



Fortinet

Exam Questions NSE7_SDW-7.0

Fortinet NSE 7 - SD-WAN 7.0

NEW QUESTION 1

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
    6D5rVsaKlMeAyVYt1z958S24Psew761wY023hnFVviwb6deIt8c5ltCa+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 2

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 3

Refer to the exhibits.

Exhibit A

Edit Traffic Shaping Policy

IP Version

IPv4IPv6

Name

Limit_YouTube

Status

EnableDisable

Comments

If Traffic Matches:

Source Internet Service

Source Address

LAN-net

Source User

Source User Group

Destination Internet Service

Destination Address

all

Schedule

Service

ALL

Application

YouTube

Application Category

Application Group

URL Category

Type Of Service

0x00

Type Of Service Mask

0x00

Then:

Action

Apply ShaperAssign Group

Outgoing Interface

underlay

Shared Shaper

low-priority

Reverse Shaper

low-priority

Per-IP Shaper

Differentiated Services

Differentiated Services Reverse

Exhibit B

Edit Firewall Policy

ID

1

Name

DIA

ZTNA

DisableFull ZTNAIP/MAC filtering

Incoming Interface

LAN

Outgoing Interface

underlay

Source Internet Service

IPv4 Source Address

LAN-net

IPv6 Source Address

Source User

Source User Group

FSSO Groups

Destination Internet Service

IPv4 Destination Address

all

IPv6 Destination Address

Service

ALL

Schedule

always

Action

DenyAcceptIPSEC

Inspection Mode

Flow-basedProxy-based

Firewall/Network Options

NAT

NATNAT46NAT64

IP Pool Configuration

Use Outgoing Interface AddressUse Dynamic IP Pool

Preserve Source Port

Protocol Options

default

Disclaimer Options

Display Disclaimer

Security Profiles

SSL/SSH Inspection

deep-inspection

Decrypted Traffic Mirror

Traffic Shaping Options

Shared Shaper

Reverse Shaper

Per-IP Shaper

Logging Options

Log Allowed Traffic

No LogLog Security EventsLog All Sessions

Capture Packets

Generate Logs when Session Starts

Exhibit A shows the traffic shaping policy and exhibit B shows the firewall policy. The administrator wants FortiGate to limit the bandwidth used by YouTube. When testing, the administrator determines that FortiGate does not apply traffic shaping on YouTube traffic. Based on the policies shown in the exhibits, what configuration change must be made so FortiGate performs traffic shaping on YouTube traffic?

A. Destination internet service must be enabled on the traffic shaping policy.

B. Application control must be enabled on the firewall policy.

C. Web filtering must be enabled on the firewall policy.

D. Individual SD-WAN members must be selected as the outgoing interface on the traffic shaping policy.

Answer: B

NEW QUESTION 4
Refer to the exhibits.
Exhibit A

Guaranteed success with Our exam guides

visit - <https://www.certshared.com>

```
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 5

Refer to the exhibits.

Exhibit A

Edit Performance SLA

Name: Level3_DNS

IP Version: **IPv4** IPv6

Probe Mode: **Active** Passive Prefer Passive

Protocol: **Ping** TCP ECHO UDP ECHO HTTP TW

Server: 4.2.2.1
4.2.2.2

Participants: All SD-WAN Members **Specify**

port1
port2 2 Entries

Enable Probe Packets: ☒

SLA Targets **+** Add Target

Link Status

Interval: 500 Milliseconds

Failure Before Inactive: 3 (max 3600)

Restore Link After: 2 (max 3600)

Action When Inactive

Update Static Route: ☒

Cascade Interfaces: ☒

Exhibit B -

```
branch1_fgt # diagnose sys sdwan member | grep port
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

branch1_fgt # get router info routing-table all | grep port
S* 0.0.0.0/0 [1/0] via 192.2.0.2, port1
    [1/0] via 192.2.0.10, port2
S 8.8.8.8/32 [10/0] via 192.2.0.11, port2
C 10.0.1.0/24 is directly connected, port5
S 172.16.0.0/16 [10/0] via 172.16.0.2, port4
C 172.16.0.0/29 is directly connected, port4
C 192.2.0.0/29 is directly connected, port1
C 192.2.0.8/29 is directly connected, port2
C 192.168.0.0/24 is directly connected, port10

branch1_fgt # diagnose sys sdwan health-check status Level3_DNS
Health Check(Level3_DNS):
Seq(1 port1): state(alive), packet-loss(0.000%) latency(1.919), jitter(0.137), bandwidth-
up(10238), bandwidth-dw(10238), bandwidth-bi(20476) sla_map=0x0
Seq(2 port2): state(alive), packet-loss(0.000%) latency(1.509), jitter(0.101), bandwidth-
up(10238), bandwidth-dw(10238), bandwidth-bi(20476) sla map=0x0
```

Exhibit A shows the SD-WAN performance SLA and exhibit B shows the SD-WAN member status, the routing table, and the performance SLA status. If port2 is detected dead by FortiGate, what is the expected behavior?

- A. Port2 becomes alive after three successful probes are detected.
- B. FortiGate removes all static routes for port2.
- C. The administrator manually restores the static routes for port2, if port2 becomes alive.
- D. Host 8.8.8.8 is reachable through port1 and port2.

Answer: B

Explanation:

This is due to Update static route is enable which removes the static route entry referencing the interface if the interface is dead

NEW QUESTION 6

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 7

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 8

Refer to the exhibits.

Exhibit A

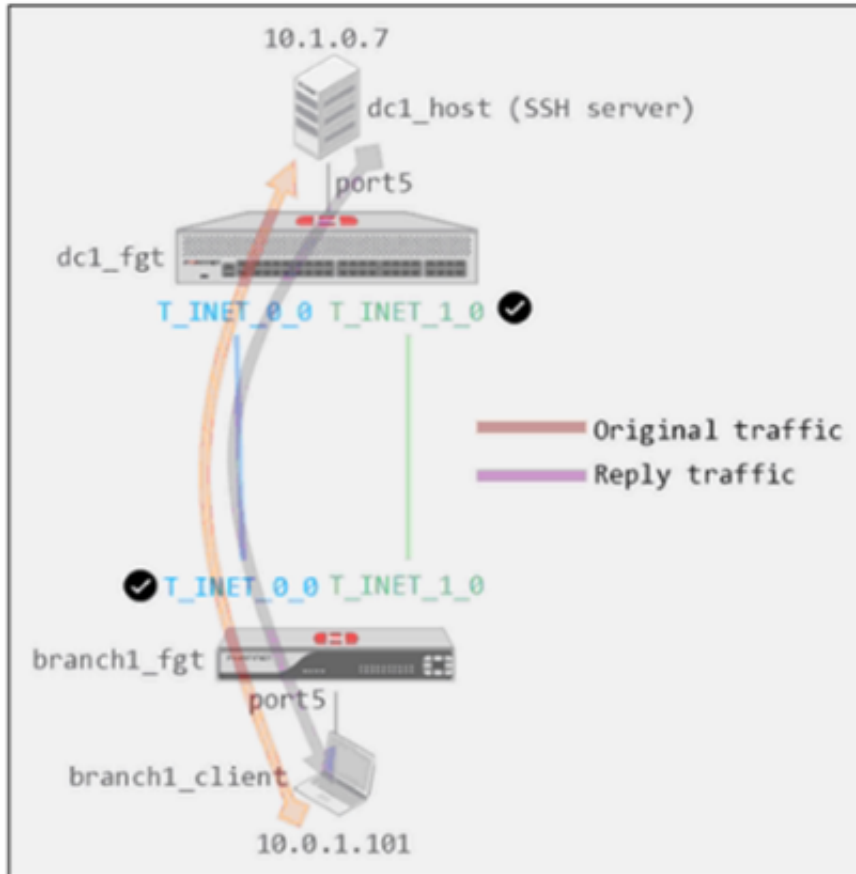


Exhibit B

```
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 9

Which two statements describe how IPsec phase 1 main mode is different from aggressive 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.

Answer: BC

NEW QUESTION 10

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?

- A. 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.
- B. The packet size exceeded the outgoing interface MTU.
- C. 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.
- D. 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.

Answer: C

NEW QUESTION 10

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

NSE7_SDW-7.0 Practice Exam Features:

- * NSE7_SDW-7.0 Questions and Answers Updated Frequently
- * NSE7_SDW-7.0 Practice Questions Verified by Expert Senior Certified Staff
- * NSE7_SDW-7.0 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * NSE7_SDW-7.0 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The NSE7_SDW-7.0 Practice Test Here](#)