work with SD-WAN?

- A. You must set ike-version to 1.
- B. You must enable net-device.
- C. You must enable auto-discovery-sender.
- D. You must disable idle-timeout.

Answer: B

NEW QUESTION 4

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 5

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.)

- A. Each BGP route is three hops away from the destination.
- B. ibgp-multipath is disabled.
- C. additional-path is enabled.
- D. You can run the get router info routing-table database command to display the additional paths.

Answer: CD

NEW QUESTION 6

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 7

Refer to the exhibit.

```
config vpn ipsec phase1-interface
  edit "T_INET_0_0"
    set type dynamic
    set interface "port1"
    set keylife 28800
    set peertype any
    set net-device disable
    set proposal aes128-sha256
    set add-route enable
    set psksecret ENC
    Zv9n4Urfk0W4jj8vWI+KywxBG4ZDT7jWHKd8YaL8j4+pRpYOx/N7mSgc7VL0BW22HQUXWJ6zvFxNKktiPYntA8aP
    i6ly7gDx2lP/OfKexTQQJzgCGRYzLM8eFTOnK7K6AuX0bFDCpBBhEIdf+03CYBMLwkF2mdU6RsT+qvyybblVX+Ioy
    HK5EXakpmz5RiltELgZ9Gg==
  next
end
```

Which configuration change is required if the responder FortiGate uses a dynamic routing protocol to exchange routes over IPsec?

- A. type must be set to static.
- B. mode-cfg must be enabled.
- C. exchange-interface-ip must be enabled.
- D. add-route must be disabled.

Answer: D

Explanation:

for using "non ike" routes (for example BGP/static and so on) you must do disable the add-route that inject automatically kernel route based on p2 selectors from the remote site from the SD-WAN_7.2_Study_Guide page 236

NEW QUESTION 8

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
origin->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=000000a2c tos=ff/ff app_list=0 app=0 url_cat=0
rpd_b_link_id= 80000000 rpd_b_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 9

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

NEW QUESTION 10

Refer to the exhibits.

Exhibit A

```
branch1_fgt (3) # show
config service
  edit 3
    set name "Corp"
    set mode sla
    set dst "Corp-net"
    set src "LAN-net"
    config sla
      edit "VPN_PING"
        set id 1
      next
      edit "VPN_HTTP"
        set id 1
      next
    end
    set priority-members 3 4 5
    set gateway enable
  next
end
```

Exhibit B

```
branch1_fgt # diagnose sys sdwan service 3

Service(3): Address Mode(IPV4) flags=0x200 use-shortcut-sla
Gen(1), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(sla), sla-compare-order
Members(2):
  1: Seq_num(5 T_MPLS_0), alive, sla(0x3), gid(0), cfg_order(2), cost(0), selected
  2: Seq_num(4 T_INET_1_0), alive, sla(0x1), gid(0), cfg_order(1), cost(0), selected
  3: Seq_num(3 T_INET_0_0), alive, sla(0x0), gid(0), cfg_order(0), cost(0), 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 # get router info routing-table all | grep T_
S      10.0.0.0/8 [1/0] via T_INET_0_0 tunnel 100.64.1.1
        [1/0] via T_INET_1_0 tunnel 100.64.1.9
S      10.201.1.254/32 [15/0] via T_INET_0_0 tunnel 100.64.1.1
S      10.202.1.254/32 [15/0] via T_INET_1_0 tunnel 100.64.1.9
S      10.203.1.254/32 [15/0] via T_MPLS_0 tunnel 172.16.1.5

branch1_fgt # diagnose sys sdwan member | grep T_
Member(3): interface: T_INET_0_0, flags=0x4 , gateway: 100.64.1.1, peer: 10.201.1.254,
priority: 0 1024, weight: 0
Member(4): interface: T_INET_1_0, flags=0x4 , gateway: 100.64.1.9, peer: 10.202.1.254,
priority: 0 1024, weight: 0
Member(5): interface: T_MPLS_0, flags=0x4 , gateway: 172.16.1.5, peer: 10.203.1.254,
priority: 0 1024, weight: 0
```

Exhibit A shows the configuration for an SD-WAN rule and exhibit B shows the respective rule status, the routing table, and the member status. The administrator wants to understand the expected behavior for traffic matching the SD-WAN rule. Based on the exhibits, what can the administrator expect for traffic matching the SD-WAN rule?

- A. The traffic will be load balanced across all three overlays.
- B. The traffic will be routed over T_INET_0_0.
- C. The traffic will be routed over T_MPLS_0.
- D. The traffic will be routed over T_INET_1_0.

Answer: C

NEW QUESTION 10

Which best describes the SD-WAN traffic shaping mode that bases itself on a percentage of available bandwidth?

- A. Interface-based shaping mode
- B. Reverse-policy shaping mode
- C. Shared-policy shaping mode
- D. Per-IP shaping mode

Answer: A

Explanation:

Interface-based shaping goes further, enabling traffic controls based on percentage of the interface bandwidth.

NEW QUESTION 12

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

NEW QUESTION 13

In a hub-and-spoke topology, what are two advantages of enabling ADVPN on the IPsec overlays? (Choose two.)

- A. It provides the benefits of a full-mesh topology in a hub-and-spoke network.
- B. It provides direct connectivity between spokes by creating shortcuts.
- C. It enables spokes to bypass the hub during shortcut negotiation.
- D. It enables spokes to establish shortcuts to third-party gateways.

Answer: AB

NEW QUESTION 14

.....

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