

Fortinet.Premium.NSE7_SDW-7.0.35q - DEMO

Number: NSE7_SDW-7.0
Passing Score: 800
Time Limit: 120 min
File Version: 1.7



Exam Code: NSE7_SDW-7.0

Exam Name: Fortinet NSE 7 - SD-WAN 7.0

Website: www.VCEplus.io

Twitter: [www.twitter.com/VCE_Plus](https://twitter.com/VCE_Plus)

Exam A

QUESTION 1

Which diagnostic command can you use to show the member utilization statistics measured by performance SLAs for the last 10 minutes?

- A. diagnose sys sdwan intf-sla-log
- B. diagnose sys sdwan health-check
- C. diagnose sys sdwan log
- D. diagnose sys sdwan sla-log

Correct Answer: D

Section:

Explanation:

QUESTION 2

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

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

Correct Answer: A, C

Section:

Explanation:

QUESTION 3

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

Correct Answer: C, D

Section:

Explanation:

QUESTION 4

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 -

www.VCEplus.io

```
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.

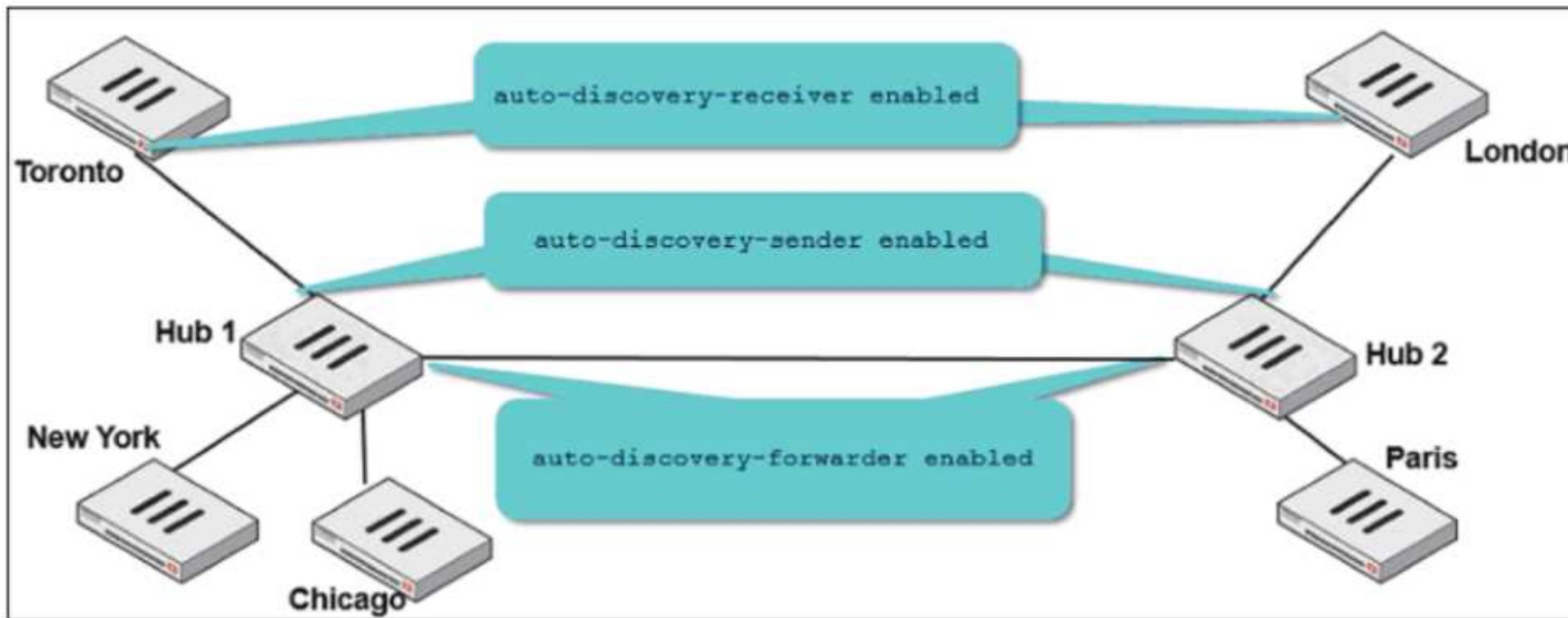
Correct Answer: C

Section:

Explanation:

QUESTION 5

Refer to the exhibit.



Two hub-and-spoke groups are connected through a site-to-site IPsec VPN between Hub 1 and Hub 2. The administrator configured ADVPN on both hub-and-spoke groups.

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

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

Correct Answer: B, D

Section:

Explanation:

QUESTION 6

Which two performance SLA protocols enable you to verify that the server response contains a specific value? (Choose two.)

- A. http
- B. icmp
- C. twamp
- D. dns

Correct Answer: A, D

Section:

Explanation:

QUESTION 7

Refer to the exhibit.

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

Correct Answer: B, C

Section:

Explanation:

QUESTION 8

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/N7mSgc7VL0BW2ZHQUXWJ6zvFxNKktiPYNtA8aP
i6ly7gDx2lP/OfKexTQQJzgCGRYzLM8eFTOnK7K6AuX0bFDCpBBhEIdf+03CYBMLwkFZmdU6RsT+qvyybblVX+Ioy
HK5EXakpmz5RiltELg29Gg==
  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.

Correct Answer: D

Section:

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 SDWAN_ 7.2_Study_Guide

page 236

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

Correct Answer: B

Section:

Explanation:

QUESTION 10

Refer to the exhibit.

www.VCEplus.io

































+ Create New ▾								✎ Edit	🗑 Delete	🔍 Where Used	🔗 Collapse All	⚙ Column Settings ▾	⋮ More ▾		🔍			
<input type="checkbox"/>	#	Name	Type	Normalized Interface	Addressing Mode	IP/Netmask	Access											
<input type="checkbox"/>	▼ Physical (10)																	
<input type="checkbox"/>	1	port1	 Physical	 port1	Manual	203.0.113.1/255.255.255.2	PING											
<input type="checkbox"/>	2	port2	 Physical	 port2	Manual	203.0.113.9/255.255.255.2	PING											
<input type="checkbox"/>	3	port3	 Physical	 port3	Manual	0.0.0.0/0.0.0.0												
<input type="checkbox"/>	4	port4	 Physical	 port4	Manual	172.16.0.9/255.255.255.24	PING											
<input type="checkbox"/>	5	port5	 Physical	 port5	Manual	10.0.2.254/255.255.255.0	PING											
<input type="checkbox"/>	6	port6	 Physical	 port6	Manual	0.0.0.0/0.0.0.0												
<input type="checkbox"/>	7	port7	 Physical	 port7	Manual	0.0.0.0/0.0.0.0												
<input type="checkbox"/>	8	port8	 Physical	 port8	Manual	0.0.0.0/0.0.0.0												
<input type="checkbox"/>	9	port9	 Physical	 port9	Manual	0.0.0.0/0.0.0.0												
<input type="checkbox"/>	10	port10	 Physical	 port10	Manual	192.168.0.32/255.255.255.	HTTPS, PING, SSH, HT											
<input type="checkbox"/>	▼ Aggregate (1)																	
<input type="checkbox"/>	11	fortilink	 Aggregate		Manual	169.254.1.1/255.255.255.0	PING, Security Fabric C											
<input type="checkbox"/>	▼ Tunnel (3)																	
<input type="checkbox"/>	12	naf.root	 Tunnel		Manual	0.0.0.0/0.0.0.0												
<input type="checkbox"/>	13	l2t.root	 Tunnel		Manual	0.0.0.0/0.0.0.0												
<input type="checkbox"/>	14	ssl.root (SSL VPN interf	 Tunnel		Manual	0.0.0.0/0.0.0.0												
<input type="checkbox"/>	▼ EMAC VLAN (1)																	
<input type="checkbox"/>	15	vl_lan_ts	 EMAC VLAN		Manual	10.0.102.1/255.255.255.0	PING											
<input type="checkbox"/>	▼ SD-WAN Zone (2)																	
<input type="checkbox"/>	16	virtual-wan-link	 SD-WAN Zone															
<input type="checkbox"/>	17	SASE	 SD-WAN Zone	 SASE														
+ Create New ▾																✎ Edit	🗑 Delete	⚙ Column Settings ▾
<input type="checkbox"/>	#	ID	Destination	Gateway	Interface	Distance	Priority	Status	Description									
<input type="checkbox"/>	▼ Static Route (2)																	
<input type="checkbox"/>	1	1	0.0.0.0/0.0.0.0	203.0.113.2	 port1	10	0	 Enable										
<input type="checkbox"/>	2	2	0.0.0.0/0.0.0.0	203.0.113.10	 port2	10	0	 Enable										

Exhibit B –

+ Create New Edit Delete Section Policy Lookup Collapse All Column Settings View Mode								
<input type="checkbox"/>	#	Name	From	To	Source	Destination	Schedule	Service
<input type="checkbox"/>	1	Internet_Access	<input checked="" type="checkbox"/> port5	<input checked="" type="checkbox"/> port1	<input checked="" type="checkbox"/> all	<input checked="" type="checkbox"/> all	<input checked="" type="checkbox"/> always	<input checked="" type="checkbox"/> ALL
<input type="checkbox"/>	▼ Implicit (2-2 / Total: 1)							
<input type="checkbox"/>	2	Implicit Deny	<input checked="" type="checkbox"/> any	<input checked="" type="checkbox"/> any	<input checked="" type="checkbox"/> all <input checked="" type="checkbox"/> all	<input checked="" type="checkbox"/> all <input checked="" type="checkbox"/> all	<input checked="" type="checkbox"/> always	<input checked="" type="checkbox"/> 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.

Correct Answer: B
Section:
Explanation:

QUESTION 11
Which two statements are correct when traffic matches the implicit SD-WAN rule? (Choose two.)

A. The sdwan_service_id flag in the session information is 0.
B. All SD-WAN rules have the default setting enabled.
C. Traffic does not match any of the entries in the policy route table.
D. Traffic is load balanced using the algorithm set for the v4-ecmp-mode setting.

Correct Answer: A, C
Section:
Explanation:

QUESTION 12
Refer to the exhibit.

www.VCEplus.io

```
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.

Correct Answer: A, C

Section:

Explanation:

QUESTION 13

Refer to the exhibit.

```
config system settings
  set firewall-session-dirty check-new
end
```

Based on the exhibit, which two actions does FortiGate perform on sessions after a firewall policy change? (Choose two.)

- A. FortiGate flushes all sessions.
- B. FortiGate terminates the old sessions.
- C. FortiGate does not change existing sessions.

D. FortiGate evaluates new sessions.

Correct Answer: C, D

Section:

Explanation:

FortiGate not to flag existing impacted session as dirty by setting firewall-session-dirty to check new.
The results is that FortiGate evaluates only new session against the new firewall policy.

QUESTION 14

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.

Correct Answer: A, C

Section:

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/newsd-wan-template-fmg>

QUESTION 15

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.

Correct Answer: C

Section:

Explanation:

QUESTION 16

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.

Correct Answer: A, D

Section:

Explanation:

QUESTION 17

What is the route-tag setting in an SD-WAN rule used for?

- A. To indicate the routes for health check probes.
- B. To indicate the destination of a rule based on learned BGP prefixes.
- C. To indicate the routes that can be used for routing SD-WAN traffic.
- D. To indicate the members that can be used to route SD-WAN traffic.

Correct Answer: B

Section:

Explanation:

QUESTION 18

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), health-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.

Correct Answer: D

Section:

Explanation:

QUESTION 19

Refer to the exhibits.

Exhibit A -

www.VCEplus.io

Edit Traffic Shaping Policy

IP Version: IPv4 IPv6

Name:

Status: Enable Disable

Comments:
0/255

If Traffic Matches:

Source Internet Service: ☐

Source Address:

Source User:

Source User Group:

Destination Internet Service: ☐

Destination Address:

Schedule:

Service:

Application:

Application Category:

Application Group:

URL Category:

Type Of Service:

Type Of Service Mask:

Then:

Action: Apply Shaper Assign Group

Outgoing Interface:

Shared Shaper:

Reverse Shaper:

Per-IP Shaper:

Differentiated Services: ☐

Differentiated Services Reverse: ☐

www.VCEplus.io

Exhibit B -

Edit Firewall Policy

ID	1
Name	DIA
ZTNA	<div>Disable</div> <div>Full ZTNA</div> <div>IP/MAC filtering</div>
Incoming Interface	LAN
Outgoing Interface	underlay
Source Internet Service	<input type="checkbox"/>
IPv4 Source Address	LAN-net
IPv6 Source Address	+
Source User	+
Source User Group	+
FSSO Groups	+
Destination Internet Service	<input type="checkbox"/>
IPv4 Destination Address	all
IPv6 Destination Address	+
Service	ALL
Schedule	always
Action	<div>Deny</div> <div>Accept</div> <div>IPSEC</div>
Inspection Mode	<div>Flow-based</div> <div>Proxy-based</div>
Firewall/Network Options	
NAT	<input checked="" type="checkbox"/> <div>NAT</div> <div>NAT46</div> <div>NAT64</div>
IP Pool Configuration	<div>Use Outgoing Interface Address</div> <div>Use Dynamic IP Pool</div>
Preserve Source Port	<input type="checkbox"/>
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.

Correct Answer: B

Section:

Explanation:

QUESTION 20

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
6D5rVsaKlMeAyVYtlz95BS24Psew761wY023hnFVviwb6deItSc5ltCa+iNYhujT8gycfD4+WuszpmuIv8rRzrVh
7DFkHaW2auAAprQ0dHUfaCzjOhME7mPw+8he2xB7Edb9ku/nZEHb0cKLkKYJc/p9J9IMweV2lZUgFjvIpXNxHxpH
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.

Correct Answer: B

Section:

Explanation:

QUESTION 21

Refer to the exhibits.

Exhibit A -

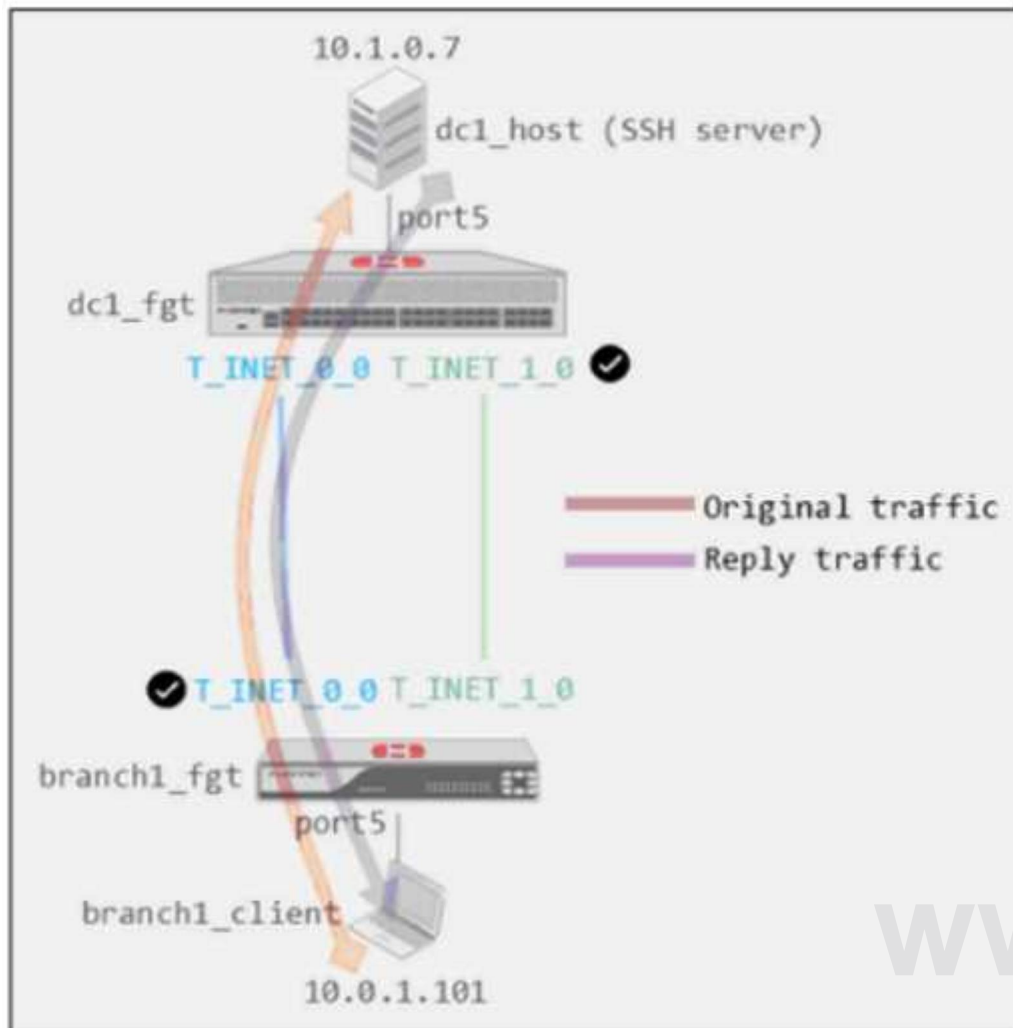


Exhibit B -

```
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 t?p-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.

Correct Answer: A

Section:

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/administrationguide/14295/controlling-return-path-with-auxiliary-session>

QUESTION 22

Refer to the exhibits.

Exhibit A -

www.VCEplus.io

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	<input type="text" value="4.2.2.1"/> <input type="text" value="4.2.2.2"/>		
Participants	All SD-WAN Members Specify <input type="text" value=""/> <div> <div>port1</div> <div>port2</div> </div> 2 Entries		
Enable Probe Packets	<input checked="" type="checkbox"/>		
SLA Targets 	<div>+ Add Target</div>		
Link Status			
Interval	500		Milliseconds
Failure Before Inactive	3		(max 3600)
Restore Link After	2		(max 3600)
Action When Inactive			
Update Static Route	<input checked="" type="checkbox"/>		
Cascade Interfaces	<input checked="" type="checkbox"/>		

Exhibit B -

www.VCEplus.io


```
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.

Correct Answer: B

Section:

Explanation:

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

QUESTION 23

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

Correct Answer: A

Section:

Explanation:

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

QUESTION 24

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.

Correct Answer: A

Section:

Explanation:

QUESTION 25

Which are three key routing principles in SD-WAN? (Choose three.)

- A. FortiGate performs route lookups for new sessions only.
- B. Regular policy routes have precedence over SD-WAN rules.
- C. SD-WAN rules have precedence over ISDB routes.
- D. By default, SD-WAN members are skipped if they do not have a valid route to the destination.
- E. By default, SD-WAN rules are skipped if the best route to the destination is not an SD-WAN member.

Correct Answer: B, D, E

Section:

Explanation:

QUESTION 26

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.

Correct Answer: C, D

Section:

Explanation:

QUESTION 27

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.

Correct Answer: A, B

Section:

Explanation:

QUESTION 28

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.

Correct Answer: C

Section:

Explanation:

QUESTION 29

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.

Correct Answer: A, B

Section:

Explanation:

QUESTION 30

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.

Correct Answer: A, C

Section:

Explanation:

QUESTION 31

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.

Correct Answer: B, C

Section:

Explanation:

QUESTION 32

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=00000a2c tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id= 80000000 rpdb_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.

Correct Answer: C

Section:

Explanation:

QUESTION 33

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.

Correct Answer: A, E

Section:

Explanation:

QUESTION 34

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.

Correct Answer: A, C

Section:

Explanation:

QUESTION 35

Refer to the exhibit.

```
config vpn ipsec phase1-interface
edit "FIRST_VPN"
set type dynamic
set interface "port1"
set peertype any
set proposal aes128-sha256 aes256-sha38
set dhgrp 14 15 19
set xauthtype auto
set authusrgrp "first-group"
set psksecret fortinet1
next
edit "SECOND_VPN"
set type dynamic
set interface "port1"
set peertype any
set proposal aes128-sha256 aes256-sha38
set dhgrp 14 15 19
set xauthtype auto
set authusrgrp "second-group"
set psksecret fortinet2
next
edit
```

FortiGate has multiple dial-up VPN interfaces incoming on port1 that match only FIRST_VPN.

Which two configuration changes must be made to both IPsec VPN interfaces to allow incoming connections to match all possible IPsec dial-up interfaces? (Choose two.)

- A. Specify a unique peer ID for each dial-up VPN interface.
- B. Use different proposals are used between the interfaces.
- C. Configure the IKE mode to be aggressive mode.
- D. Use unique Diffie Hellman groups on each VPN interface.

Correct Answer: A, C

Section:

Explanation:

www.VCEplus.io