

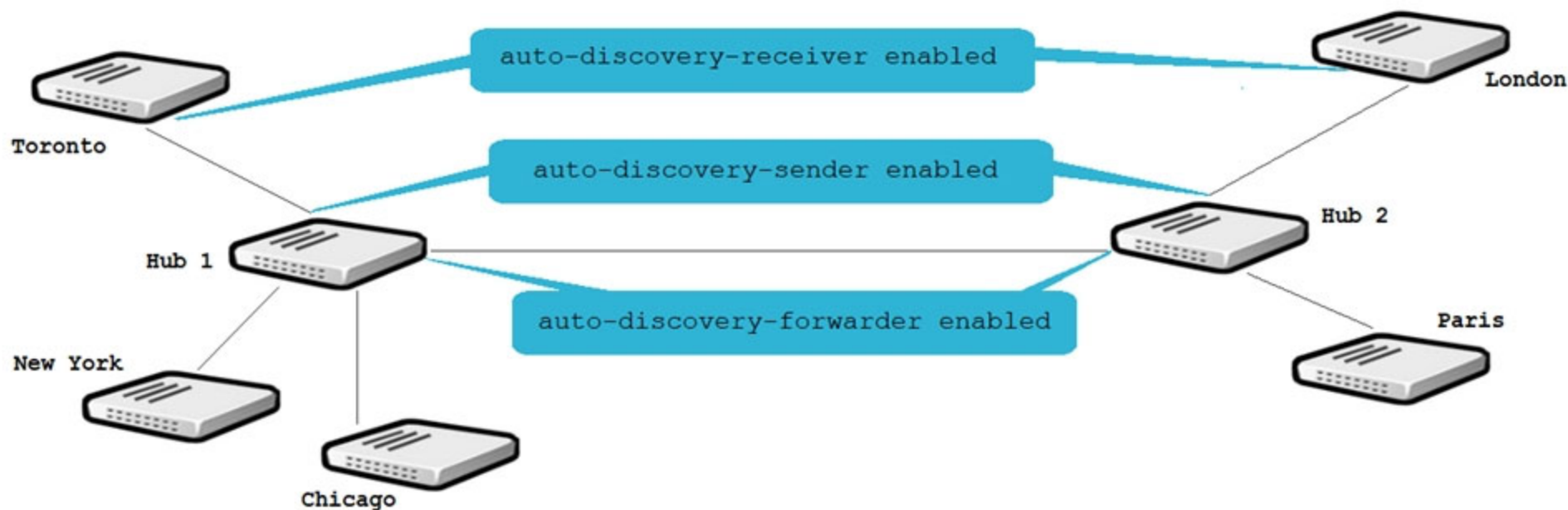
Actual exam question from Fortinet's NSE7_SDW-6.4

Question #: 1

Topic #: 1

[\[All NSE7_SDW-6.4 Questions\]](#)

Refer to the exhibit.



Multiple IPsec VPNs are formed between two hub-and-spokes groups, and site-to-site between Hub 1 and Hub 2. The administrator configured ADVPN on the dual regions topology.

Which two statements are correct if a user in Toronto sends traffic to London? (Choose two.)

- A. Toronto needs to establish a site-to-site tunnel with Hub 2 to bypass Hub 1.
- B. The first packets from Toronto to London are routed through Hub 1 then to Hub 2.
- C. London generates an IKE information message that contains the Toronto public IP address.
- D. Traffic from Toronto to London triggers the dynamic negotiation of a direct site-to-site VPN.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_SDW-6.4

Question #: 2

Topic #: 1

[\[All NSE7_SDW-6.4 Questions\]](#)

Refer to exhibits.

Exhibit A
Exhibit B

Edit Traffic Shaping Policy

Name

Status ↑ Enabled ↓ Disabled

Comments 0/255

If Traffic Matches:

Source + ✕

Destination + ✕

Schedule

Service + ✕

Application i +

URL Category + ✕

Then:

Action Apply Shaper Assign Shaping Class ID

Outgoing interface + ✕

Shared shaper

Reverse shaper

Per-IP shaper

Exhibit A
Exhibit B

Edit Policy

Name i

Incoming interface

Outgoing interface

Source + ✕

Destination + ✕

Schedule

Service + ✕

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

Security Profiles

AntiVirus

WebFilter

DNS Filter

Application Control

IPS

SSL Inspection SSL ✎

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

FortiGate is not performing traffic shaping as expected, based on the policies shown in the exhibits.

To correct this traffic shaping issue on FortiGate, what configuration change must be made on which policy?

- A. The URL category must be specified on the traffic shaping policy.
- B. The shaper mode must be applied per-IP shaper on the traffic shaping policy.
- C. The web filter profile must be enabled on the firewall policy.
- D. The application control profile must be enabled on the firewall policy.

Show Suggested Answer



Actual exam question from Fortinet's NSE7_SDW-6.4

Question #: 3

Topic #: 1

[\[All NSE7_SDW-6.4 Questions\]](#)

Which statement defines how a per-IP traffic shaper of 10 Mbps is applied to the entire network?

- A. The 10 Mbps bandwidth is shared equally among the IP addresses.
- B. Each IP is guaranteed a minimum 10 Mbps of bandwidth.
- C. FortiGate allocates each IP address a maximum 10 Mbps of bandwidth.
- D. A single user uses the allocated bandwidth divided by total number of users.

Show Suggested Answer





Actual exam question from Fortinet's NSE7_SDW-6.4

Question #: 4

Topic #: 1

[\[All NSE7_SDW-6.4 Questions\]](#)

Which three parameters are available to configure SD-WAN rules? (Choose three.)

- A. Application signatures
- B. URL categories
- C. Internet service database (ISDB) address object
- D. Source and destination IP address
- E. Type of physical link connection

Show Suggested Answer





Actual exam question from Fortinet's NSE7_SDW-6.4

Question #: 5

Topic #: 1

[\[All NSE7_SDW-6.4 Questions\]](#)

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

- A. diagnose sys virtual-wan-link health-check
- B. diagnose sys virtual-wan-link log
- C. diagnose sys virtual-wan-link sla-log
- D. diagnose sys virtual-wan-link intf-sla-log

Show Suggested Answer





Actual exam question from Fortinet's NSE7_SDW-6.4

Question #: 6

Topic #: 1

[\[All NSE7_SDW-6.4 Questions\]](#)

Which diagnostic command can you use to show the SD-WAN rules interface information and state?

- A. diagnose sys virtual-wan-link route-tag-list.
- B. diagnose sys virtual-wan-link service.
- C. diagnose sys virtual-wan-link member.
- D. diagnose sys virtual-wan-link neighbor.

Show Suggested Answer



Actual exam question from Fortinet's NSE7_SDW-6.4

Question #: 7

Topic #: 1

[\[All NSE7_SDW-6.4 Questions\]](#)

Refer to exhibits.

Exhibit A		Exhibit B				
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 A		Exhibit B				
<pre> 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 </pre>						

Exhibit A shows the performance SLA exhibit B shows the SD-WAN diagnostics output.

Based on the exhibits, which statement is correct?

- A. Port1 became dead because no traffic was offload through the egress of port1.
- B. SD-WAN member interfaces are affected by the SLA state of the inactive interface.
- C. Both SD-WAN member interfaces have used separate SLA targets.
- D. The SLA state of port1 is dead after five unanswered requests by the SLA servers.

Show Suggested Answer



Actual exam question from Fortinet's NSE7_SDW-6.4

Question #: 8

Topic #: 1

[\[All NSE7_SDW-6.4 Questions\]](#)

Which statement is correct about the SD-WAN and ADVPN?

- A. Spoke support dynamic VPN as a static interface.
- B. Dynamic VPN is not supported as an SD-WAN interface.
- C. ADVPN interface can be a member of SD-WAN interface.
- D. Hub FortiGate is limited to use ADVPN as SD-WAN member interface.

Show Suggested Answer





Actual exam question from Fortinet's NSE7_SDW-6.4

Question #: 9

Topic #: 1

[\[All NSE7_SDW-6.4 Questions\]](#)

Which two reasons make forward error correction (FEC) ideal to enable in a phase one VPN interface? (Choose two.)

- A. FEC is useful to increase speed at which traffic is routed through IPsec tunnels.
- B. FEC transmits the original payload in full to recover the error in transmission.
- 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.
- E. FEC reduces the stress on the remote device jitter buffer to reconstruct packet loss.

Show Suggested Answer



Actual exam question from Fortinet's NSE7_SDW-6.4

Question #: 10

Topic #: 1

[\[All NSE7_SDW-6.4 Questions\]](#)

Refer to exhibits.

Exhibit A

Exhibit B

```
config system global
    set snat-route-change enable
end
```

Exhibit A

Exhibit B

```
FortiGate # get router info routing-table details
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 192.168.73.2, port2, [1/0]
      [1/0] via 192.168.1.1, port1, [10/0]
C     10.0.1.0/24 is directly connected, port3
C     192.168.1.0/24 is directly connected, port1
C     192.168.73.0/24 is directly connected, port2
```

Exhibit A shows the source NAT global setting and exhibit B shows the routing table on FortiGate.

Based on the exhibits, which two statements about increasing the port2 interface priority to 20 are true? (Choose two.)

- A. All the existing sessions that do not use SNAT will be flushed and routed through port1.
- B. All the existing sessions will continue to use port2, and new sessions will use port1.
- C. All the existing sessions using SNAT will be flushed and routed through port1.
- D. All the existing sessions will be blocked from using port1 and port2.

Show Suggested Answer



Actual exam question from Fortinet's NSE7_SDW-6.4

Question #: 11

Topic #: 1

[\[All NSE7_SDW-6.4 Questions\]](#)

Which components make up the secure SD-WAN solution?

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

Show Suggested Answer



Actual exam question from Fortinet's NSE7_SDW-6.4

Question #: 12

Topic #: 1

[\[All NSE7_SDW-6.4 Questions\]](#)

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 status of the VPN tunnel are true? (Choose two.)

- A. There are separate virtual interfaces for each dial-up client.
- B. VPN static routes are prevented from populating the FortiGate routing table.
- C. FortiGate created a single IPsec virtual interface that is shared by all clients.
- D. 100.64.3.1 is one of the remote IP address that comes through index interface 1.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_SDW-6.4

Question #: 13

Topic #: 1

[\[All NSE7_SDW-6.4 Questions\]](#)

Refer to exhibits.

Exhibit A		Exhibit B			
ID	Name	Source	Destination	Criteria	Members
IPv4 3					
1	Google.ICMP	all	Google-ICMP	Latency	port1 port2
2	Vimeo	all	Vimeo		port2
3	All_Access_Rules	all	all		port1
Implicit 1					
	sd-wan	all	all	Source-Destination IP	any

Exhibit A		Exhibit B				
Date/Time	Source	Destination	Application Name	Result	Policy	Destination Interface
2020/10/15 11:12:27	10.0.1.10	151.101.250.109 (i.vimeocdn.com)	Vimeo	UTM Allowed	Internet Access (1)	port2
2020/10/15 11:12:22	10.0.1.10	34.120.15.67 (fresnel-events.vimeocdn.com)	Vimeo	2.00 kB / 4.33 kB	Internet Access (1)	port1
2020/10/15 11:12:20	10.0.1.10	172.217.13.227 (ocsp.pki.goog)	OCSP	1.28 kB / 1.49 kB	Internet Access (1)	port1
2020/10/15 11:12:07	10.0.1.10	23.47.205.151 (detectportal.firefox.com)	HTTP.BROWSER_Firefox	1.44 kB / 1.55 kB	Internet Access (1)	port1
2020/10/15 11:12:07	10.0.1.10	23.47.205.151 (detectportal.firefox.com)	HTTP.BROWSER_Firefox	1.43 kB / 1.60 kB	Internet Access (1)	port1
2020/10/15 11:12:04	10.0.1.10	99.84.221.62 (snippets.cdn.mozilla.net)	HTTPS.BROWSER	2.08 kB / 13.44 kB	Internet Access (1)	port1

Exhibit A shows the SD-WAN rules and exhibit B shows the traffic logs. The SD-WAN traffic logs reflect how FortiGate processed traffic.

Which two statements about how the configured SD-WAN rules are processing traffic are true? (Choose two.)

- A. The implicit rule overrides all other rules because parameters widely cover sources and destinations.
- B. SD-WAN rules are evaluated in the same way as firewall policies: from top to bottom.
- C. The All_Access_Rules rule load balances Vimeo application traffic among SD-WAN member interfaces.
- D. The initial session of an application goes through a learning phase in order to apply the correct rule.

Show Suggested Answer



Actual exam question from Fortinet's NSE7_SDW-6.4

Question #: 14

Topic #: 1

[\[All NSE7_SDW-6.4 Questions\]](#)

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.

Show Suggested Answer



Actual exam question from Fortinet's NSE7_SDW-6.4

Question #: 15

Topic #: 1

[\[All NSE7_SDW-6.4 Questions\]](#)

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 tupless=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 gw=192.168.73.2/10.0.1.10
hook=post dir=org act=snat 10.0.1.10:2246->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=00000a2c 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. Changes have been made on firewall policy ID 1 on FortiGate.
- C. Firewall policy ID 1 has source NAT disabled.
- D. FortiGate has terminated the session after a change on policy ID 1.

Show Suggested Answer



Actual exam question from Fortinet's NSE7_SDW-6.4

Question #: 16

Topic #: 1

[\[All NSE7_SDW-6.4 Questions\]](#)

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. FortiGate has obtained a configuration from the platform template in FortiGate cloud.
- D. A factory reset performed on FortiGate.
- E. The zero-touch provisioning process has completed internally, behind FortiGate.

Show Suggested Answer





Actual exam question from Fortinet's NSE7_SDW-6.4

Question #: 17

Topic #: 1

[\[All NSE7_SDW-6.4 Questions\]](#)

Which two statements reflect the benefits of implementing the ADVPN solution to replace conventional VPN topologies? (Choose two.)

- A. It creates redundant tunnels between hub-and-spokes, in case failure takes place on the primary links.
- B. It dynamically assigns cost and weight between the hub and the spokes, based on the physical distance.
- C. It ensures that spoke-to-spoke traffic no longer needs to flow through the tunnels through the hub.
- D. It provides direct connectivity between all sites by creating on-demand tunnels between spokes.

Show Suggested Answer



Actual exam question from Fortinet's NSE7_SDW-6.4

Question #: 18

Topic #: 1

[\[All NSE7_SDW-6.4 Questions\]](#)

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

Show Suggested Answer

Actual exam question from Fortinet's NSE7_SDW-6.4

Question #: 19

Topic #: 1

[\[All NSE7_SDW-6.4 Questions\]](#)

Refer to the exhibit.

```
FortiGate # 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 two statements about the debug output are correct? (Choose two.)

- A. The debug output shows per-IP shaper values and real-time readings.
- B. This traffic shaper drops traffic that exceeds the set limits.
- C. Traffic being controlled by the traffic shaper is under 1 Kbps.
- D. FortiGate provides statistics and reading based on historical traffic logs.

Show Suggested Answer



Actual exam question from Fortinet's NSE7_SDW-6.4

Question #: 20

Topic #: 1

[\[All NSE7_SDW-6.4 Questions\]](#)

In the default SD-WAN minimum configuration, which two statements are correct when traffic matches the default implicit SD-WAN rule? (Choose two.)

- A. Traffic has matched none of the FortiGate policy routes.
- B. Matched traffic failed RPF and was caught by the rule.
- C. The FIB lookup resolved interface was the SD-WAN interface.
- D. An absolute SD-WAN rule was defined and matched traffic.

Show Suggested Answer



Actual exam question from Fortinet's NSE7_SDW-6.4

Question #: 21

Topic #: 1

[\[All NSE7_SDW-6.4 Questions\]](#)

Refer to the exhibit.

```
id=20085 trace_id=5087 func=print_pkt_detail line=5588 msg="vd-root:0 received a
packet(proto=6, 10.1.10.1:41370->31.13.80.12:443) from port3. flag [.] , seq 1213725680,
ack 1169005655, win 65535"
id=20085 trace_id=5087 func=resolve_ip_tuple_fast line=5669 msg="Find an existing
session, id-00001ca4, original direction"
id=20085 trace_id=5087 func=fw_forward_dirty_handler line=447 msg="blocked by quota
check, drop"
```

Which statement about the trace evaluation by FortiGate is true?

- A. Packets exceeding the configured maximum concurrent connection limit are denied by the per-IP shaper.
- B. The packet exceeded the configured bandwidth and was dropped based on the priority configuration.
- C. The packet exceeded the configured maximum bandwidth and was dropped by the shared shaper.
- D. Packets exceeding the configured concurrent connection limit are dropped based on the priority configuration.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_SDW-6.4

Question #: 22

Topic #: 1

[\[All NSE7_SDW-6.4 Questions\]](#)

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.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_SDW-6.4

Question #: 23

Topic #: 1

[\[All NSE7_SDW-6.4 Questions\]](#)

Refer to exhibits.

Exhibit A

Exhibit B

Edit Policy

Name i	Internet Access
Incoming interface	port3 ▼
Outgoing interface	SD-WAN ▼
Source	all + x
Destination	all + x
Schedule	always ▼
Service	ALL + x
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY
Inspection Mode	<input checked="" type="checkbox"/> Flow-based <input type="checkbox"/> Proxy-based

Firewall / Network Options

NAT	<input checked="" type="checkbox"/>
IP Pool Configuration	<input checked="" type="checkbox"/> Use Outgoing Interface Address <input type="checkbox"/> Use Dynamic
Preserve Source Port	<input type="checkbox"/>
Protocol Options	<input checked="" type="checkbox"/> PRX <input type="checkbox"/> default ▼

Exhibit A

Exhibit B

Edit Traffic Shaping Policy

Name	inbound_outbound_shaper
Status	<input checked="" type="checkbox"/> Enabled <input type="checkbox"/> Disabled
Comments	Write a comment... 0/255

If Traffic Matches:

Source	all + x
Destination	all + x
Schedule	<input type="checkbox"/>
Service	ALL + x
Application i	+
URL Category	+

Then:

Action	<input checked="" type="checkbox"/> Apply Shaper <input type="checkbox"/> Assign Shaping Class ID
Outgoing interface	SD-WAN + x
Shared shaper	<input checked="" type="checkbox"/> guarantee-10mbps ▼
Reverse shaper	<input type="checkbox"/>
Per-IP shaper	<input type="checkbox"/>

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

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?

- The guaranteed-10mbps option must be selected as the per-IP shaper option.
- The guaranteed-10mbps option must be selected as the reverse shaper option.
- A new firewall policy must be created and SD-WAN must be selected as the incoming interface.
- The reverse shaper option must be enabled and a traffic shaper must be selected.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_SDW-6.4

Question #: 24

Topic #: 1

[\[All NSE7_SDW-6.4 Questions\]](#)

Refer to the exhibit.

VPN Community Install Wizard

All VPN Communities

H2S Dial up

Name: **H2S**
 Number of VPN: **3**
 Authentication: **Pre-shared Key**

IKE Security (Phase 1) Properties: **aes128-sha256, aes256-sha256, aes128-sha1, aes256-sha1**
 IPsec Security (Phase 2) Properties: **aes128-sha1, aes256-sha1, aes128-sha256, aes256-sha256, aes128gcm, aes256gcm, chacha20poly1305**

Edit

+ Create New Edit Clone Delete Column Settings

Name	Role	Default VPN Interface	Protected Subnet
<input type="checkbox"/> NFGW-1[root]	Hub	port1	SSLVPN_TUNNEL_ADDR1
<input type="checkbox"/> Spoke-1	Spoke	port1	FABRIC_DEVICE
<input type="checkbox"/> Spoke-2	Spoke	port1	FIREWALL_AUTH_PORTAL_ADDRESS

What must you configure to enable ADVPN?

- A. ADVPN should only be enabled on unmanaged FortiGate devices.
- B. Each VPN device has a unique pre-shared key configured separately on phase one.
- C. The protected subnets should be set to address object to all (0.0.0.0/0).
- D. On the hub VPN, only the device needs additional phase one settings.

Show Suggested Answer



Actual exam question from Fortinet's NSE7_SDW-6.4

Question #: 25

Topic #: 1

[\[All NSE7_SDW-6.4 Questions\]](#)

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.

Show Suggested Answer



Actual exam question from Fortinet's NSE7_SDW-6.4

Question #: 26

Topic #: 1

[\[All NSE7_SDW-6.4 Questions\]](#)

What are two benefits of 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.

Show Suggested Answer





Actual exam question from Fortinet's NSE7_SDW-6.4

Question #: 27

Topic #: 1

[\[All NSE7_SDW-6.4 Questions\]](#)

What would best describe the SD-WAN traffic shaping mode that bases itself on a percentage of available bandwidth?

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

Show Suggested Answer



Actual exam question from Fortinet's NSE7_SDW-6.4

Question #: 28

Topic #: 1

[\[All NSE7_SDW-6.4 Questions\]](#)

Refer to exhibits.

Exhibit A	Exhibit B
Link Status	
Check interval	<input type="text" value="500"/> ms
Failures before inactive i	<input type="text" value="3"/>
Restore link after i	<input type="text" value="2"/> check(s)
Actions when Inactive	
Update static route i	<input checked="" type="checkbox"/>

Exhibit A	Exhibit B
<pre>FortiGate # diagnose sys virtual-wan-link health-check Seq(1 port1): state(alive), packet-loss(0.000%) latency(15.049), jitter(2.739) sla_map=0x0 Seq(2 port2): state(dead), packet-loss(5.000%) sla_map=0x0</pre>	

Exhibit A, which shows the SD-WAN performance SLA and exhibit B shows the health of the participating SD-WAN members.

Based on the exhibits, which statement is correct?

- A. The dead member interface stays unavailable until an administrator manually brings the interface back.
- B. Port2 needs to wait 500 milliseconds to change the status from alive to dead.
- C. The SLA state of port2 has exceeded three consecutive unanswered requests from the SLA server.
- D. Check interval is the time to wait before a packet sent by a member interface considered as lost.

Show Suggested Answer



Actual exam question from Fortinet's NSE7_SDW-6.4

Question #: 29

Topic #: 1

[\[All NSE7_SDW-6.4 Questions\]](#)

What is the Inkmttd process responsible for?

- A. Flushing route tags addresses
- B. Monitoring links for any bandwidth saturation
- C. Logging interface quality information
- D. Processing performance SLA probes

Show Suggested Answer



Actual exam question from Fortinet's NSE7_SDW-6.4

Question #: 30

Topic #: 1

[\[All NSE7_SDW-6.4 Questions\]](#)

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

- A. VPN topologies are formed using only BGP dynamic routing with SD-WAN.
- B. Route tags are used for a BGP community and the SD-WAN rules are assigned the same tag.
- C. BGP tags require that the adding of static routes be enabled on all ADVPN interfaces.
- D. BGP tags match the SD-WAN rule based on the order that these rules were installed.

Show Suggested Answer





Actual exam question from Fortinet's NSE7_SDW-6.4

Question #: 31

Topic #: 1

[\[All NSE7_SDW-6.4 Questions\]](#)

Which statement about using BGP routes in SD-WAN is true?

- A. Adding static routes must be enabled on all ADVPN interfaces.
- B. VPN topologies must be form using only BGP dynamic routing with SD-WAN.
- C. Learned routes can be used as dynamic destinations in SD-WAN rules.
- D. Dynamic routing protocols can be used only with non-encrypted traffic.

Show Suggested Answer





Actual exam question from Fortinet's NSE7_SDW-6.4

Question #: 32

Topic #: 1

[\[All NSE7_SDW-6.4 Questions\]](#)

An administrator is troubleshooting VoIP quality issues that occur when calling external phone numbers. The SD-WAN interface on the edge FortiGate is configured with the default settings, and is using two upstream links. One link has random jitter and latency issues, and is based on a wireless connection. Which two actions must the administrator apply simultaneously on the edge FortiGate to improve VoIP quality using SD-WAN rules? (Choose two.)

- A. Select the corresponding SD-WAN balancing strategy in the SD-WAN rule.
- B. Choose the suitable interface based on the interface cost and weight.
- C. Use the performance SLA targets to detect latency and jitter instantly.
- D. Place the troublesome link at the top of the interface preference list.
- E. Configure an SD-WAN rule to load balance all traffic without VoIP.

Show Suggested Answer



Actual exam question from Fortinet's NSE7_SDW-6.4

Question #: 33

Topic #: 1

[\[All NSE7_SDW-6.4 Questions\]](#)

Refer to exhibits.

Exhibit A
Exhibit B

Link Status

Check interval

Failures before inactive i

Restore link after i

ms

check(s)

Actions when Inactive

Update static route i

Exhibit A
Exhibit B

Interfaces	Gateway	Cost	Download	Upload
port1	10.200.1.254	0	0 bps	0 bps
port2	10.200.2.254	0	0 bps	0 bps

Destination ↕	Gateway IP ↕	Interface ↕	Status ↕
IPv4 4			
0.0.0.0/0		SD-WAN	✓ Enabled
10.0.20.0/23	192.168.1.1	port1	✓ Enabled
100.64.1.0/24	192.168.73.2	port2	✓ Enabled
172.20.0.0/16	192.168.73.2	port2	✓ Enabled

Exhibit A shows the SD-WAN performance SLA and exhibit B shows the SD-WAN interface and the static routes configuration.

Port1 and port2 are member interfaces of the SD-WAN, and port2 becomes a dead member after reaching the failure thresholds.

Which statement about the dead member is correct?

- A. Port2 might become alive when a single response is received from an SLA server.
- B. Dead members require manual administrator access to bring them back alive.
- C. Subnets 100.64.1.0/24 and 172.20.0.0/16 are reachable only through port1.
- D. SD-WAN interface becomes disabled and port1 becomes the WAN interface.

Show Suggested Answer



Actual exam question from Fortinet's NSE7_SDW-6.4

Question #: 34

Topic #: 1

[\[All NSE7_SDW-6.4 Questions\]](#)

What are two roles that SD-WAN orchestrator plays when it works with FortiManager? (Choose two.)

- A. It configures and monitors SD-WAN networks on FortiGate devices that are managed by FortiManager.
- B. It acts as a standalone device to assist FortiManager to manage SD-WAN interfaces on the managed FortiGate devices.
- C. It acts as a hub FortiGate with an SD-WAN interface enabled and managed along with other FortiGate devices by FortiManager.
- D. It acts as an application that is released and signed by Fortinet to run as a part of management extensions on FortiManager.

Show Suggested Answer



Actual exam question from Fortinet's NSE7_SDW-6.4

Question #: 35

Topic #: 1

[\[All NSE7_SDW-6.4 Questions\]](#)

Refer to the exhibit.

```
config system virtual-wan-link
  config service
    edit 1
      set name "Tagged_Traffic"
      set mode manual
      set route-tag 15
    next
  end
end
```

Which statement about the command route-tag in the SD-WAN rule is true?

- A. It ensures route tags match the SD-WAN rule based on the rule order.
- B. It tags each route and references the tag in the routing table.
- C. It enables the SD-WAN rule to load balance and assign traffic with a route tag.
- D. It uses route tags for a BGP community and assigns the SD-WAN rules with same tag.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_SDW-6.4

Question #: 36

Topic #: 1

[\[All NSE7_SDW-6.4 Questions\]](#)

Which two configuration tasks are required to use SD-WAN? (Choose two.)

- A. Add one or more members to an SD-WAN zone.
- B. Configure at least one firewall policy for SD-WAN traffic.
- C. Specify the outgoing interface routing cost.
- D. Specify the incoming interfaces in SD-WAN rules.

Show Suggested Answer



Actual exam question from Fortinet's NSE7_SDW-6.4

Question #: 37

Topic #: 1

[\[All NSE7_SDW-6.4 Questions\]](#)

Refer to the exhibit.

```
ike 0:H2S_0_0:2: notify msg received: SHORTCUT-QUERY
ike 0:H2S_0_0: rcv shortcut-query 289635615481843711
ce3375c4c7fb498f/0000000000000000
100.64.3.1 10.1.1.254->10.1.2.254 psk 64 ppk 0 ttl 32 nat 0 ver 1 mode 0
ike 0:H2S_0: iif 15 10.1.1.254->10.1.2.254 route lookup oif 15
ike 0:H2S_0_1: forward shortcut-query 289635615481843711
ce3375c4c7fb498f/0000000000000000 100.64.3.1 10.1.1.254->10.1.2.254 psk 64
ppk 0 ttl 31
ver 1 mode 0, ext-mapping 100.64.3.1:500
```

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

- A. This is a spoke that has received a query from a remote hub and has forwarded the response to its hub.
- B. Two hubs, 10.1.1.254 and 10.1.2.254, are receiving and forwarding queries between each other.
- C. Two spokes, 100.64.3.1 and 10.1.2.254, forward their queries to their hubs.
- D. This is a hub that has received a query from a spoke and has forwarded it to another spoke.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_SDW-6.4

Question #: 38

Topic #: 1

[\[All NSE7_SDW-6.4 Questions\]](#)

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. Three packets are exchanged between an initiator and a responder instead of six packets.
- D. The use of Diffie Hellman keys is limited by the responder and needs initiator acceptance.

Show Suggested Answer



Actual exam question from Fortinet's NSE7_SDW-6.4

Question #: 39

Topic #: 1

[\[All NSE7_SDW-6.4 Questions\]](#)

Refer to the exhibit.

```
FortiGate # diagnose firewall proute list
list route policy info(vf-root):

id=1 dscp tag=0xff 0xff flags=0x0 tos=0x00 tos mask=0x00 protocol=0 sport=
0:0 iif=0
dport=0-65535 oif=3 (port1)
source wildcard(1): 0.0.0.0/0.0.0.0
destination wildcard(1): 100.64.1.0/255.255.255.0
hit_count=4 last_used=2020-10-16 07:49:10

id=0x7f090001 vwl_service=1 (Google.ICMP), 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 oif=3
(port1)
oif=4 (port2)
source(1): 0.0.0.0-255.255.255.255
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(1): Vimeo(4294838044, 0, 0, 0 25360)
hit_count=0 last_used=2020-10-16 07:49:14

id=0x7f090003 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 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=2020-10-16 07:49:14
```

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

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

Show Suggested Answer



Actual exam question from Fortinet's NSE7_SDW-6.4

Question #: 40

Topic #: 1

[\[All NSE7_SDW-6.4 Questions\]](#)

Which diagnostic command can you use to show the SD-WAN rules interface information and state?

- A. diagnose sys sdwan route-tag-list.
- B. diagnose sys sdwan service.
- C. diagnose sys sdwan member.
- D. diagnose sys sdwan neighbor.

Show Suggested Answer





Actual exam question from Fortinet's NSE7_SDW-6.4

Question #: 41

Topic #: 1

[\[All NSE7_SDW-6.4 Questions\]](#)

Which two protocols in the IPsec suite are most used for authentication and encryption? (Choose two.)

- A. Internet Key Exchange (IKE)
- B. Secure Shell (SSH)
- C. Security Association (SA)
- D. Encapsulating Security Payload (ESP)

Show Suggested Answer





Actual exam question from Fortinet's NSE7_SDW-6.4

Question #: 42

Topic #: 1

[\[All NSE7_SDW-6.4 Questions\]](#)

What are two reasons for using FortiManager to organize and manage the network for a group of FortiGate devices? (Choose two.)

- A. To improve SD-WAN performance on the managed FortiGate devices
- B. To send probe packets as health checks to the beacon servers on behalf of FortiGate
- C. To simplify the deployment and administration of SD-WAN on managed FortiGate devices
- D. To reduce WAN usage on FortiGate devices by acting as a local FortiGuard server

Show Suggested Answer





Actual exam question from Fortinet's NSE7_SDW-6.4

Question #: 43

Topic #: 1

[\[All NSE7_SDW-6.4 Questions\]](#)

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

Show Suggested Answer



Actual exam question from Fortinet's NSE7_SDW-6.4

Question #: 44

Topic #: 1

[\[All NSE7_SDW-6.4 Questions\]](#)

Refer to exhibits.




Exhibit A	Exhibit B
Link Status	
Check interval	<input type="text" value="500"/> ms
Failures before inactive 	<input type="text" value="3"/>
Restore link after 	<input type="text" value="2"/> check(s)
Actions when Inactive	
Update static route 	<input checked="" type="checkbox"/>

Exhibit A	Exhibit B
<pre>NGFW-1 # diagnose sys sdwan health-check Health Check (Ping): Seq (1 port1): state (alive), packet-loss (0.000%) latency (6.196), jitter (0.079) sla_map=0x0 Seq (2 port2): state (dead), packet-loss (6.000%) sla_map=0x0</pre>	

Exhibit A, which shows the SD-WAN performance SLA and exhibit B shows the health of the participating SD-WAN members.

Based on the exhibits, which statement is correct?

- A. The dead member interface stays unavailable until an administrator manually brings the interface back.
- B. Port2 needs to wait 500 milliseconds to change the status from alive to dead.
- C. Static routes using port2 are active in the routing table.
- D. FortiGate has not received three consecutive requests from the SLA server configured for port2.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_SDW-6.4

Question #: 45

Topic #: 1

[\[All NSE7_SDW-6.4 Questions\]](#)

Refer to the exhibit.

```
FortGate # diagnose firewall shaper traffic-shaper list name VoIP_Shaper
name VoIP_Shaper
maximum-bandwidth 6250 KB/sec
guaranteed-bandwidth 2500 KB/sec
current-bandwidth 93 KB/sec
priority 2
overhead 0
tos ff
packets dropped 0
bytes dropped 0
```

Which two conclusions for traffic that matches the traffic shaper are true? (Choose two.)

- A. The traffic shaper drops packets if the bandwidth exceeds 6250 KBps.
- B. The traffic shaper limits the bandwidth of each source IP to a maximum of 6250 KBps.
- C. The traffic shaper drops packets if the bandwidth is less than 2500 KBps.
- D. The measured bandwidth is less than 100 KBps.

Show Suggested Answer



Actual exam question from Fortinet's NSE7_SDW-6.4

Question #: 46

Topic #: 1

[\[All NSE7_SDW-6.4 Questions\]](#)

Which two statements are correct when traffic matches the default implicit SD-WAN rule? (Choose two.)

- A. The `sdwan_service_id` flag in the session information is 0.
- B. Traffic has matched none of the FortiGate policy routes.
- C. Matched traffic failed RPF and was caught by the rule.
- D. An absolute SD-WAN rule was defined and matched traffic.

Show Suggested Answer



Actual exam question from Fortinet's NSE7_SDW-6.4

Question #: 47

Topic #: 1

[\[All NSE7_SDW-6.4 Questions\]](#)

Refer to the exhibit.

```
config vpn ipsec phase1-interface
  edit "FIRST_VPN"
    set type dynamic
    set interface "port1"
    set peertype any
    set proposal aes-128-sha256 aes256-sha384
    set add-route enable
    set dhgrp 14 15 19
    set xauthtype auto
    set authusrgrp "first-group"
    set psksecret fortinet1
  next
end
```

Which configuration setting is correct if the responder FortiGate is using a dynamic routing protocol over the IPsec VPN interface?

- A. add-route must be disabled to prevent FortiGate from installing static routes for remote protected networks
- B. peertype must be set to accept a unique peer ID per IPsec VPN
- C. type must be set to static
- D. Dial-up clients must have XAuth enabled

Show Suggested Answer

Actual exam question from Fortinet's NSE7_SDW-6.4

Question #: 48

Topic #: 1

[\[All NSE7_SDW-6.4 Questions\]](#)

Refer to the exhibit.

```
id=20085 trace_id=847 func=print_pkt_detail line=5428 msg= "vd-root:0 received a
packet (proto=6, 10.1.10.1:33920->74.125.195.93:443) from port3. flag [.] , seq
2018554516, ack 4141536963, win 2238"
id=20085 trace_id=847 func=resolve_ip_tuple_fast line=5508 msg= "Find an existing
session, id-000008c1, original direction"
id=20085 trace_id=847 func=shaper_handler line=821 msg= "exceeded shaper limit,
drop"
```

Which conclusion about the packet debug flow output is correct?

- A. The original traffic exceeded the maximum bandwidth of the outgoing interface, and the packet was dropped.
- B. The reply traffic exceeded the maximum bandwidth configured in the traffic shaper, and the packet was dropped.
- C. The original traffic exceeded the maximum packets per second of the outgoing interface, and the packet was dropped.
- D. The original traffic exceeded the maximum bandwidth configured in the traffic shaper, and the packet was dropped.

Show Suggested Answer



Actual exam question from Fortinet's NSE7_SDW-6.4

Question #: 49

Topic #: 1

[\[All NSE7_SDW-6.4 Questions\]](#)

Which feature enables SD-WAN to combine IPsec VPN dynamic shortcut tunnels between spokes and a static tunnel to the hub?

- A. ADVPN
- B. GRE
- C. SSLVPN
- D. OCVPN

Show Suggested Answer





Actual exam question from Fortinet's NSE7_SDW-6.4

Question #: 50

Topic #: 1

[\[All NSE7_SDW-6.4 Questions\]](#)

Which action FortiGate performs on traffic that is subject to a per-IP traffic shaper of 10 Mbps?

- A. FortiGate shares 10 Mbps of bandwidth equally among all source IP addresses.
- B. FortiGate applies traffic shaping to the original traffic direction only.
- C. FortiGate limits each source IP address to a maximum bandwidth of 10 Mbps.
- D. FortiGate guarantees a minimum of 10 Mbps of bandwidth to each source IP address.

Show Suggested Answer





Actual exam question from Fortinet's NSE7_SDW-6.4

Question #: 51

Topic #: 1

[\[All NSE7_SDW-6.4 Questions\]](#)

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

- A. SD-WAN rules that use BGP tags have precedence over regular policy routes.
- B. Routes tags are mapped to the local preference attribute.
- C. Route tags can be used to specify the destination subnets in SD-WAN rules.
- D. If the destination network learned using BGP tag changes, you must re-configure the BGP tag so the information on the SD-WAN rule is updated.

Show Suggested Answer



Actual exam question from Fortinet's NSE7_SDW-6.4

Question #: 52

Topic #: 1

[\[All NSE7_SDW-6.4 Questions\]](#)

Refer to the exhibit.

```
config system interface
  edit "port2"
    set vdom "root"
    set ip 192.168.73.132 255.255.255.0
    set allowaccess ping
    set type physical
    set snmp-index 2
    set preserve-session-route enable
  next
end
```

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.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_SDW-6.4

Question #: 53

Topic #: 1

[\[All NSE7_SDW-6.4 Questions\]](#)

Refer to exhibits.

Exhibit A
Exhibit B

Edit Policy

Name i

Incoming interface

Outgoing interface

Source + x

Destination + x

Schedule

Service + 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

Exhibit A
Exhibit B

Edit Traffic Shaping Policy

Name

Status Enabled Disabled

Comments 0/255

If Traffic Matches:

Source + x

Destination + x

Schedule

Service + x

Application i

URL Category + x

Then:

Action Apply Shaper Assign Shaping Class ID

Outgoing interface + x

Shared shaper

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

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.

Show Suggested Answer





Actual exam question from Fortinet's NSE7_SDW-6.4

Question #: 54

Topic #: 1

[\[All NSE7_SDW-6.4 Questions\]](#)

What are two reasons why it is effective to implement the internet service database (ISDB) in an SD-WAN rule? (Choose two.)

- A. The ISDB is dynamically updated and reduces administrative overhead.
- B. The ISDB applies rules to traffic from specific sources, based on application type.
- C. The ISDB requires application control to maintain signatures and perform load-balancing.
- D. The ISDB contains the IP addresses and port ranges of well-known destinations.

Show Suggested Answer

