

Fortinet

Exam Questions NSE7_SDW-7.2

Fortinet NSE 7 - SD-WAN 7.2



NEW QUESTION 1

Refer to the exhibit.

```
branch1_fgt # diagnose firewall proute list
list route policy info(vf=root):

id=1 dscp_tag=0xff 0xff flags=0x0 tos=0x00 tos_mask=0x00 protocol=17 sport=0-65535 iif=7
dport=53 path(1) oif=3(port1)
source wildcard(1): 0.0.0.0/0.0.0.0
destination wildcard(1): 4.2.2.1/255.255.255.255
hit_count=0 last_used=2022-03-25 10:53:26

id=2131165185(0x7f070001) vwl_service=1(Critical-DIA) vwl_mbr_seq=1 2 dscp_tag=0xff 0xff
flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 sport=0-65535 iif=0 dport=1-65535 path(2)
oif=3(port1) oif=4(port2)
source(1): 10.0.1.0-10.0.1.255
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(3): GoToMeeting(4294836966,0,0,0, 16354)
Microsoft.Office.365.Portals(4294837474,0,0,0, 41468) Salesforce(4294837976,0,0,0, 16920)
hit_count=0 last_used=2022-03-24 12:18:16

id=2131165186(0x7f070002) vwl_service=2(Non-Critical-DIA) vwl_mbr_seq=2 dscp_tag=0xff
0xff flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 sport=0-65535 iif=0 dport=1-65535
path(1) oif=4(port2)
source(1): 10.0.1.0-10.0.1.255
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(2): Facebook(4294836806,0,0,0, 15832) Twitter(4294838278,0,0,0, 16001)
hit_count=0 last_used=2022-03-24 12:18:16

id=2131165187(0x7f070003) vwl_service=3(all_rules) vwl_mbr_seq=1 dscp_tag=0xff 0xff
flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 sport=0-65535 iif=0 dport=1-65535 path(1)
oif=3(port1)
source(1): 0.0.0.0-255.255.255.255
destination(1): 0.0.0.0-255.255.255.255
hit_count=0 last used=2022-03-25 10:58:12
```

Based on the output, which two conclusions are true? (Choose two.)

- A. There is more than one SD-WAN rule configured.
- B. The SD-WAN rules take precedence over regular policy routes.
- C. The all_rules rule represents the implicit SD-WAN rule.
- D. Entry 1(id=1) is a regular policy route.

Answer: AD

NEW QUESTION 2

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 3

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.)

- A. FortiGate flags the sessions as dirty.
- B. FortiGate continues routing the sessions with no SNAT, over port2.
- C. FortiGate performs a route lookup for the original traffic only.
- D. FortiGate updates the gateway information of the sessions with SNAT so that they use port1 instead of port2.

Answer: BD

NEW QUESTION 4

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
6D5rVsaKlMeAyVYt1z95BS24Psew761wY023hnFVviwb6deItSc51tCa+iNYhujT8gycfD4+Wus2pmuIv8rRzrVh
7DFkHaw2ZauAAprQ0dHUFaCzjOhME7mPw+8he2xB7Edb9ku/nZEhb0cKLkKYJc/p9J9IMweV2lZUgFjvIpXNxHxpH
LReOFShoH0lSPFKz5IYCVA==
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 5

Which are two benefits of using CLI templates in FortiManager? (Choose two.)

- A. You can reference meta fields.
- B. You can configure interfaces as SD-WAN members without having to remove references first.
- C. You can configure FortiManager to sync local configuration changes made on the managed device, to the CLI template.
- D. You can configure advanced CLI settings.

Answer: AD

NEW QUESTION 6

What are two benefits of using forward error correction (FEC) in IPsec VPNs? (Choose two.)

- A. FEC supports hardware offloading.
- B. FEC improves reliability of noisy links.
- C. FEC transmits parity packets that can be used to reconstruct packet loss.
- D. FEC can leverage multiple IPsec tunnels for parity packets transmission.

Answer: BC

NEW QUESTION 7

Which two settings can you configure to speed up routing convergence in BGP? (Choose two.)

- A. update-source
- B. set-route-tag
- C. holdtime-timer
- D. link-down-failover

Answer: CD

NEW QUESTION 8

Refer to the exhibit.

```
config firewall policy
  edit 1
    set anti-replay disable
  next
end
```

In a dual-hub hub-and-spoke SD-WAN deployment, which is a benefit of disabling the anti-replay setting on the hubs?

- A. It instructs the hub to disable the reordering of TCP packets on behalf of the receiver, to improve performance.
- B. It instructs the hub to disable TCP sequence number check, which is required for TCP sessions originated from spokes to fail over back and forth between the hubs.
- C. It instructs the hub to not check the ESP sequence numbers on IPsec traffic, to improve performance.
- D. It instructs the hub to skip content inspection on TCP traffic, to improve performance.

Answer: B

NEW QUESTION 9

Refer to the exhibits.

Exhibit A

```
config duplication
  edit 1
    set srcaddr "10.0.1.0/24"
    set dstaddr "10.1.0.0/24"
    set srcintf "port5"
    set dstintf "overlay"
    set service "ALL"
    set packet-duplication force
  next
end

branch1 fgt # diagnose sys sdwan zone
Zone SASE index=2
  members(0):
Zone overlay index=4
  members(3): 19(T_INET_0_0) 20(T_INET_1_0) 21(T_MPLS_0)
Zone underlay index=3
  members(2): 3(port1) 4(port2)
Zone virtual-wan-link index=1
  members(0):

1.274665 port5 in 10.0.1.101 -> 10.1.0.7: icmp: echo request
1.275788 T_INET_0_0 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
1.275790 T_INET_1_0 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
1.275801 T_MPLS_0 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
1.278365 T_INET_1_0 in 10.1.0.7 -> 10.0.1.101: icmp: echo reply
1.278553 port5 out 10.1.0.7 -> 10.0.1.101: icmp: echo reply
```

Exhibit B

```
3.874431 T_INET_1_0 in 10.0.1.101 -> 10.1.0.7: icmp: echo request
3.874630 port5 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
3.874895 T_INET_0_0 in 10.0.1.101 -> 10.1.0.7: icmp: echo request
3.875125 T_MPLS_0 in 10.0.1.101 -> 10.1.0.7: icmp: echo request
3.875054 port5 in 10.1.0.7 -> 10.0.1.101: icmp: echo reply
3.875308 T_INET_1_0 out 10.1.0.7 -> 10.0.1.101: icmp: echo reply
```

Exhibit A shows the packet duplication rule configuration, the SD-WAN zone status output, and the sniffer output on FortiGate acting as the sender. Exhibit B shows the sniffer output on a FortiGate acting as the receiver.

The administrator configured packet duplication on both FortiGate devices. The sniffer output on the sender FortiGate shows that FortiGate forwards an ICMP echo request packet over three overlays, but it only receives one reply packet through T_INET_1_0.

Based on the output shown in the exhibits, which two reasons can cause the observed behavior? (Choose two.)

- A. On the receiver FortiGate, packet-de-duplication is enabled.
- B. The ICMP echo request packets sent over T_INET_0_0 and T_MPLS_0 were dropped along the way.
- C. The ICMP echo request packets received over T_INET_0_0 and T_MPLS_0 were offloaded to NPU.
- D. On the sender FortiGate, duplication-max-num is set to 3.

Answer: AD

NEW QUESTION 10

Which two statements about SLA targets and SD-WAN rules are true? (Choose two.)

- A. When configuring an SD-WAN rule, you can select multiple SLA targets of the same performance SLA.
- B. SD-WAN rules use SLA targets to check if the preferred members meet the SLA requirements.
- C. SLA targets are used only by SD-WAN rules that are configured with Lowest Cost (SLA) or Maximize Bandwidth (SLA) as strategy.
- D. Member metrics are measured only if an SLA target is configured.

Answer: BD

NEW QUESTION 10

Refer to the exhibits. Exhibit A -

Edit Traffic Shaping Policy

IP Version: **IPv4** IPv6

Name: Limit_YouTube

Status: **Enable** Disable

Comments:
 0/255

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 Shaper** Assign 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: **Disable** Full ZTNA IP/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: Deny **Accept** IPSEC

Inspection Mode: **Flow-based** Proxy-based

Firewall/Network Options

NAT: ☒ NAT NAT46 NAT64

IP Pool Configuration: **Use Outgoing Interface Address** Use 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 Log ☐ Log Security Events **Log 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: C

NEW QUESTION 12

Refer to the exhibit.

```
branch1_fgt # diagnose sys sdwan service 3

Service(3): Address Mode(IPV4) flags=0x200 use-shortcut-sla
Gen(5), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(priority), link-cost-
factor(latency), link-cost-threshold(10), heath-check(VPN_PING)
Members(3):
  1: Seq_num(3 T_INET_0_0), alive, latency: 101.349, selected
  2: Seq_num(4 T_INET_1_0), alive, latency: 151.278, selected
  3: Seq_num(5 T_MPLS_0), alive, latency: 200.984, 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 priority-members 3 4 5
next
end
```

The exhibit shows the SD-WAN rule status and configuration.
Based on the exhibit, which change in the measured latency will make T_MPLS_0 the new preferred member?

- A. When T_INET_0_0 and T_MPLS_0 have the same latency.
- B. When T_MPLS_0 has a latency of 100 ms.
- C. When T_INET_0_0 has a latency of 250 ms.
- D. When T_N1PLS_0 has a latency of 80 ms.

Answer: D

NEW QUESTION 13

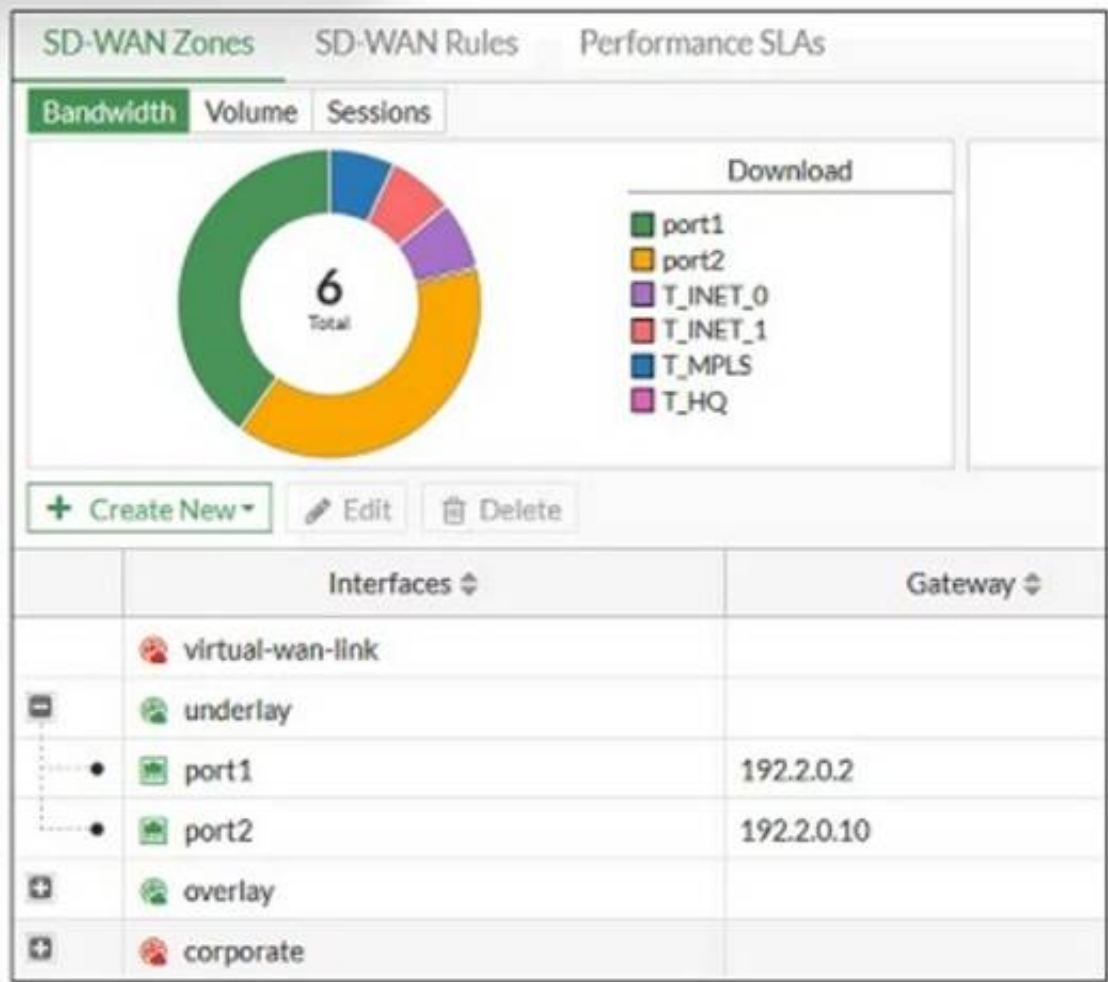
Which components make up the secure SD-WAN solution?

- A. Application, antivirus, and URL, and SSL inspection
- B. Datacenter, branch offices, and public cloud
- C. FortiGate, FortiManager, FortiAnalyzer, and FortiDeploy
- D. Telephone, ISDN, and telecom network.

Answer: C

NEW QUESTION 18

Refer to the exhibit, which shows an SD-WAN zone configuration on the FortiGate GUI.



Based on the exhibit, which statement is true?

- A. You can delete the virtual-wan-link zone because it contains no member.
- B. The corporate zone contains no member.
- C. You can move port1 from the underlay zone to the overlay zone.
- D. The overlay zone contains four members.

Answer: B

Explanation:

Based on the exhibit, the "corporate" zone contains no member (B). In the FortiGate GUI, zones without members do not display any interfaces listed under them, which is the case for the corporate zone in the exhibit. References: This conclusion is based on standard Fortinet GUI interpretation and the operational logic of SD-WAN zones as per Fortinet's guidelines and user interface standards.

NEW QUESTION 19

Refer to the exhibits. Exhibit A -

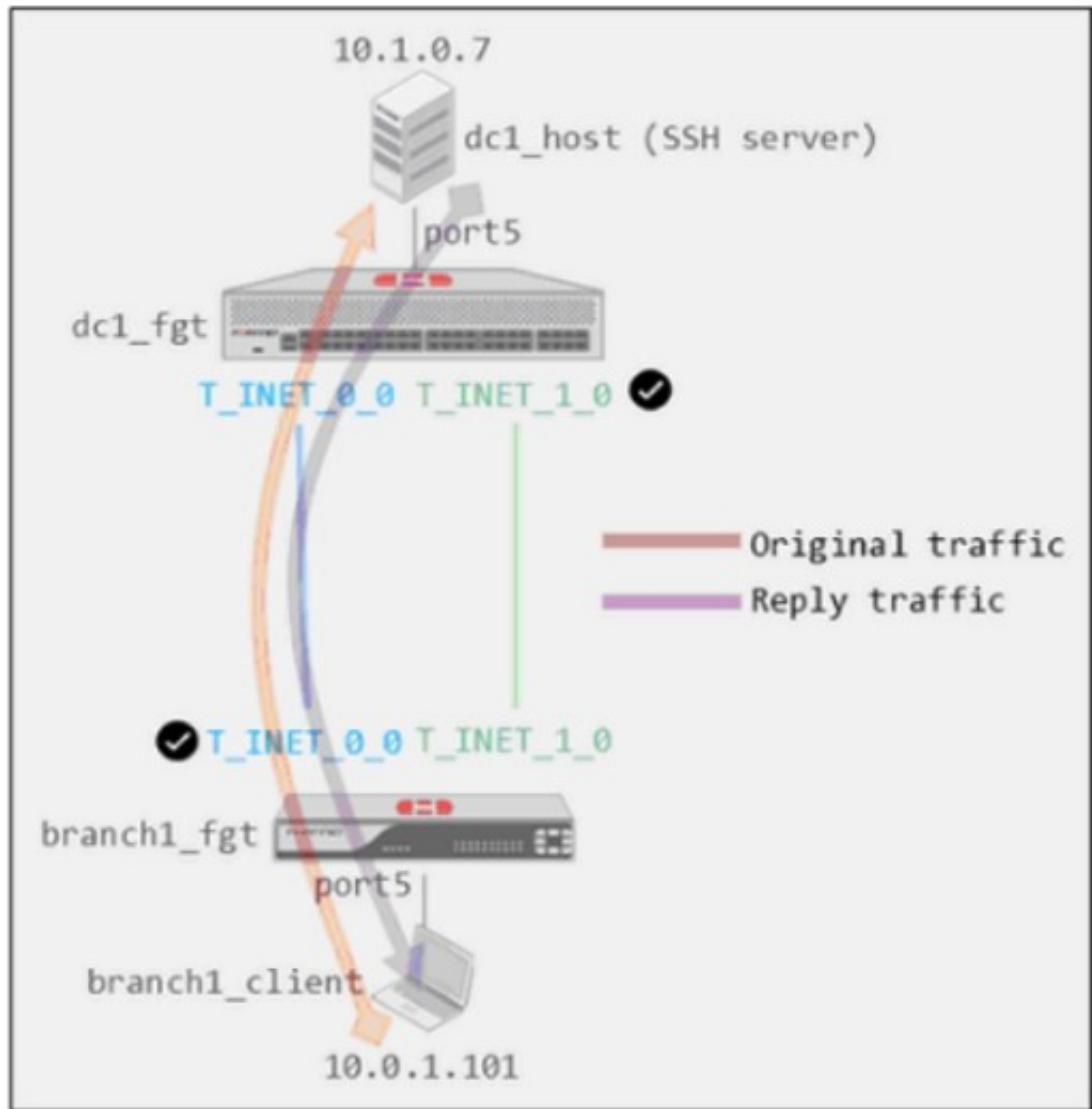


Exhibit B -

```
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

NEW QUESTION 21

The SD-WAN overlay template helps to prepare SD-WAN deployments. To complete the tasks performed by the SD-WAN overlay template, the administrator must perform some post-run tasks. What are three mandatory post-run tasks that must be performed? (Choose three.)

- A. Create policy packages for branch devices.

- B. Assign an sdwan_id metadata variable to each device (branch and hub).
- C. Configure routing through overlay tunnels created by the SD-WAN overlay template.
- D. Assign a branch_id metadata variable to each branch device.
- E. Configure SD-WAN rules.

Answer: ABC

NEW QUESTION 25

Exhibit A shows the firewall policy and exhibit B shows the traffic shaping policy.

Exhibit A

Exhibit B

Edit Policy

Name ⓘ

Internet Access

Incoming interface

port3

Outgoing interface

virtual-wan link

Source

all

+

x

Destination

all

+

x

Schedule

always

Service

ALL

+

x

Action

✓ ACCEPT

⊘ DENY

Inspection Mode

Flow-based

Proxy-based

Firewall / Network Options

NAT

⏻

IP Pool Configuration

Use Outgoing Interface Address

Use Dynamic

Preserve Source Port

⏻

Protocol Options

PROT

default

▼

Exhibit A

Exhibit B

Edit Traffic Shaping Policy

Name

inbound_outbound_shaper

Status

Enabled

Disabled

Comments

Write a comment...

0/255

If Traffic Matches:

Source

all

+

x

Destination

all

+

x

Schedule

Service

ALL

+

x

Application

+

URL Category

Streaming Media and Download

+

x

Then:

Action

Apply Shaper

Assign Shaping Class ID

Outgoing interface

virtual-wan link

+

x

Shared shaper

guarantee-10mbps

The traffic shaping policy is being applied to all outbound traffic; however, inbound traffic is not being evaluated by the shaping policy. Based on the exhibits, what configuration change must be made in which policy so that traffic shaping can be applied to inbound traffic?

- A. Create a new firewall policy, and the select the SD-WAN zone as Incoming Interface.
- B. In the traffic shaping policy, select Assign Shaping Class ID as Action.
- C. In the firewall policy, select Proxy-based as Inspection Mode.
- D. In the traffic shaping policy, enable Reverse shaper, and then select the traffic shaper to use.

Answer: D

NEW QUESTION 30

What are two advantages of using an IPsec recommended template to configure an IPsec tunnel in a hub-and-spoke topology? (Choose two.)

- A. VPN monitor tool provides additional statistics for tunnels defined with an IPsec recommended template.
- B. FortiManager automatically installs IPsec tunnels to every spoke when they are added to the FortiManager ADOM.
- C. IPsec recommended template guides the administrator to use Fortinet recommended settings.
- D. IPsec recommended template ensures consistent settings between phase1 and phase2

Answer: BC

Explanation:

According to the SD-WAN 7.2 Study Guide, IPsec recommended templates are designed to simplify the configuration of IPsec tunnels in a hub-and-spoke topology. They have the following advantages:
 ? FortiManager automatically installs IPsec tunnels to every spoke when they are added to the FortiManager ADOM. This reduces the manual effort and ensures that all spokes have the same configuration.
 ? IPsec recommended template guides the administrator to use Fortinet recommended settings, such as encryption algorithms, key lifetimes, and dead peer detection. This ensures optimal performance and security of the IPsec tunnels.

NEW QUESTION 35

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

Explanation:

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

NEW QUESTION 37

What are two benefits of choosing packet duplication over FEC for data loss correction on noisy links? (Choose two.)

- A. Packet duplication can leverage multiple IPsec overlays for sending additional data.
- B. Packet duplication does not require a route to the destination.
- C. Packet duplication supports hardware offloading.
- D. Packet duplication uses smaller parity packets which results in less bandwidth consumption.

Answer: AC

NEW QUESTION 39

Which statement is correct about SD-WAN and ADVPN?

- A. Routes for ADVPN shortcuts must be manually configured.
- B. SD-WAN can steer traffic to ADVPN shortcuts, established over IPsec overlays, configured as SD-WAN members.
- C. SD-WAN does not monitor the health and performance of ADVPN shortcuts.
- D. You must use IKEv2 on IPsec tunnels.

Answer: B

NEW QUESTION 42

Refer to the exhibit.

```
# diagnose firewall shaper per-ip-shaper list
name FTP_5M
maximum-bandwidth 625 KB/sec
maximum-concurrent-session 5
tos ff/ff
packets dropped 65
bytes dropped 81040
    addr=10.1.0.1 status: bps=0 ses=1
    addr=10.1.0.100 status: bps=0 ses=1
    addr=10.1.10.1 status: bps=1656 ses=3
```

Which are two expected behaviors of the traffic that matches the traffic shaper? (Choose two.)

- A. The number of simultaneous connections among all source IP addresses cannot exceed five connections.
- B. The traffic shaper limits the combined bandwidth of all connections to a maximum of 5 MB/sec.
- C. The number of simultaneous connections allowed for each source IP address cannot exceed five connections.
- D. The traffic shaper limits the bandwidth of each source IP address to a maximum of 625 KB/sec.

Answer: CD

NEW QUESTION 44

.....

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-7.2 Practice Exam Features:

- * NSE7_SDW-7.2 Questions and Answers Updated Frequently
- * NSE7_SDW-7.2 Practice Questions Verified by Expert Senior Certified Staff
- * NSE7_SDW-7.2 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * NSE7_SDW-7.2 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The NSE7_SDW-7.2 Practice Test Here](#)