



Vendor: Fortinet

Exam Code: NSE7_SDW-7.2

Exam Name: Fortinet NSE 7 - SD-WAN 7.2

Version: 23.111

QUESTION 1

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

Explanation:

CLI templates are useful for pushing advanced CLI settings that reference meta fields.

QUESTION 2

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.

Answer: B

QUESTION 3

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.

Answer: D

Explanation:

link-cost-threshold is set to 10 (percent) so the other link must have a latency of less than 90% of the preferred link.

QUESTION 4

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		Disclaimer Options	
ID	1	Display Disclaimer	<input type="checkbox"/>
Name	DIA	Security Profiles	<input type="checkbox"/>
ZTNA	<input checked="" type="radio"/> Disable <input type="radio"/> Full ZTNA <input type="radio"/> IP/MAC filtering	SSL/SSH Inspection	<input checked="" type="radio"/> deep-inspection
Incoming Interface	<input checked="" type="radio"/> LAN	Decrypted Traffic Mirror	<input type="text" value="+"/>
Outgoing Interface	<input checked="" type="radio"/> underlay	Traffic Shaping Options	
Source Internet Service	<input type="checkbox"/>	Shared Shaper	<input type="text" value="+"/>
IPv4 Source Address	<input checked="" type="radio"/> LAN-net	Reverse Shaper	<input type="text" value="+"/>
IPv6 Source Address	<input type="text" value="+"/>	Per-IP Shaper	<input type="text" value="+"/>
Source User	<input type="text" value="+"/>	Logging Options	
Source User Group	<input type="text" value="+"/>	Log Allowed Traffic	<input checked="" type="radio"/> No Log <input type="radio"/> Log Security Events <input checked="" type="radio"/> Log All Sessions
FSSO Groups	<input type="text" value="+"/>	<input type="checkbox"/> Capture Packets	
Destination Internet Service	<input type="checkbox"/>	<input type="checkbox"/> Generate Logs when Session Starts	
IPv4 Destination Address	<input checked="" type="radio"/> all		
IPv6 Destination Address	<input type="text" value="+"/>		
Service	<input checked="" type="radio"/> ALL		
Schedule	<input checked="" type="radio"/> always		
Action	<input type="radio"/> Deny <input checked="" type="radio"/> Accept <input type="radio"/> IPSEC		
Inspection Mode	<input checked="" type="radio"/> Flow-based <input type="radio"/> Proxy-based		
Firewall/Network Options			
NAT	<input checked="" type="checkbox"/> NAT <input type="checkbox"/> NAT46 <input type="checkbox"/> NAT64		
IP Pool Configuration	<input checked="" type="radio"/> Use Outgoing Interface Address <input type="radio"/> Use Dynamic IP Pool		
Preserve Source Port	<input type="checkbox"/>		
Protocol Options	<input checked="" type="radio"/> default		

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

- A. Destination internet service must be enabled on the traffic shaping policy.
- B. Application control must be enabled on the firewall policy.
- C. Web filtering must be enabled on the firewall policy.
- D. Individual SD-WAN members must be selected as the outgoing interface on the traffic shaping policy.

Answer: B

QUESTION 5

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+WuszpmuIv8rRzrVh
7DFkHaW2auAAprQ0dHUfaCzjOhME7mPw+8he2xB7Edb9ku/nZEHb0cKLkKYJc/p9J9IMweV21ZUgFjvIpXNxHxpH
LReOFShoH01SPFKz5IYCVA==
    next
  end
```

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

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

Answer: B

Explanation:

For SPOKE you need to configure "net-device Enable" and "auto-discovery-sender Enable".

QUESTION 6

Refer to the exhibits.

Exhibit A

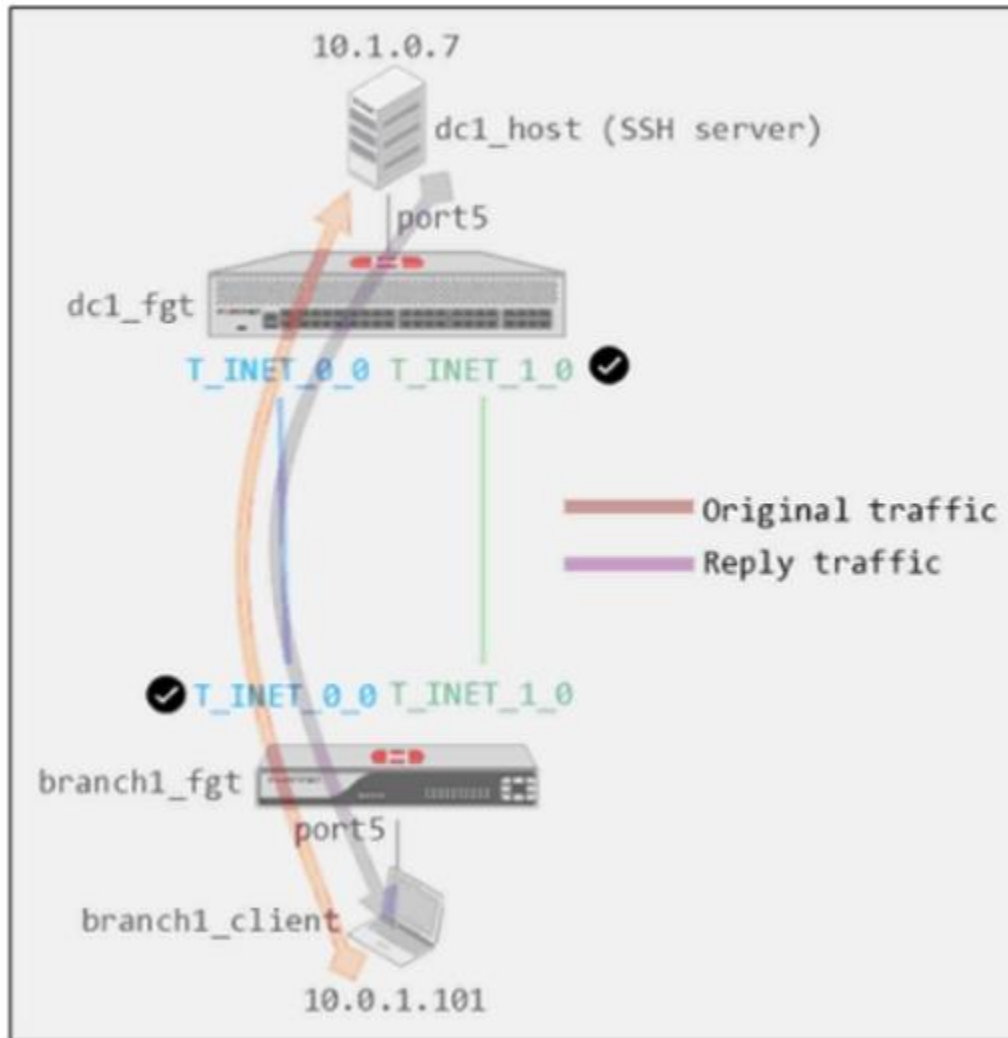


Exhibit B

```
dc1_fgt # show system global
config system global
    set admin-https-redirect disable
    set admintimeout 480
    set alias "FortiGate-VM64"
    set hostname "dc1_fgt"
    set timezone 04
end

dc1_fgt # show system settings
config system settings
    set tcp-session-without-syn enable
    set allow-subnet-overlap enable
    set gui-allow-unnamed-policy enable
    set gui-multiple-interface-policy enable
end
```

Exhibit A shows a site-to-site topology between two FortiGate devices: branch1_fgt and dc1_fgt. Exhibit B shows the system global and system settings configuration on dc1_fgt. When branch1_client establishes a connection to dc1_host, the administrator observes that, on dc1_fgt, the reply traffic is routed over T_INET_0_0, even though T_INET_1_0 is the preferred member in the matching SD-WAN rule.

Based on the information shown in the exhibits, what configuration change must be made on dc1_fgt so dc1_fgt routes the reply traffic over T_INET_1_0?

- A. Enable auxiliary-session under config system settings.
- B. Disable tp-session-without-syn under config system settings.
- C. Enable snat-route-change under config system global.
- D. Disable allow-subnet-overlap under config system settings.

Answer: A

Explanation:

Controlling return path with auxiliary session When multiple incoming or outgoing interfaces are used in ECMP or for load balancing, changes to routing, incoming, or return traffic interfaces impacts how an existing sessions handles the traffic. Auxiliary sessions can be used to handle these changes to traffic patterns.

QUESTION 7

Refer to the exhibits.

Exhibit A

Edit Performance SLA

Name	Level3_DNS	
IP Version	IPv4	IPv6
Probe Mode	Active	Passive Prefer Passive
Protocol	Ping	TCP ECHO UDP ECHO HTTP TW
Server	<input type="text" value="4.2.2.1"/> <input type="text" value="4.2.2.2"/>	
Participants	All SD-WAN Members Specify <div> <input type="text" value=""/> <div> <div>port1</div> <div>port2</div> </div> </div> 2 Entries	
Enable Probe Packets	<input checked="" type="checkbox"/>	
SLA Targets ⓘ	+ Add Target	
Link Status		
Interval	<input type="text" value="500"/>	Milliseconds
Failure Before Inactive	<input type="text" value="3"/>	(max 3600)
Restore Link After	<input type="text" value="2"/>	(max 3600)
Action When Inactive		
Update Static Route	<input checked="" type="checkbox"/>	
Cascade Interfaces	<input checked="" type="checkbox"/>	

Exhibit B


```
branch1_fgt # diagnose sys sdwan member | grep port
Member(1): interface: port1, flags=0x0 , gateway: 192.2.0.2, priority: 0 1024, weight: 0
Member(2): interface: port2, flags=0x0 , gateway: 192.2.0.10, priority: 0 1024, weight: 0

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

branch1_fgt # diagnose sys sdwan health-check status Level3_DNS
Health Check(Level3 DNS):
Seq(1 port1): state(alive), packet-loss(0.000%) latency(1.919), jitter(0.137), bandwidth-
up(10238), bandwidth-dw(10238), bandwidth-bi(20476) sla_map=0x0
Seq(2 port2): state(alive), packet-loss(0.000%) latency(1.509), jitter(0.101), bandwidth-
up(10238), bandwidth-dw(10238), bandwidth-bi(20476) sla_map=0x0
```

Exhibit A shows the SD-WAN performance SLA and exhibit B shows the SD-WAN member status, the routing table, and the performance SLA status.

If port2 is detected dead by FortiGate, what is the expected behavior?

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

Answer: B

Explanation:

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

QUESTION 8

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

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

Answer: A

Explanation:

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

QUESTION 9

Refer to the exhibit.

```
config system sdwan
  set status enable
  set load-balance source-dest-ip-based
  config zone
    edit "virtual-wan-link"
    next
    edit "SASE"
    next
    edit "underlay"
    next
  end
  config members
    edit 1
      set interface "port1"
      set zone "underlay"
      set gateway 192.2.0.2
    next
    edit 2
      set interface "port2"
      set zone "underlay"
      set gateway 192.2.0.10
    next
  end
  ...
end
```

Which algorithm does SD-WAN use to distribute traffic that does not match any of the SD-WAN rules?

- A. All traffic from a source IP to a destination IP is sent to the same interface.
- B. All traffic from a source IP is sent to the same interface.
- C. All traffic from a source IP is sent to the most used interface.
- D. All traffic from a source IP to a destination IP is sent to the least used interface.

Answer: A

Explanation:

By default when no sd-wan rule is matched, uses a source-IP load balancing algorithm, BUT from the exhibit the has been changed to Source-Destination IP.

QUESTION 10

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.

Answer: BDE

QUESTION 11

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

- A. It simplifies the deployment and administration of SD-WAN on managed FortiGate devices.
- B. It improves SD-WAN performance on the managed FortiGate devices.
- C. It sends probe signals as health checks to the beacon servers on behalf of FortiGate.
- D. It acts as a policy compliance entity to review all managed FortiGate devices.
- E. It reduces WAN usage on FortiGate devices by acting as a local FortiGuard server.

Answer: AE

QUESTION 12

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.

Answer: AC

QUESTION 13

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.

Answer: AC

QUESTION 14

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

```
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.Portal(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
```

- 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.

Answer: BC

QUESTION 15

Which two tasks about using central VPN management are true? (Choose two.)

- A. You can configure full mesh, star, and dial-up VPN topologies.
- B. FortiManager installs VPN settings on both managed and external gateways.
- C. You configure VPN communities to define common IPsec settings shared by all VPN gateways.
- D. You must enable VPN zones for SD-WAN deployments.

Answer: AC

QUESTION 16

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.

Answer: B

QUESTION 17

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

Answer: A

QUESTION 18

Refer to exhibits. 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?

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
+

URL Category
+
x

Then:

Action
☒ Apply Shaper
☐ Assign Shaping Class ID

Outgoing interface
+
x

Shared shaper
☒

- 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

QUESTION 19

Based on the exhibit, which status description is correct?

```
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 sdwan 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), health-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
```

- A. Port1 is dead because it does not meet the SLA target.
- B. Port2 is alive because its packet loss is lower than 10%.
- C. The SD-WAN members are monitored by different performance SLAs.
- D. Traffic matching the SD-WAN rule is steered through port2.

Answer: D

QUESTION 20

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

- A. Learned routes can be used as dynamic destinations in SD-WAN rules.
- B. You must use BGP to route traffic for both overlay and underlay links.
- C. You must configure AS path prepending.
- D. You must use external BGP.

Answer: A

QUESTION 21

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

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

Answer: BD

QUESTION 22

Which statement is correct about SD-WAN and ADVPN?

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

Answer: B

QUESTION 23

Refer to the exhibit. Which two statements about the IPsec VPN configuration and the status of the IPsec VPN tunnel are true? (Choose two.)

```
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
```

- A. FortiGate creates separate virtual interfaces for each dial-up client.
- B. FortiGate creates a single IPsec virtual interface that is shared by all clients.
- C. FortiGate maps the remote gateway 100.64.3.1 to tunnel index interface 1.
- D. FortiGate does not install IPsec static routes for remote protected networks in the routing table.

Answer: BC

Explanation:

If net-device is disabled, FortiGate creates a single IPSEC virtual interface that is shared by all IPSEC clients connecting to the same dialup VPN. In this case, the tunnel-search setting determines how FortiGate learns the network behind each remote client.

QUESTION 24

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

Answer: A

Explanation:

The diagnose sys sdwan sla-log command shows the member utilization statistics measured by performance SLAs for the last 10 minutes.

Option A, diagnose sys sdwan intf-sla-log, shows the interface utilization statistics measured by performance SLAs for the last 10 minutes.

Option B, diagnose sys sdwan health-check, shows the health check statistics for all interfaces.

Option C, diagnose sys sdwan log, shows all SD-WAN logs.

QUESTION 25

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)

Answer: AC

Explanation:

ESP is used for encryption, while IKE is used for authentication and key exchange. SSH is not a part of the IPsec suite, and SA is a term used to refer to a security association, which is a set of parameters that define how two peers will communicate securely.

QUESTION 26

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

Explanation:

The holdtime-timer is the amount of time that a BGP router will wait for a BGP update from a neighbor before declaring the neighbor down. The link-down-failover setting tells BGP to immediately withdraw routes from a neighbor if the link to the neighbor goes down.

The update-source and set-route-tag settings do not affect routing convergence.

QUESTION 27

Refer to the exhibits.

Exhibit A

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

Exhibit B

```
branch1_fgt # diagnose sys sdwan service 3

Service(3): Address Mode(IPV4) flags=0x200 use-shortcut-sla
  Gen(1), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(sla), sla-compare-order
  Members(2):
    1: Seq_num(5 T_MPLS_0), alive, sla(0x3), gid(0), cfg_order(2), cost(0), selected
    2: Seq_num(4 T_INET_1_0), alive, sla(0x1), gid(0), cfg_order(1), cost(0), selected
    3: Seq_num(3 T_INET_0_0), alive, sla(0x0), gid(0), cfg_order(0), cost(0), selected
  Src address(1):
    10.0.1.0-10.0.1.255

  Dst address(1):
    10.0.0.0-10.255.255.255

branch1_fgt # get router info routing-table all | grep T_
S      10.0.0.0/8 [1/0] via T_INET_0_0 tunnel 100.64.1.1
        [1/0] via T_INET_1_0 tunnel 100.64.1.9
S      10.201.1.254/32 [15/0] via T_INET_0_0 tunnel 100.64.1.1
S      10.202.1.254/32 [15/0] via T_INET_1_0 tunnel 100.64.1.9
S      10.203.1.254/32 [15/0] via T_MPLS_0 tunnel 172.16.1.5

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

Exhibit A shows the configuration for an SD-WAN rule and exhibit B shows the respective rule status, the routing table, and the member status.

The administrator wants to understand the expected behavior for traffic matching the SD-WAN rule. Based on the exhibits, what can the administrator expect for traffic matching the SD-WAN rule?

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

Answer: D

Explanation:

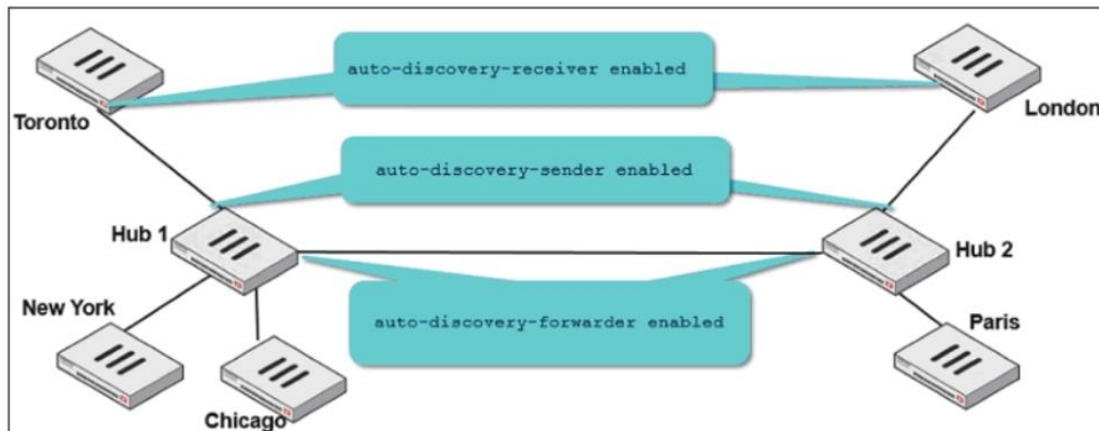
MPLS doesn't have a valid route for destination AND set gateway enable without also set default enable will not allow packets to flow to this member without a valid route.

INET_1 has route and meets one sla target (0x1).

INET_0 has route but doesn't meet sla targets (0x0)

QUESTION 28

Refer to the exhibit.



Two hub-and-spoke groups are connected through a site-to-site IPsec VPN between Hub 1 and Hub 2

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.

Answer: BD

QUESTION 29

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

Answer: AD

QUESTION 30

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.

Answer: BC

QUESTION 31

Refer to the exhibit.

```
# get router info routing-table all
...
B      10.0.2.0/24 [200/0] via 10.201.1.2 [3] (recursive via VPN0 tunnel 100.64.1.1), 00:00:54
          [200/0] via 10.202.1.2 [3] (recursive via VPN1 tunnel 100.64.1.9), 00:00:54
          [200/0] via 10.203.1.1 [3] (recursive via VPN2 tunnel 172.16.1.5), 00:00:54
...
```

The device exchanges routes using IBGP.

Which two statements are correct about the IBGP configuration and routing information on the device? (Choose two.)

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

Answer: CD

Explanation:

C - the [3] means that additional-path is enabled makes the duplicate routes are consolidated in the routing table

D - get router info routing table database - shows duplicate routes without the [3]

QUESTION 32

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

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

Answer: AB

QUESTION 33

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

Explanation:

These are the components that make up the secure SD-WAN solution from Fortinet.

- FortiGate is the physical or virtual security appliance that provides the core security functionality for the SD-WAN solution.
- FortiManager is the central management platform for the SD-WAN solution. It provides centralized configuration, provisioning, and monitoring of FortiGate appliances.
- FortiAnalyzer is the centralized security analytics platform for the SD-WAN solution. It collects and analyzes security logs from FortiGate appliances to provide visibility into security threats and incidents.
- FortiDeploy is the provisioning and orchestration tool for the SD-WAN solution. It automates the deployment and configuration of FortiGate appliances.

QUESTION 34

Refer to the exhibit.

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

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

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

Answer: AB

QUESTION 35

What are two reasons why FortiGate would be unable to complete the zero-touch provisioning process? (Choose two.)

- A. The FortiGate cloud key has not been added to the FortiGate cloud portal.
- B. FortiDeploy has connected with FortiGate and provided the initial configuration to contact FortiManager
- C. The zero-touch provisioning process has completed internally, behind FortiGate.
- D. FortiGate has obtained a configuration from the platform template in FortiGate cloud.
- E. A factory reset performed on FortiGate.

Answer: AC

QUESTION 36

Which two statements describe how IPsec phase 1 main mode is different from aggressive mode when performing IKE negotiation? (Choose two)

- A. A peer ID is included in the first packet from the initiator, along with suggested security policies.
- B. XAuth is enabled as an additional level of authentication, which requires a username and password.
- C. A total of six packets are exchanged between an initiator and a responder instead of three packets.
- D. The use of Diffie Hellman keys is limited by the responder and needs initiator acceptance.

Answer: BC

QUESTION 37

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 gwy=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. FortiGate has terminated the session after a change on policy ID 1.
- C. Changes have been made on firewall policy ID 1 on FortiGate.
- D. Firewall policy ID 1 has source NAT disabled.

Answer: C

QUESTION 38

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+qvybblVX+Ioy
HK5EXakpmz5RiltELgZ9Gg==
next
end
```

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

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

Answer: D

Explanation:

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

QUESTION 39

Which CLI command do you use to perform real-time troubleshooting for ADVPN negotiation?

- A. get router info routing-table all
- B. diagnose debug application ike
- C. diagnose vpn tunnel list
- D. get ipsec tunnel list

Answer: B





























Explanation:

The diagnose debug application ike command displays real-time debugging information for the IKE protocol. This information can be used to troubleshoot ADVPN negotiation problems.

QUESTION 40

Refer to the exhibit.

Exhibit A

+ 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	port5	port1	all	all	always	ALL
<input type="checkbox"/>	▼ Implicit (2-2 / Total: 1)							
<input type="checkbox"/>	2	Implicit Deny	any	any	all	all	always	ALL

Exhibit A shows the system interface with the static routes and exhibit B shows the firewall policies on the managed FortiGate.

Based on the FortiGate configuration shown in the exhibits, what issue might you encounter when creating an SD-WAN zone for port1 and port2?

- A. port1 is assigned a manual IP address.
- B. port1 is referenced in a firewall policy.
- C. port2 is referenced in a static route.
- D. port1 and port2 are not administratively down.

Answer: B

QUESTION 41

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.

Answer: AC

Explanation:

sdwan_service_id is 0 = match SD-WAN implicit rule

SD-WAN rules internally are interpreted as a Policy route, so when the traffic doesn't match with any policy route, it will be flowing by implicit policy.

QUESTION 42

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

QUESTION 43

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.

Answer: CD

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 44

Which two statements about SD-WAN central management are true? (Choose two.)

- A. The objects are saved in the ADOM common object database.
- B. It does not support meta fields.
- C. It uses templates to configure SD-WAN on managed devices.
- D. It supports normalized interfaces for SD-WAN member configuration.

Answer: AC

Explanation:

Normalized interfaces are not supported for SD-WAN templates. You can create multiple SD-WAN zones and add interface members to the SD-WAN zones. You must bind the interface members by name to physical interfaces or VPN interfaces.

QUESTION 45

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.

QUESTION 46

Refer to the exhibits. Which two statements about the IPsec VPN configuration and the status of the IPsec VPN tunnel are true? (Choose two.)

```
dcl_fgt # show vpn ipsec phase1-interface T_INET_1_0
config vpn ipsec phase1-interface
  edit "T_INET_1_0"
    set type dynamic
    set interface "port2"
    set ike-version 2
    set keylife 28800
    set peertype any
    set net-device disable
    set proposal aes128-sha256
    set add-route disable
    set psksecret ENC
GayzHJ/UhxCc9FYtwas5o4rkNCmjJNUEj4Q4fZNS6I65RIVF9zum6sJALsU9Cg+1jsXz3ZtIM+WNkHLSXkHqydgS
G/Zx8Vp9Rcht6zKHPEctOcFVbaG+UeO3Rw4lpmGP/Z3rIz3tdXJxfYSzKjRqggqahsmDovkrKRHTVFU1zA07Zt6W
iPL9co/Zf3cX+Qpnm38MQ==
  next
end
```

```
dcl_fgt # diagnose vpn tunnel list name T_INET_1_0_0
list ipsec tunnel by names in vd 0
-----
name=T_INET_1_0_0 ver=2 serial=7 100.64.1.9:0->192.2.0.9:0 tun_id=192.2.0.9 dst_mtu=0
dpd-link=on weight=1
bound_if=4 lgwy=static/1 tun=tunnel/255 mode=dial_inst/3 encap=none/8832
options[2280]=rgwy-chg frag-rfc run_state=0 accept_traffic=1 overlay_id=0
parent=T_INET_1_0 index=0
proxyid_num=1 child_num=0 refcnt=6 ilast=17 olast=23464 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=1
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=T_INET_1_0_0 proto=0 sa=1 ref=2 serial=1 add-route
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:10.0.1.0-10.0.1.255:0
  SA: ref=3 options=20683 type=00 soft=0 mtu=1280 expire=972/0B replaywin=2048
    seqno=1 esn=0 replaywin_lastseq=00000000 itn=0 qat=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=1790/1800
  dec: spi=02f9844e esp=aes key=16 7fb5011247248d3a45ac3d802d8c8d64
    ah=sha1 key=20 bb217ce87ae060f27823b005005233811993a303
  enc: spi=ffc6576a esp=aes key=16 825bddbc5c995feb70411a773867c2d0
    ah=sha1 key=20 02db4176f7f21fae7d141526099a707f639893f1
  dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
```

- A. FortiGate does not install IPsec static routes for remote protected networks in the routing table.
- B. The phase 1 configuration supports the network-overlay setting.
- C. FortiGate facilitated the negotiation of the T_INET_1_0_0 ADVPN shortcut over T_INET_1_0.
- D. Dead peer detection is disabled.

Answer: AB

QUESTION 47

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: AD

QUESTION 48

Refer to the exhibits.

Exhibit A

```
config system sdwan
  config health-check
    edit "Passive"
      set detect-mode passive
      set members 3 4
    next
  end
end

config system sdwan
  config service
    edit 1
      set name "Facebook-YouTube"
      set src "all"
      set internet-service enable
      set internet-service-app-ctrl 15832 31077
      set health-check "Passive"
      set priority-member 3 4
      set passive-measurement enable
    next
  end
end

branch1_fgt # get application name status | grep "id: 15832" -B1
app-name: "Facebook"
id: 15832

branch1_fgt # get application name status | grep "id: 31077" -B1
app-name: "YouTube"
id: 31077
```

Exhibit B


```
config firewall policy
  edit 1
    set name "DIA"
    set uuid b973e4ec-5f90-51ec-cadb-017c830d9418
    set srcintf "port5"
    set dstintf "underlay"
    set action accept
    set srcaddr "LAN-net"
    set dstaddr "all"
    set schedule "always"
    set service "ALL"
    set passive-wan-health-measurement enable
    set utm-status enable
    set ssl-ssh-profile "certificate-inspection"
    set application-list "default"
    set logtraffic all
    set auto-asic-offload disable
    set nat enable
  next
end

branch1_fgt # diagnose sys sdwan zone | grep underlay -A1
Zone underlay index=3
  members(2): 3(port1) 4(port2)
```

Exhibit A shows the SD-WAN performance SLA configuration, the SD-WAN rule configuration, and the application IDs of Facebook and YouTube. Exhibit B shows the firewall policy configuration and the underlay zone status.

Based on the exhibits, which two statements are correct about the health and performance of port1 and port2? (Choose two.)

- A. The performance is an average of the metrics measured for Facebook and YouTube traffic passing through the member.
- B. FortiGate is unable to measure jitter and packet loss on Facebook and YouTube traffic.
- C. FortiGate identifies the member as dead when there is no Facebook and YouTube traffic passing through the member.
- D. Non-TCP Facebook and YouTube traffic are not used for performance measurement.

Answer: AD

QUESTION 49

Refer to the exhibits.

Exhibit A

Network Properties	
Service	Critical-DIA
Identity	
Device ID	FGVM01TM22000077
Device Name	branch1_fgt
Type	
Sub Type	sdwan
Type	event
Alerts	
Level	notice
General	
Log Description	SDWAN status
Log ID	0113022923
Message	Service prioritized by performance metric will be redirected in sequence order.
Sequence Number	2,1
Virtual Domain	root
Others	
Date/Time	23:57:29
Destination End User ID	3
Destination Endpoint ID	3
Device Time	2022-03-04 14:57:27
Event Time	1646434647595788893
Event Type	Service
Metric	latency
Service ID	1
Time Stamp	2022-03-04 23:57:29
Time Zone	-0800
UEBA Endpoint ID	3
UEBA User ID	3
logver	700030237

Exhibit B

branch1_fgt # diagnose sys sdwan member
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
config service
edit 1
set name "Critical-DIA"
set mode priority
set src "LAN-net"
set internet-service enable
set internet-service-app-ctrl 16354 41468 16920
set health-check "Level3_DNS"
set priority-members 1 2
next
end

Exhibit A shows an SD-WAN event log and exhibit B shows the member status and the SD-WAN rule configuration.

Based on the exhibits, which two statements are correct? (Choose two.)

- A. FortiGate updated the outgoing interface list on the rule so it prefers port2.
- B. Port2 has the highest member priority.
- C. Port2 has a lower latency than port1.
- D. SD-WAN rule ID 1 is set to lowest cost (SLA) mode.

Answer: AC

QUESTION 50

Which two interfaces are considered overlay links? (Choose two.)

- A. LAG
- B. IPsec
- C. Physical
- D. GRE

Answer: BD

QUESTION 51

What are two benefits of using 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 requires application control to maintain signatures and perform load balancing.
- C. The ISDB applies rules to traffic from specific sources, based on application type.
- D. The ISDB contains the IP addresses and port ranges of well-known internet services.

Answer: AD

QUESTION 52

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

QUESTION 53

What does enabling the exchange-interface-ip setting enable FortiGate devices to exchange?

- A. The gateway address of their IPsec interfaces
- B. The tunnel ID of their IPsec interfaces
- C. The IP address of their IPsec interfaces
- D. The name of their IPsec interfaces

Answer: C

QUESTION 54

Which diagnostic command can you use to show the configured SD-WAN zones and their assigned members?

- A. diagnose sys sdwan zone
- B. diagnose sys sdwan service
- C. diagnose sys sdwan member
- D. diagnose sys sdwan interface

Answer: A

Explanation:

diagnose sys sdwan zone displays the configured zones and their members. Note that the output indicates the kernel interface index number of a member, which should match the index displayed by diagnose netlink interface list.

QUESTION 55

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 # diag sys sdwan zone
Zone overlay index=3
    members(3): 19(T_INET_0) 20(T_INET_1) 21(T_MPLS)
Zone underlay index=2
    members(2): 3(port1) 4(port2)
Zone virtual-wan-link index=1
    members(0):
```

```
17.779659 port5 in 10.0.1.101 -> 10.1.0.7: icmp: echo request
17.779717 T_INET_0 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
17.779795 T_INET_1 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
17.779821 T_MPLS out 10.0.1.101 -> 10.1.0.7: icmp: echo request
17.781852 T_INET_1 in 10.1.0.7 -> 10.0.1.101: icmp: echo reply
17.781874 port5 out 10.1.0.7 -> 10.0.1.101: icmp: echo reply
```

Exhibit B

```
3.679621 T_INET_1 in 10.0.1.101 -> 10.1.0.7: icmp: echo request
3.679735 port5 out 10.0.1.101 -> 10.1.0.7: icmp: echo request
3.679798 T_INET_0 in 10.0.1.101 -> 10.1.0.7: icmp: echo request
3.679835 T_MPLS in 10.0.1.101 -> 10.1.0.7: icmp: echo request
3.681827 port5 in 10.1.0.7 -> 10.0.1.101: icmp: echo reply
3.681853 T_INET_1 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

QUESTION 56

Refer to the exhibit.

Create New SD-WAN Interface Member

Sequence Number	1
Interface Member	
SD-WAN Zone	virtual-wan-link
Gateway IP	0.0.0.0
Cost	0
Status	<input checked="" type="checkbox"/>
Priority	0
Advanced Options >	

Which two SD-WAN template member settings support the use of FortiManager meta fields?
(Choose two.)

- A. Cost
- B. Interface member
- C. Priority
- D. Gateway IP

Answer: BD

QUESTION 57

Which statement about using BGP for ADVPN is true?

- A. IBGP is preferred over EBGP, because IBGP preserves next hop information.
- B. You must use BGP to route traffic for both overlay and underlay links.
- C. You must configure BGP communities.
- D. You must configure AS path prepending.

Answer: A

QUESTION 58

Refer to the exhibits.

Exhibit A.

```
branch1_fgt # diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
Tie break: cfg
Gen(8), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(manual)
Members(2):
    1: Seq_num(1 port1), alive, selected
    2: Seq_num(2 port2), alive, selected
Internet Service(3): GoToMeeting(4294836841,0,0,0,0 16354)
Microsoft.Office.365.Portal(4294837312,0,0,0,0 41468) Salesforce(42948377 84,0,0,0,0 16920)
Src address(1):
    10.0.1.0-10.0.1.255

Service(2): Address Mode(IPV4) flags=0x200 use-shortcut-sla
Tie break: cfg
Gen(7), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(manual)
Members(1):
    1: Seq_num(2 port2), alive, selected
Internet Service(2): Facebook(4294836714,0,0,0,0 15832) Twitter(4294838045,0,0,0,0 16001)
Src address(1):
    10.0.1.0-10.0.1.255

branch1_fgt # diagnose sys sdwan internet-service-app-ctrl-list

Facebook(15832 4294836714): 157.240.229.35 6 443 Wed Apr 26 07:49:30 2023
GoToMeeting(16354 4294836841): 23.205.106.86 6 443 Wed Apr 26 07:49:30 2023
GoToMeeting(16354 4294836841): 23.212.249.144 6 443 Wed Apr 26 07:49:31 2023
Salesforce(16920 4294837784): 23.212.249.11 6 443 Wed Apr 26 07:49:30 2023

branch1_fgt # get router info routing-table all
...
S*    0.0.0.0/0 [1/0] via 192.2.0.2, port1, [1/0]
        [1/0] via 192.2.0.10, port2, [1/0]
...
```

Exhibit B.

Destination IP	Service	Application	Security Event List	SD-WAN Rule Name	Destination Interface
23.212.248.205	HTTPS	GoToMeeting	APP: 2	Critical-DIA	port2
23.205.106.86	HTTPS	GoToMeeting	APP: 2	Critical-DIA	port1
23.205.106.86	HTTPS	GoToMeeting	APP: 2	Critical-DIA	port1
23.205.106.86	HTTPS	GoToMeeting	APP: 2	Critical-DIA	port1
23.212.249.144	HTTPS	GoToMeeting	APP: 2	Critical-DIA	port1
23.212.249.144	HTTPS	GoToMeeting	APP: 2	Critical-DIA	port1
23.212.249.144	HTTPS	GoToMeeting	APP: 2	Critical-DIA	port2
23.205.106.86	HTTPS	GoToMeeting	APP: 2	Critical-DIA	port2

Security
APP Count
Level
Log ID
Session ID
Tran Display
Virtual Domain
Source
Country
Device ID
Device Name

0000000013
769
snat
root
Reserved
FGVM01TM22000077
branch1_fgt

An administrator is testing application steering in SD-WAN. Before generating test traffic, the administrator collected the information shown in exhibit A.

After generating GoToMeeting test traffic, the administrator examined the respective traffic log on FortiAnalyzer, which is shown in exhibit B. The administrator noticed that the traffic matched the implicit SD-WAN rule, but they expected the traffic to match rule ID 1.

Which two reasons explain why the traffic matched the implicit SD-WAN rule? (Choose two.)

- A. FortiGate did not refresh the routing information on the session after the application was detected.
- B. Port1 and port2 do not have a valid route to the destination.
- C. Full SSL inspection is not enabled on the matching firewall policy.
- D. The session 3-tuple did not match any of the existing entries in the ISDB application cache.

Answer: AC

QUESTION 59

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

QUESTION 60

Which two statements are true about using SD-WAN to steer local-out traffic? (Choose two.)

- A. FortiGate does not consider the source address of the packet when matching an SD-WAN rule for local-out traffic.
- B. By default, local-out traffic does not use SD-WAN.
- C. By default, FortiGate does not check if the selected member has a valid route to the destination.
- D. You must configure each local-out feature individually, to use SD-WAN.

Answer: BD