Question #1 *Topic 1*

Which two statements correctly describe what happens when traffic matches the implicit SD-WAN rule? (Choose two.)

A. The session information output displays no SD-WAN service id.

B. Traffic is load balanced using the algorithm set for the v4-ecmp-mode setting.

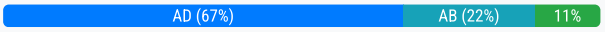
C. FortiGate flags the session with may_dirty and vwl_default.

D. Traffic does not match any of the entries in the policy route table.

E. The traffic is distributed, regardless of weight, through all available static routes.

**Suggested Answer:** *AD*

*Community vote distribution*




**jajajaf342** 1 month ago

**Selected Answer: AD**

As others have stated, the answer is AD.

A - There will be no service ID.
D - If there was a policy route matching the traffic, it would not hit the implicit SD-WAN rule, since policy routes are processed before SD-WAN rules (including the implicit SD-WAN rule).

upvoted 1 times

**one_1996** 1 month, 1 week ago

**Selected Answer: AD**

A/D are correct

upvoted 1 times

**one_1996** 1 month, 1 week ago

**Selected Answer: A**

When SD-WAN is enabled on a FortiGate firewall, the v4-ecmp-mode setting is replaced by the load-balance-mode setting under config system sdwan so the B is incorrect.
I think policy route is the sd-wan rule

upvoted 1 times

**felixcater** 1 month, 2 weeks ago

**Selected Answer: AD**

A: Correct. When a rule doesn't meet any of the sdwan rules, then it hit the implicit rule which is not a policy route. Policy routes like the real policy, isdb and sdwan rules have service id, however implicit rule does not.
B: Not Correct. v4-ecmp-mode setting becomes available when sdwan is enabled
C. Correct. The implicit rule is hit because the traffic did not hit any of the policy route table

upvoted 4 times

**MJ43891** 1 month, 3 weeks ago

**Selected Answer: AB**

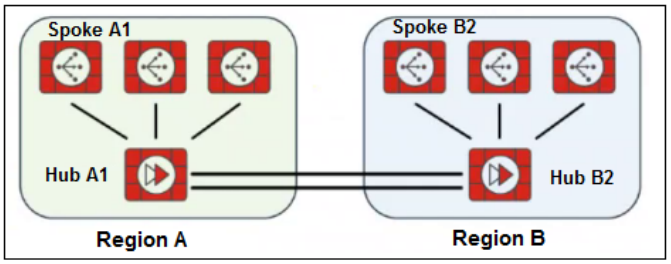
A is correct → No explicit SD-WAN rule = no service-id in session table.

B is correct → Traffic is handled by global ECMP load-balancing method (not SD-WAN service rules).

upvoted 2 times

Question #2 *Topic 1*

Refer to the exhibit.




Two hub-and-spoke groups are connected through redundant site-to-site IPsec VPNs between Hub1 and Hub2.
Which two configuration settings are required for the spoke A1 to establish an ADVPN shortcut with the spoke B2? (Choose two.)

A. On hubs, auto-discovery-sender must be enabled on the IPsec VPNs to spokes.

B. On hubs, auto-discovery-forwarder must be enabled on the IPsec VPNs to hubs.

C. On hubs, auto-discovery-receiver must be enabled on the IPsec VPNs to spokes.

D. On hubs, auto-discovery-forwarder must be enabled on the IPsec VPNs to spokes.

**Suggested Answer:** *AB*

*Community vote distribution*

AB (100%)

**jajajaf342** 1 month ago

**Selected Answer: AB**

The answer is AB.

A: auto-discovery-sender must be enabled on IPsec tunnels to spokes (basic configuration in any scenario)
B: auto-discovery forwarder must be enabled on IPsec tunnels to hubs for shortcuts between spokes that don't connect to the same hub via tunnels.

upvoted 1 times

**MJ43891** 1 month, 3 weeks ago

**Selected Answer: AB**

A (auto-discovery-sender on hubs → spokes)
Hubs must be able to send shortcut offers when they see transit traffic for a remote spoke. That is what tells the origin spoke "hey — I can offer you a direct shortcut to that remote spoke." So the hub → spoke phase-1s need auto-discovery-sender enabled.

B (auto-discovery-forwarder on hub→hub tunnels)
In a multi-hub (redundant hub) topology the hubs must forward discovery offers between regions: the hub-to-hub tunnels need auto-discovery-forwarder enabled so an offer that originates in Region A can be forwarded to the appropriate hub in Region B (and vice versa). Without the forwarder on the hub-to-hub VPN, spokes in different hub regions won't learn about each other and won't build the ADVPN shortcut.

upvoted 2 times

**felixcater** 1 month, 3 weeks ago

**Selected Answer: AB**

Hub-to-Spoke: Auto-discovery Sender must be enabled on the Hub. And Receiver on the Spokes.
Hub-to-Hub: Auto-discovery Forwarder must be enabled on the two Hubs.

upvoted 4 times

Question #3 *Topic 1*

Refer to the exhibit.

**Diagnose output**

```
fgt1_1 # diagnose sys sdwan service4

Service(1): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
     Tie break: cfg
     Shortcut priority: 2
      Gen(1), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(priority),
     link-cost-factor ( latency), link-cost-threshold(10), heath-check (Corp_HC)
      Members(2):
          1: Seq_num (2 port2 underlay), alive, latency: 0.906, selected
          2: Seq_num (1 port1 underlay), alive, latency: 1.079, selected
     Application Control(2): Microsoft.Portal(41469,0) Business(0,29)
     Src address(1):
          10.0.1.0-10.0.1.255

Service(2): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
     Tie break: cfg
     Shortcut priority: 2
      Gen(1), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(priority),
     link-cost-factor ( latency), link-cost-threshold(10), heath-check (Corp_HC)
      Members(1):
          1: Seq_num (2 port2 underlay), alive, selected
     Application Control(2): Social.Media(0,23) General.Interest(0,12)
     Src address(1):
          10.0.1.0-10.0.1.255

Service(3): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
     Tie break: cfg
     Shortcut priority: 2
      Gen(1), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(sla hash-
mode=round-robin)
      Members(3):
          1: Seq_num(4 HQ_T1 overlay), alive, sla(0x3), gid(0), cfg_order(0),
local cost(0), selected
          2: Seq_num(5 HQ_T2 overlay), alive, sla(0x3), gid(0), cfg_order(1),
local cost(0), selected
          3: Seq_num(6 HQ_T3 overlay), alive, sla(0x3), gid(0), cfg_order(2),
local cost(0), selected
     Src address(1):
          10.0.1.0-10.0.1.255

     Dst address(1):
          0.0.0.0-255.255.255.255
```

The exhibit shows output of the command diagnose sys sdwan service4 collected on a FortiGate device
The administrator wants to know through which interface FortiGate will steer traffic from local users on subnet 10 0.1.0/255.255.255.192 and with a destination of the social media application Facebook.
Based on the exhibits, which two statements are correct? (Choose two.)

A. FortiGate steers traffic for social media applications according to the service rule 2 and steers traffic through port2.

B. When FortiGate cannot recognize the application of the flow, it load balances the traffic through the tunnels HQ_T1, HQ_T2, HQ_T3.

C. There is no service defined for the Facebook application, so FortiGate appliesservice rule 3 and directs the traffic to headquarters.

D. When FortiGate cannot recognize the application of the flow, it steers the traffic through the preferred member of rule 3, HQ_T1.

**Suggested Answer:** *AB*

*Community vote distribution*

AB (86%) 14%

**jajajaf342** 1 month ago

**Selected Answer: AB**

The answer is AB.

If it recognizes the traffic as going to Facebook, it will use the rule with service ID 2, and be routed through port 2 per the rule.

If it does not recognize the application traffic, it will hit the catch-all rule with service ID rule 3. This uses Lowest Cost SLA and load-balancing for round-robin - all members are alive and meet SLA.

Therefore, per page 250 of the SD-WAN 7.4 Architect notes, priority, cost or configuration order will not be considered, and traffic will be load-balanced in circular fashion.

upvoted 3 times

**one_1996** 1 month, 1 week ago

**Selected Answer: AB**

A/B are correct because the round-robin mode use all active link

upvoted 3 times

**one_1996** 1 month, 1 week ago

But the tie-break is set to cfg, so the member with the lowest cfg_order wins, which is HQ_T1. Therefore, the correct answer is D.

upvoted 2 times

**jajajaf342** 1 month ago

You are mistaken - please update or edit your comment. The answer is AB.

Per page 250 of the SD-WAN 7.4 Architect notes:

"Note that FortiGate doesn't consider the member cost, priority, and configuration order. With the manual strategy FortiGate considers all members that are alive. With the lowest cost (SLA) strategy, FortiGate considers only the number of SLA targets the member meets."

In our case, we use Lowest Cost (SLA) with round-robin - therefore no tie-breakers are considered (in your case, you reference the 'cfg' order, but this doesn't matter in the load-balanced scenario). Only members that meet SLA are considered, and traffic is round-robin'ed through each alive member (all 3).

Consider that you MUST set some sort of configuration priority order for members on any SD-WAN rule - if what you were saying were true, it would be IMPOSSIBLE to configure load-balancing in Manual mode, since there will always be a "tie" for all alive members, and consequently all traffic would be routed through the highest configuration priority member (therefore rendering load-balancing impossible).

upvoted 1 times

**felixcater** 1 month, 3 weeks ago

**Selected Answer: AD**

A. Clearly, Social Media is enabled in the Application Control profile. Therefore the local users would be able to reach Facebook via Service 2.
D. should in case the user cannot access Facebook application via Service 2, for example, the underlay path to Facebook is not stable, therefore, rule 3, HQ_T1 should be preferred because it is one of the Tunnels for the HUB and from the Hub, traffic can then be directed to the Internet via the HUB's virtual-wan-Link.

upvoted 1 times

**felixcater** 1 month, 1 week ago

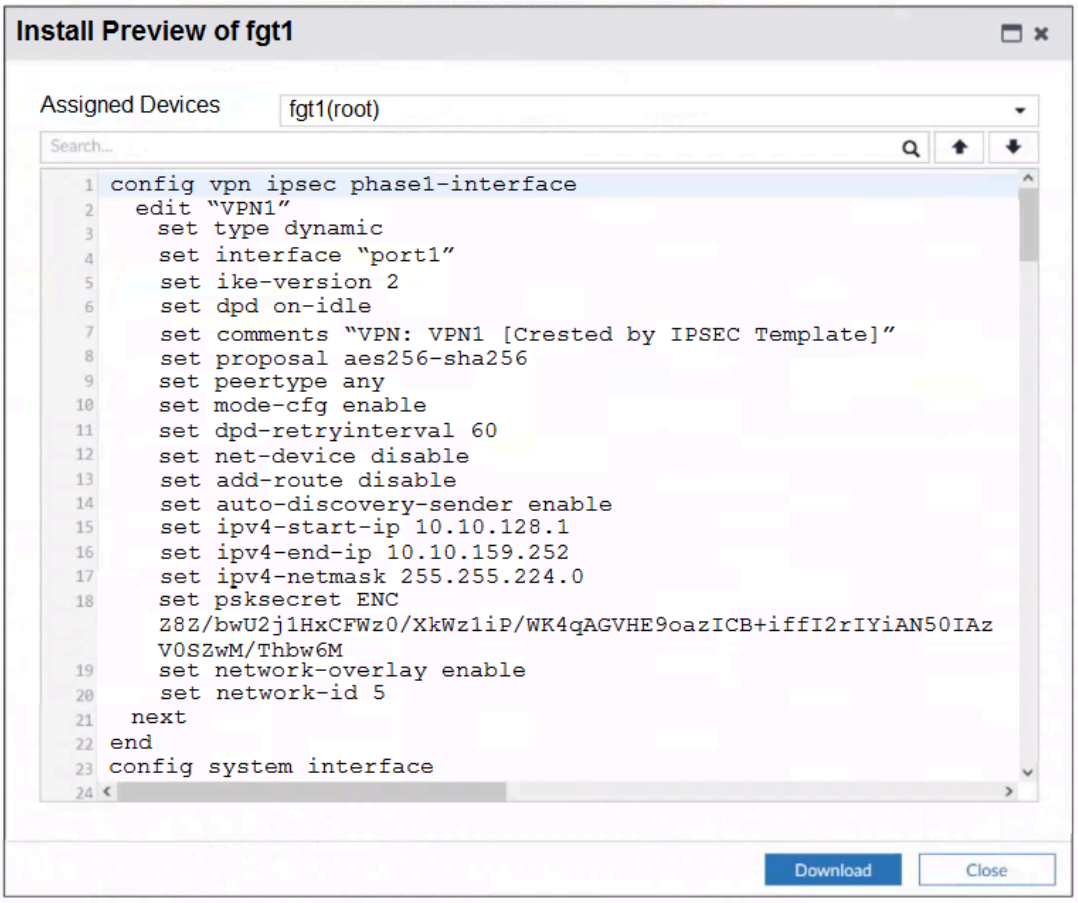
I have had a re-think over the answers.
A: Clearly, Social Media is enabled in the Application Control profile. Therefore the local users would be able to reach Facebook via Service 2.

B: Correct because when fortigate cannot recongnize the application in th flow, it will load-balance the traffic across the three overlay tunnels. Load balances because the sla hash-mode is round-robin.

upvoted 4 times

Question #4 *Topic 1*

Refer to the exhibit.




The administrator used the SD-WAN overlay template to prepare an IPsec tunnels configuration for a hub-and-spoke SD-WAN topology. The exhibit shows the FortiManager installation preview for one FortiGate device.

Based on the exhibit, which statement best describes the configuration applied to the FortiGate device?

A. It is a spoke device that establishes dynamic IPsec tunnels to the hub. The local subnet range is 10.10 128.0/23.

B. It is a hub device. It can send ADVPN shortcut offers.

C. It is a hub device. It will automatically discover the spoke devices and add them to the SD-WAN topology.

D. It is a spoke device that establishes dynamic IPsec tunnels to the hub. It can send ADVPN shortcut requests.

**Suggested Answer:** *B*

*Community vote distribution*

B (100%)

**jajajaf342** 1 month ago

Selected Answer: B

Indeed, correct answer is B.

"set auto-discovery-sender enable" would only be enabled on a hub device so that it can send ADVPN shortcut messages to spokes.

A - you would not set this on a spoke device.
C - While it is a hub device, it is not because it can "automatically discover the spoke devices and add them to the SD-WAN topology"
D - It is not a spoke device

upvoted 2 times

**MJ43891** 1 month, 3 weeks ago

Selected Answer: B

set auto-discovery-sender enable <----- Enable ADVPN on Hub
Hence it is a Hub

upvoted 3 times

**felixcater** 1 month, 3 weeks ago

**Selected Answer: B**

B. This is correct. It is the Hub that will send the shortcut offer while the Spoke sends shortcut request.

C. Incorrect. Hub does not discovery the Spoke. It is the Spoke that discovers the Hub.

D. It is not a Spoke device because in the Spoke "set type" should be "Static" and not "dynamic". Hub should be set to dynamic.

upvoted 2 times

Question #5 *Topic 1*

You are planning a new SD-WAN deployment with the following criteria:

Two regions -
Most of the traffic is expected to remain within its region
No requirement for inter-region ADVPN
To remain within the recommended best practices, which routing protocol should you select for the overlays?

A. IBGP with BGP on loopback within each region and EBGP between the regions.

B. OSPF for the routing within each region and EBGP between the regions.

C. IBGP within each region and between the regions.

D. IBGP with BGP per overlays within each region and IBGP with BGP on loopback between the regions.

**Suggested Answer:** *A*

*Community vote distribution*

A (100%)

**one_1996** 1 month, 1 week ago

**Selected Answer: A**

IBGP for intraregion on loopback and EBGP for interregion

upvoted 3 times

**felixcater** 1 month, 1 week ago

**Selected Answer: A**

A: IBGP within the Region and EBGP between the regions

upvoted 3 times

Question #6 *Topic 1*

Refer to the exhibit.

```
ike V=root:0:VPN1_0:9: received informational request
ike V=root:0:VPN1_0:9: processing notify type SHORTCUT_QUERY
ike V=root:0:VPN1_0: recv shortcut-query 5752810260829471092
6d5cdb5ceab1874d
/0000000000000000 192.2.0.1 10.0.1.101:2048 -> 10.0.3.101:0 0 psk 64 ppk 0
ttl
32 nat 0 ver 2 mode 0 network-id 1
ike V=root:0:VPN1: iif 20 10.0.1.101 -> 10.0.3.101 0 route lookup oif 20
VPN1
gwy 192.168.1.4
ike V=root:0: shared dev tunnel lookup, tun-id=192.168.1.4
ike V=root:0:VPN1_3: forward shortcut-query 5752810260829471092 6
d5cdb5ceab18
74d/0000000000000000 192.2.0.1 10.0.1.101->10.0.3.101 0 psk 64 ppk 0 ttl 31
ver 2 mode 0, exr-mapping 192.2.0.1:0, network-id 1
```

Which statement best describe the role of the ADVPN device in handling traffic?

A. This is a hub that has received a query from a spoke and has forwarded it to another spoke.

B. This is a hub in a dual-region topology. The remote hub tunnel ID is 10.0.2.101.

C. This is a spoke that has received a shortcut query from another spoke and has forwarded the response to its hub.

D. This is a spoke. The kernel received a shortcut request and forwards the query to another spoke.

**Suggested Answer:** *A*

*Community vote distribution*

A (100%)

**jajajaf342** 1 month ago

**Selected Answer: A**

A is correct.

B - no indication that this is a multi-hub topology.
C - the key is "forward" - only hubs forward shortcut queries, not spokes themselves. Therefore, this cannot be a spoke.
D - For the same reason as C, this cannot be a spoke.

upvoted 1 times

**eleazar_garrido** 1 month, 2 weeks ago

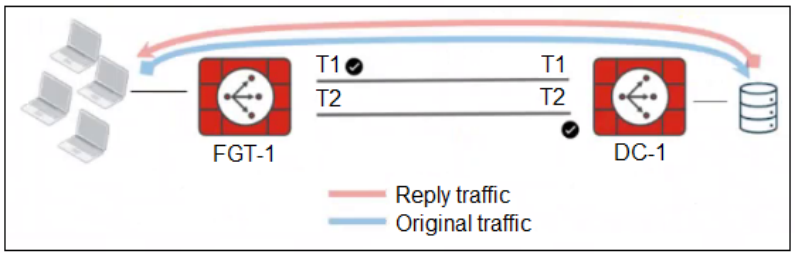
**Selected Answer: A**

FORWARD THE QUERY

upvoted 2 times

Question #7 *Topic 1*

Refer to the exhibit.




The administrator analyzed the traffic between a branch FortiGate and the server located in the data center, and noticed the behavior shown in the diagram. When the LAN clients located behind FGT1 establish a session to a server behind DC-1, the administrator observes that, on DC-1, the reply traffic is routed over T2, even though T1 is the preferred member in the matching SD-WAN rule.
What can the administrator do to instruct DC-1 to route the reply traffic through the member with the best performance?

A. Enable auxiliary-session under config system settings.

B. Enable snat-route-change under config system global.

C. Enable reply-session under config system sdwan.

D. FortiGate route lookup for reply traffic only considers routes over the original ingress interface.

**Suggested Answer:** *A*

*Community vote distribution*

A (89%) 11%

**felixcater** Highly Voted 1 month, 2 weeks ago

Selected Answer: A

A: "auxiliary-session" must be enabled on DC-1 Fortigate to reply the traffic over T2 because it has better performance over T1. Initially "auxiliary-session" is disabled by default.

upvoted 5 times

**jajajaf342** Most Recent 1 month ago

Selected Answer: A

Correct answer is A:

From SD-WAN 7.4 Architect pages 189-190:

"... by default, when performing route lookups for the reply direction, FortiGate considers only routes through the same ingress interface used in the original direction... Auxiliary sessions solve the two previous issues by enabling FortiGate to: ... Select the best route for reply traffic through any member, not necessarily the same interface where the original incoming traffic was received."

upvoted 3 times

**NitinKumar4654** 1 month ago

Selected Answer: C

Initially "auxiliary-session" is disabled by default.

upvoted 1 times

Question #8 *Topic 1*

You are planning a large SD-WAN deployment with approximately 1000 spokes and want to allow ADVPN between the spokes. Some remote sites use FortiSASE to connect to the company's SD-WAN hub.
Which overlay routing configuration should you use?

A. BGP on loopback with IPsec phase2 selectors for ADVPN shortcut routing.

B. BGP per overlay with dynamic BGP for ADVPN shortcut routing.

C. BGP per overlay with BGP next-hop convergence for ADVPN shortcut routing.

D. BGP on loopback with dynamic BGP for ADVPN shortcut routing.

**Suggested Answer:** *D*

*Community vote distribution*

D (100%)

**jajajaf342** 1 month ago

**Selected Answer: D**

D is the correct answer. Refer to SD-WAN 7.4 Architect, page 371.

The table shows that only the following options support FortiSASE integration:
- BGP per overlay + BGP next-hop convergence
- BGP on loopback + BGP next-hop convergence
- BGP on loopback + Dynamic BGP

However, given the scalability requirements, of these only BGP on loopback + Dynamic BGP provides good scalability - therefore, D is the correct answer.

upvoted 2 times

Question #9 *Topic 1*

Refer to the exhibit that shows event logs on FortiGate.

**Event log on FortiGate**

```
6: date=2024-12-18 time=15:15:06 eventtime=1734563705745090691 tz= "-0800" logid=
"0113022925" type= "event" subtype= "sdwan" level= "information" vd= "root" logdesc=
"SDWAN SLA information" eventtype= "SLA" healthcheck= "HUB1_HC" slatargetid=1
interface= "HUB1-VPN3" status= "up" latency= "1.001" jitter= "0.162" packetloss=
"0.000" moscodec= "g711" mosvalue= "4.404" inbandwidthavailable= "10.00Gbps"
outbandwidthavailable= "10.00Gbps" bidandwidthavailable= "20.00Gbps" inbandwidthused=
"0kbps" outbandwidthused= "0bkps" bibandwidthused= "0kbps" slamap= "0x1" msg= "Health
Check SLA status."

7: date=2024-12-18 time=15:14:26 eventtime=1734563666333265394 tz= "-0800" logid=
"0101037141" type= "event" subtype= "vpn" level= "notice" vd= "root" logdesc= "IPsec
tunnel statistics" action= "tunnel-stats" remip=120.64.1.1 locip=192.2.0.1 remport=
500 locport=500 outintf="port1" srccountry= "Reserved" cookies=
"50b8a3684ddfd2cb/af3f725d883c5585" user= "10.0.64.1.1" group= "N/A" useralt= "N/A"
xauthuser= "N/A" xauthgroup= "N/A" assignip=172.168.1.1 vpntunnel= "VPN4_0"
tunnelip=N/A tunnelid=3050027470 tunneltype= "ipsec" duration=2968 sentbyte=245849
rcvdbyte=246456 nextstat=600 fctuid= "N/A" advpnsc=0

8: date=2024-12-18 time=15:04:26 eventtime=1734563066334261977 tz= "-0800" logid=
"0101037141" type= "event" subtype= "vpn" level= "notice" vd= "root" logdesc= "IPsec
tunnel statistics" action= "tunnel-stats" remip=100.64.33.1 locip=192.2.0.1 remport=
4500 locport=4500 outintf="port1" srccountry= "Reserved" cookies=
"cff150ded109a548/165f413d17cecc49" user= "Branch3" group= "N/A" useralt= "N/A"
xauthuser= "N/A" xauthgroup= "N/A" assignip=N/A vpntunnel= "HUB1-VPN1_0" tunnelip=
192.168.1.4 tunnelid=3050027486 tunneltype= "ipsec" duration=1122 sentbyte=92064
rcvdbyte=0 nextstat=600 fctuid= "N/A" advpnsc=1

9: date=2024-12-18 time=15:04:26 eventtime=1734563066334252138 tz= "-0800" logid=
"0101037141" type= "event" subtype= "vpn" level= "notice" vd= "root" logdesc= "IPsec
tunnel statistics" msg="IPsec tunnel statistics" action= "tunnel-stats" remip=
172.16.1.1 locip=172.16.0.1 remport=500 locport=500 outintf="port4" srccountry=
"Reserved" cookies= "celc2c62ecc04871/a4d93a059b8df005" user= "172.16.1.1" group=
"N/A" useralt= "N/A" xauthuser= "N/A" xauthgroup= "N/A" assignip=192.168.1.193
vpntunnel= "HUB2-VPN3" tunnelip=N/A tunnelid=3050027467 tunneltype= "ipsec" duration=
2367 sentbyte=195836 rcvdbyte=196492  nextstat=600 fctuid= "N/A" advpnsc=0
```

Based on the output shown in the exhibit, what can you say about the tunnels on this device?

A. The master tunnel HUB2-VPN3 cannot accept ADVPN shortcuts.

B. There is one shortcut tunnel built from master tunnel VPV4.

C. The device steers voice traffic through the VPN tunnel HUB1-VPN3.

D. The VPN tunnel HUB1-VPN1_0 is a shortcut tunnel.

**Suggested Answer:** *D*

*Community vote distribution*

D (100%)

**jajajaf342** 1 month ago

Selected Answer: D

Correct answer is D, as "advpnsc=1" is shown at the end for HUB1-VPN1_0.

upvoted 1 times

**felixcater** 1 month, 1 week ago

Selected Answer: D

D: it is correct because advpnsc=1 in the paragraph 3.

upvoted 1 times

Question #10 *Topic 1*

Which three characteristics apply to provisioning templates available on FortiManager? (Choose three.)

A. A template group can include a system template and an SD-WAN template.

B. A CLI template group can contain CLI templates of both types.

C. Each template group can contain up to three IPsec tunnel templates.

D. A CLI template can be of type CLI script or Peri script.

E. CLI templates are applied in order, from top to bottom.

**Suggested Answer:** *ABE*

*Community vote distribution*

ABE (100%)

**jajajaf342** 1 month ago

**Selected Answer: ABE**

ABE are correct.

C is incorrect because there's no artificial restriction on how many IPsec tunnel templates can be added to a template group
D is incorrect because there's no "Perl" type for scripts - only CLI and Jinja
upvoted 1 times

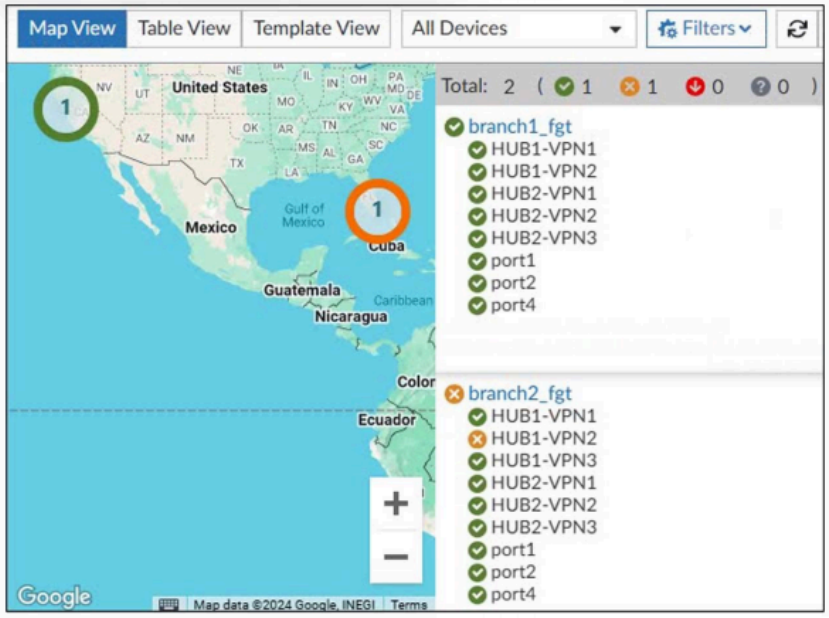
**4dc6bba** 3 weeks, 4 days ago

Agree with your answer, however I believe only one IPsec tunnel template can be added to a single template group, speaking from experience
upvoted 1 times

Question #11 *Topic 1*

Refer to the exhibit.

**FortiManager SD-WAN monitor**




An administrator checks the status of an SD-WAN topology using the FortiManager SD-WAN monitor menus. All members are configured with one or two SLAs.

Which two conclusions can you draw from the output shown? (Choose two.)

A. The template view should be used to see the hub devices.

B. This SD-WAN topology contains only two branch devices.

C. One member of branch2_fgt is missing the SLAs.

D. branch2_fgt establishes six tunnels to the hubs and they are all up.

**Suggested Answer:** *BC*

*Community vote distribution*

BC (83%) CD (17%)

**jajajaf342** Highly Voted 1 month ago

Selected Answer: BC

BC is correct.

B is correct, since you can see the "Total: 2" at the top, indicating there are 2 branch devices total.

C is correct, because branch 2 has a member that's failing SOME SLA checks - not all. It would be red otherwise.

upvoted 5 times

**4dc6bba** Most Recent 3 weeks, 4 days ago

Selected Answer: CD

I believe D seems correct because the branch establishes 6 total tunnels to the hub and all are up, only 1 is failing SLA but it's not "Down" (red)

C is correct because the SLA checks is failing for 1 member (yellow)

I don't think B is correct because only 2 branch devices are shown, but where are the hubs? The output implies they connect to hubs.

upvoted 1 times

**4dc6bba** 2 weeks, 4 days ago

Correction I think it's BC, hubs aren't mentioned anywhere even if they're configured.

upvoted 1 times

Question #12 *Topic 1*

Refer to the exhibit.

**SD-WAN configuration on FortiGate**

```
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, [10/0]
C    10.0.1.0/24 is directly connected, port5
B    10.1.0.0/24 [200/0] via 192.168.1.61 (recursive is directly connected, HUB1-VPN1), 1d03h58m, [1/0]
                 [200/0] via 192.168.1.125 (recursive is directly connected, HUB1-VPN2), 1d03h58m, [1/0]
                 [200/0] via 192.168.1.189 (recursive is directly connected, HUB1-VPN3), 1d03h58m, [1/0]
C    10.200.99.1/32 is directly connected, Branch-Lo
B    10.2.0.0/16 [200/0] via 192.168.1.61 (recursive is directly connected, HUB1-VPN1), 00:03:01, [1/0]
                 [200/0] via 192.168.1.125 (recursive is directly connected, HUB1-VPN2), 00:00:51, [1/0]
                  [200/0] via 192.168.1.189 (recursive is directly connected, HUB1-VPN3), 00:00:51, [1/0]
B    10.2.5.0/24 [200/0] via 192.168.1.61 (recursive is directly connected, HUB1-VPN3), 00:03:01, [1/0]
…

branch_fgt # diag sys sdwan service4

Service(3): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
 Tie break: fib
 Shortcut priority: 2
  Gen(3), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(sla), sla-compare-order
  Members(3):
     1: Seq_num(5 HUB1-VPN2 HUB1), alive sla(0x1), gid(0), cfg_order(1), local cost(0), selected
     2: Seq_num(6 HUB1-VPN3 HUB1), alive sla(0x1), gid(0), cfg_order(2), local cost(0), selected
     3: Seq_num(4 HUB1-VPN1 HUB1), alive sla(0x0), gid(0), cfg_order(0), local 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

Service(4): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
 Tie break: fib
 Shortcut priority: 2
  Gen(2), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(sla), sla-compare-order
  Members(2):
     1: Seq_num(2 port2 underlay), alive sla(0x3), gid(0), cfg_order(1), local cost(0), selected
     2: Seq_num(1 port1 underlay), alive sla(0x1), gid(0), cfg_order(0), local cost(0), selected
   Src address(1):
     10.0.1.0-10.0.1.255

  Dst address(1):
     10.2.0.0-10.2.255.255
```

Which SD-WAN rule and interface uses FortiGate to steer the traffic from the LAN subnet 10.0.1.0/24 to the corporate server 10.2.5.254?

A. SD-WAN service rule 3 and interface HUB1-VPN2.

B. SD-WAN service rule 3 and interface HUB1-VPN3.

C. SD-WAN service rule 4 and interface port2.

D. SD-WAN service rule 4 and port1 or port.

**Suggested Answer:** *B*

*Community vote distribution*

B (60%) A (40%)

**471dfbf** 3 weeks, 3 days ago

**Selected Answer: B**

HUB1-VPN3 is the only route available in the FIB (longest /24 match). SD-WAN will ignore other options configured if no valid route exist.

upvoted 1 times

**7abc0bc** 3 weeks, 6 days ago

**Selected Answer: B**

Is option B --> Tie Breaker: FIB it choose the most specific route, if Tie Breaker was CFG would be option A

upvoted 2 times

**jajajaf342** 1 month ago

**Selected Answer: B**

The answer is B - HUB1-VPN3.

First off, the traffic matches the SD-WAN rule with service ID 3. We can see that there is at least one valid route in the FIB, so the SD-WAN rule will be selected.

Next, we see HUB1-VPN2 and HUB1-VPN3 have the same slamap value of 0x1 - therefore, they are equally valid members to choose from, and a tiebreak occurs (since there is no load balancing configured).

Looking at the routes, HUB1-VPN3 has a more SPECIFIC route (i.e. better route) and therefore, it wins the tiebreak.

upvoted 3 times

**3101a6a** 1 month ago

**Selected Answer: A**

In my understanding, it is alternative A

upvoted 2 times

**one_1996** 1 month, 1 week ago

**Selected Answer: A**

I think the traffic follows service 3. The traffic should follow member 3 but it has sla (0x0) so it does not respect the sla and goes to member 1 with cfg_order(1) which respects an sla so the answer is HIB1-VPN2

upvoted 3 times

**felixcater** 1 month, 1 week ago

**Selected Answer: A**

A: is correct because the destination 10.2.5.254 belongs to the subnets 10.2.0.0/16 and 10.2.5.0/24 which were advertised via the BGP in the "get router info routing-table all" through HUB1-VPN2 Tunnel. Therefore, the Service Rule 3 is chosen. The Tunnel "HUB-VPN2" is right because it is the next in the "cfg_order" since sla (0x0) cannot be chosen because it doesn't meet the sla. cfg_order(1) is that interface that"HUB1-VPN2" belongs to.

upvoted 1 times

**jajajaf342** 1 month ago

This is incorrect because the most specific route is the tiebreak, not the cfg-order. The answer is B.

upvoted 2 times

**altres** 1 month ago

But the Tie Break is configured to fib. According to the guide p204, in this case the Traffic should be routed via hub1-vpn3 since it has the best route to the target. VPN1 and VPN3 both meet the SLA. VPN2 would be chosen if Tie Break would be configured as cfg order

upvoted 2 times

**one_1996** 1 month, 1 week ago

**Selected Answer: B**

on the routing table fgt prefers a smaller length so fgt prefers HUB1-VPN3 in the service flow matches service 3 and only the second sequence number has a valid path

upvoted 3 times

Question #13 *Topic 1*

Within the context of SD-WAN, what does SIA correspond to?

A. Remote Breakout

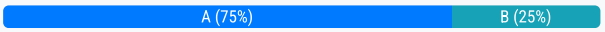
B. Software Internet Access

C. Secure Internet Authorization

D. Local Breakout

**Suggested Answer:** *A*

*Community vote distribution*




**jajajaf342** 1 month ago

**Selected Answer: A**

Answer is A.

Straight from page 12 of the SD-WAN 7.4 Architect documentation:

"Secure internet access (SIA), also known as remote breakout, is another use case for SD-WAN."

upvoted 1 times

**felixcater** 1 month, 1 week ago

**Selected Answer: A**

A: Correct. SIA is Secure Internet Access also known as Remote Breakout. Meaning traffic are backhauled to the HUB via the Overlay and break out to the Internet at the HUB.

upvoted 2 times

**one_1996** 1 month, 1 week ago

**Selected Answer: B**

I think software-based Internet access is the right answer. Direct Internet access (DIA) is a local breakout

upvoted 1 times

**one_1996** 1 month, 1 week ago

I made a mistake: SIA stands for Security-Driven Intelligent Application and it is used for RIA. A is correct

upvoted 2 times

Question #14 *Topic 1*

The exhibits show the configuration for SD.WAN performance, SD-WAN rule, the application IDs of Facebook and YouTube along with the firewall policy configuration and the underlay zone status.

**Configuration for SD-WAN performance SLA, SD-WAN rule configuration, and application IDs of Facebook and YouTube.**

```
config system sdwan
     configure 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

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

branch_fgt # get application name status | grep "id: 31077" -B1
app-name: "Youtube"
id: 31077
```

**Underlay zone status**

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

Which two statements are true about the health and performance of SD.WAN members 3 and 4? (Choose two.)

A. The performance is an average of the metrics measured for Facebook and YouTube traffic passing through the member

B. Only related TCP traffic is used for performance measurement

C. FortiGate identifies the member as dead when there is no Facebook and YouTube traffic passing through the member.

D. Encrypted traffic is not used for the performance measurement.

**Suggested Answer:** *AB*

*Community vote distribution*

AB (100%)

**jajajaf342** 1 month ago

**Selected Answer: AB**

AB is correct.

Refer to: https://community.fortinet.com/t5/FortiGate/Technical-Tip-Different-types-of-Health-checks-used-in-SD-WAN/ta-p/286779

In passive health checks, TCP RTT traffic is used to determine link quality, so B is correct. In addition, passive health checks use an average measure of latency, jitter, and packet loss to determine quality of the link - so A is also correct.

C is incorrect because passive monitoring does not mark members as dead. D is a complete red herring, as encryption has nothing to do how passive health checks gauge SLA status.

upvoted 3 times

**one_1996** 1 month, 1 week ago

**Selected Answer: AB**

the correct answars are A and B

upvoted 2 times

Question #15 *Topic 1*

When a customer delegates the installation and management of its SD-WAN infrastructure to an MSP, the MSSP usually keeps the hub within its infrastructure for ease of management and to share costly resources.
In which two situations will the MSSP install the hub in customer premises? (Choose two.)

A. The administrator expects a large volume of traffic between the branches.

B. The customer requires SIA with centralized breakout

C. The customer expects a large amount of VoIP traffic.

D. The majority of the branch traffic is directed to a corporate data center.

**Suggested Answer:** *BD*

*Community vote distribution*


**jajajaf342** 3 weeks, 4 days ago

**Selected Answer: BD**

BD is correct.

From page 326 of SD-WAN 7.4 Architect:

"Another popular MSSP choice is to deploy the hubs on the customer premises, such as at a central office or a data center. The traffic flow in this blueprint is quite different from the two previous scenarios described. The majority of the traffic is likely to be either spoke-to-hub—branch sites accessing workloads hosted in the data center or an RIA through a centralized breakout owned by the customer—or DIA on the spokes. In this type of topology, occasional spoke-to-spoke traffic is possible, but rare, and usually non-existent."

upvoted 2 times

**fernandosanchez88** 4 weeks, 1 day ago

**Selected Answer: BD**

Option B should be: Customer requeris RIA with centralized breakout
Option D is ok, because traffic flow is Spoke-to-hub, spoke-to-spoke is possible but rare.

upvoted 2 times

**one_1996** 1 month, 1 week ago

**Selected Answer: BD**

I think BD because branch traffic is forwarded in shortcut from branch to branch this traffic don't goes to hub

upvoted 4 times

Question #16 *Topic 1*

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

A. Create policy packages and assign them to the branch devices.

B. Configure SD-WAN rules.

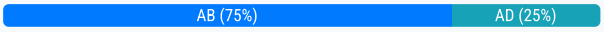
C. Configure routing through the overlay tunnels created by the SD-WAN overlay template

D. Assign an sdwan_id metadata variable to each device (branch and hub).

E. Assign a hub_id metadata variable to each hub device.

**Suggested Answer:** *AB*

*Community vote distribution*




**jajajaf342** 3 weeks, 4 days ago

**Selected Answer: AB**

AB is correct.

From the slide on page 77 of SD-WAN 7.4 Architect, the options under "Mandatory" are:
- Assign metadata variables to devices (branch_id)
- Configure SD-WAN rules by editing SD-WAN template
- Create policy packages for branch and hub devices
- Install the changes to SD-WAN devices using the install wizard

Of the 4 options, only A and B are matches - there is no such thing as an "sdwan_id" or "hub_id" metadata variable (at least, not created by the overlay template), and routing is taken care of through the overlay template wizard.

upvoted 3 times

**leonel_marco** 3 weeks, 5 days ago

**Selected Answer: AD**

The overlay template creates the infrastructure (IPsec tunnels, SD-WAN zones, etc.), but the administrator must assign values to the metadata variables (sdwan_id, branch_id, etc.) so that each device has its unique identity in the overlay.

Once the infrastructure is ready, policy packages must be created and assigned to devices to allow traffic (including health checks) and enforce security rules.

upvoted 1 times

Question #17 *Topic 1*

SD-WAN interacts with many other FortiGate features. Some of them are required to allow SD-WAN to steer the traffic.
Which three configuration elements that you must configure before FortiGate can steer traffic according to SD-WAN rules? (Choose three.)

A. Interfaces

B. Routing

C. Firewall policies

D. Traffic shaping

E. Security profiles

**Suggested Answer:** *ABC*

*Community vote distribution*

ABC (100%)

**felixcater** 1 month, 1 week ago

**Selected Answer: ABC**

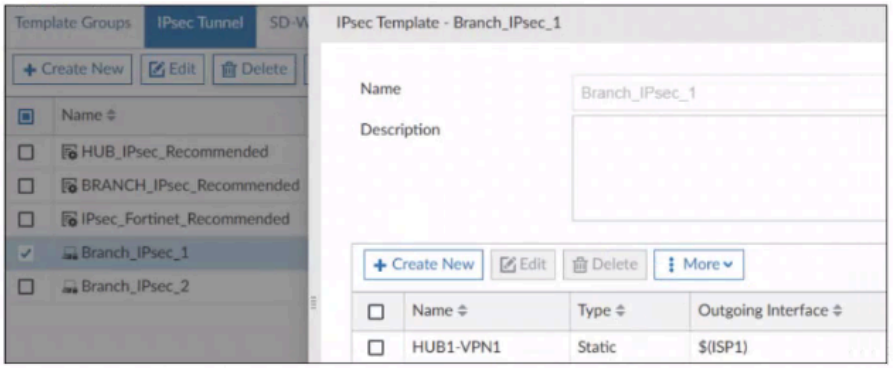
ABC are correct. The interfaces must be configured. The Routing must be in the FIB and also there must be a firewall policies.

upvoted 2 times

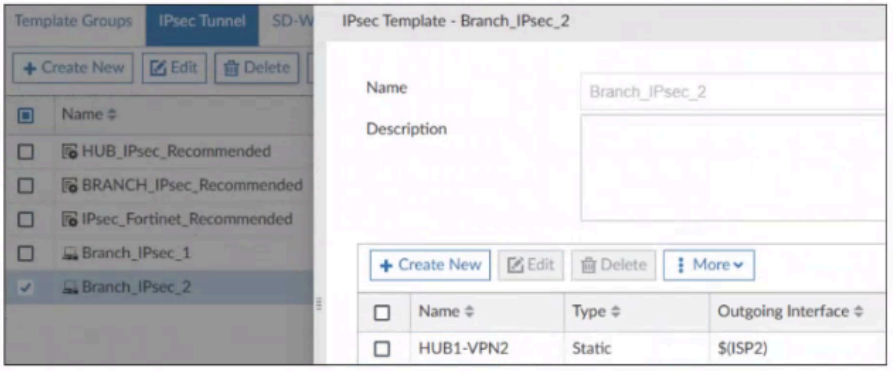
Question #18 *Topic 1*

Refer to the exhibits.

**IPsec template for Branch_IPsec_1**




**IPsec template for Branch_IPsec_2**




**Error message in FortiManager**


The exhibits show two IPsec templates to define Branch_IPsec_1 and Branch_IPsec_2. Each template defines a VPN tunnel. The error message that FortiManager displayed when the administrator tried to assign the second template to the FortiGate device is also shown.
Which statement best describes the cause of the issue?

A. You should use the same outgoing interface of both templates.

B. You can assign only one IPsec template to each FortiGate device.

C. You should review the branch1_fgt configuration for configured tunnels in the root VDOM.

D. You can assign only one template with a tunnel type of static to each FortiGate device.

**Suggested Answer:** *B*

*Community vote distribution*

B (100%)

**felixcater** 1 month, 1 week ago

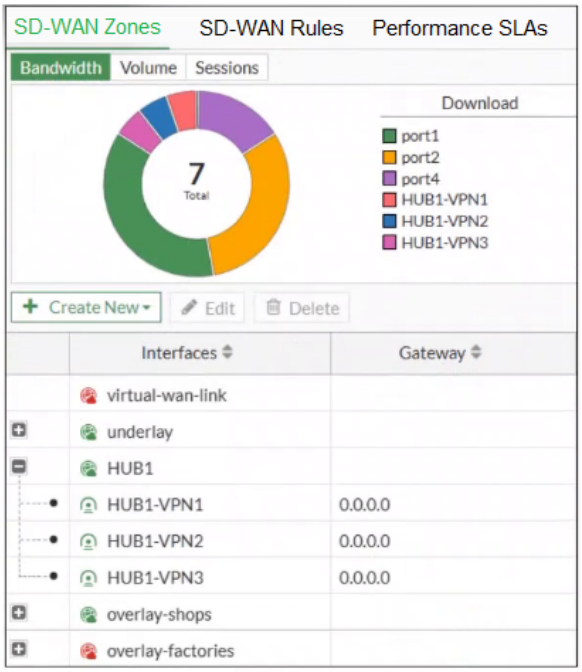
**Selected Answer: B**

B. Only one IPsec template can be assigned to each Fortigate device.

upvoted 2 times

Question #19 *Topic 1*

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




What can you conclude about the zone and member configuration on this device?

A. The overlay-factories zone contains no member.

B. The underlay zone contains three members.

C. You can move HUB1-VPN3 from the HUB1 zone to the overlay-shops zone.

D. You can delete the virtual-wan-link zones.

**Suggested Answer:** *C*

*Community vote distribution*

C (100%)

**one_1996** Highly Voted 1 month, 1 week ago

Selected Answer: C

I think the correct answer is c because next to overlay-factories there is a plus symbol

upvoted 6 times

**jajajaf342** Most Recent 3 weeks, 4 days ago

Selected Answer: C

C is correct. You can freely move members between zones.

- overlay-factories does appear to have a member, since it has an expandable menu option - not A
- There's no real way to know how many members the underlay zone contains - not B
- You cannot delete the built-in virtual-wan-link zone - not D

upvoted 1 times

Refer to the exhibits.

**Ping result**

```
root@branch1-client-cli# ping facebook.com
PING facebook.com (157.240.19.35) 56(84) bytes of data.
64 bytes from edge-star-mini-shv-01-dfw5.facebook.com (157.240.19.35):
icmp_seq=1 ttl=56 time=33.4 ms
64 bytes from edge-star-mini-shv-01-dfw5.facebook.com (157.240.19.35):
icmp_seq=2 ttl=56 time=32.5 ms
64 bytes from edge-star-mini-shv-01-dfw5.facebook.com (157.240.19.35):
icmp_seq=3 ttl=56 time=32.5 ms
64 bytes from edge-star-mini-shv-01-dfw5.facebook.com (157.240.19.35):
icmp_seq=4 ttl=56 time=32.6 ms
```

**Diagnose output**

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

id=1(0x1) dscp_tag=0xfc flags=0x0 tos=0x00 tos_mask=0x00 protocol=0
port=src(0->0):dst(0->0) iif=0(any)
path(1): oif=21(HUB1-VPN2)
source(1): 10.0.1.0-10.0.1.255
destination wildcard(1): 10.1.0.7/255.255.255.255
hit_count=0 rule_last_used=2025-01-06 00:41:44

id=2130903041 (0x7f030001) vwl_service=1 (Critical-DIA) vwl_mbr_seq=1 2
dscp_tag=0xfc 0xfc flags=0x0 tos=0x00
tos_mask=0x00 protocol=0 port=src(0->0):dst (0->0) iif=0(any)
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
application control(2): Salesforce(16920,0) Microsoft.Portal (41469,0)
hit_count=13 rule_last_used=2025-01-06 01:55:12

id=2130903042 (0x7f030002) vwl_service=2 (Non-Critical-DIA) vwl_mbr_seq=2
dscp_tag=0xfc 0xfc flags=0x0 tos=0x00
tos_mask=0x00 protocol=0 port=src(0->0):dst (0->0) iif=0(any)
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
application control(3): Facebook(15832, 0), LinkedIn(16331, 0), Game(0, 8)
hit_count=27 rule_last_used=2025-01-06 01:55:12

id=2130903043 (0x7f030003) vwl_service=3 (Corp) vwl_mbr_seq=4 5 6 7 8 9
dscp_tag=0xfc 0xfc flags=0x0 tos=0x00
tos_mask=0x00 protocol=0 port=src(0->0):dst (0->0) iif=0(any)
path(6): oif=20(HUB1-VPN1), oif=21(HUB1-VPN2), oif=22(HUB1-VPN3), oif=23
(HUB2-VPN1), oif=24(HUB2-VPN2), oif=25(HUB2-VPN3),
source(1): 10.0.1.0-10.0.1.255
destination (1): 10.0.0.0-10.255.255.255
hit_count=0 rule_last_used=2025-01-06 00:41:49

id=2130903045 (0x7f030005) vwl_service=5 (Internet) vwl_mbr_seq=3 2
1dscp_tag=0xfc 0xfc flags=0x0 tos=0x00
tos_mask=0x00 protocol=0 port=src(0->0):dst (0->0) iif=0(any)
path(3): oif=6(port4), oif=4(port2) path_last_used=2025-01-06 02:12:08,
oif=3(port1)
source(1): 10.0.1.0-10.0.1.255
destination (1): 10.0.0.0-10.255.255.255
hit_count=27 rule_last_used=2025-01-06 02:12:08
```

**Diagnose output**

```
branch1_fgt # diagnose sys sdwan internet-service-app-ctrl-list
List App Ctrl Database Entry(IPv4) in Kernel:

Max_App_Ctrl_Size=32768 Num_App_Ctrl_Entry=8

Facebook(15832 23): IP=157.240.19.35 6 443

Addicting.Games(30156 8): IP=172.64.80.1 6 443

Microsoft.Portal(41469 28): IP=184.27.181 201 6 443

LinkedId(16331 23): IP=13.107.42.14 6 443

MSN.Game(16135 8): IP=13.107.246.35 6 443

Salesforce(16920 29): IP=32,222.17 73 6 443

Salesforce(16920 29): IP=32,222.17 76 6 443

Facebook(15832 23): IP=31.13.80.36 6 443
```

You connect to a device behind a branch FortiGate device and initiate a ping test. The device is part of the LAN subnet and its IP address is 10.0.1.101.

Based on the exhibits, which interface uses branch1_fgt to steer the test traffic?

A. port4

B. HUB1-VPN1

C. port1

D. port2

**Suggested Answer:** *D*

*Community vote distribution*

D (100%)

**jajajaf342** 3 weeks, 4 days ago

Selected Answer: D

The answer is D.

- The PC is pinging Facebook
- The exhibit showing the 3-tuple of identified applications shows that the IP address being pinged is recognized as Facebook

Therefore, we go top-to-bottom on each SD-WAN rule.

- First rule - not matched due to destination
- Second rule - not matched due to application control parameters
- Third rule - matched by source and application control parameter

The rule states that the only outgoing interface is port2, making D the answer.

upvoted 2 times

**felixcater** 1 month, 1 week ago

Selected Answer: D

D: Port2 in the Paragraph 3 Has Facebook enabled in the Service rule 2.

upvoted 2 times

Question #21 *Topic 1*

What are three key routing principles of SD-WAN? (Choose three.)

A. SD-WAN rules are skipped if the best route to the destination is a static route.

B. SD-WAN members are skipped if they do not have a valid route to the destination.

C. SD-WAN rules are skipped the best route to the destination is not an SD-WAN member.

D. Directly connected routes have precedence over SD-WAN rules.

E. Policy routes have precedence over SD-WAN rules.

**Suggested Answer:** *BCE*

*Community vote distribution*

BCE (100%)

**jajajaf342** 3 weeks, 4 days ago

**Selected Answer: BCE**

BCE are correct.

From page 161 of SD-WAN 7.4 Architect:

Key Routing Principles
1. SD-WAN rules are policy routes
2. Regular policy routes have precedence over SD-WAN rules (E)
3. Route lookup is done for new and dirty sessions
4. SD-WAN rules are skipped if:
- Best route to destination isn't an SD-WAN member (C)
- None of the members have a valid route to the destination (B)
5. Implicit SD-WAN rule equals standard forwarding information base (FIB) lookup.

Therefore, BCE are the correct answers.

upvoted 2 times

**felixcater** 1 month, 1 week ago

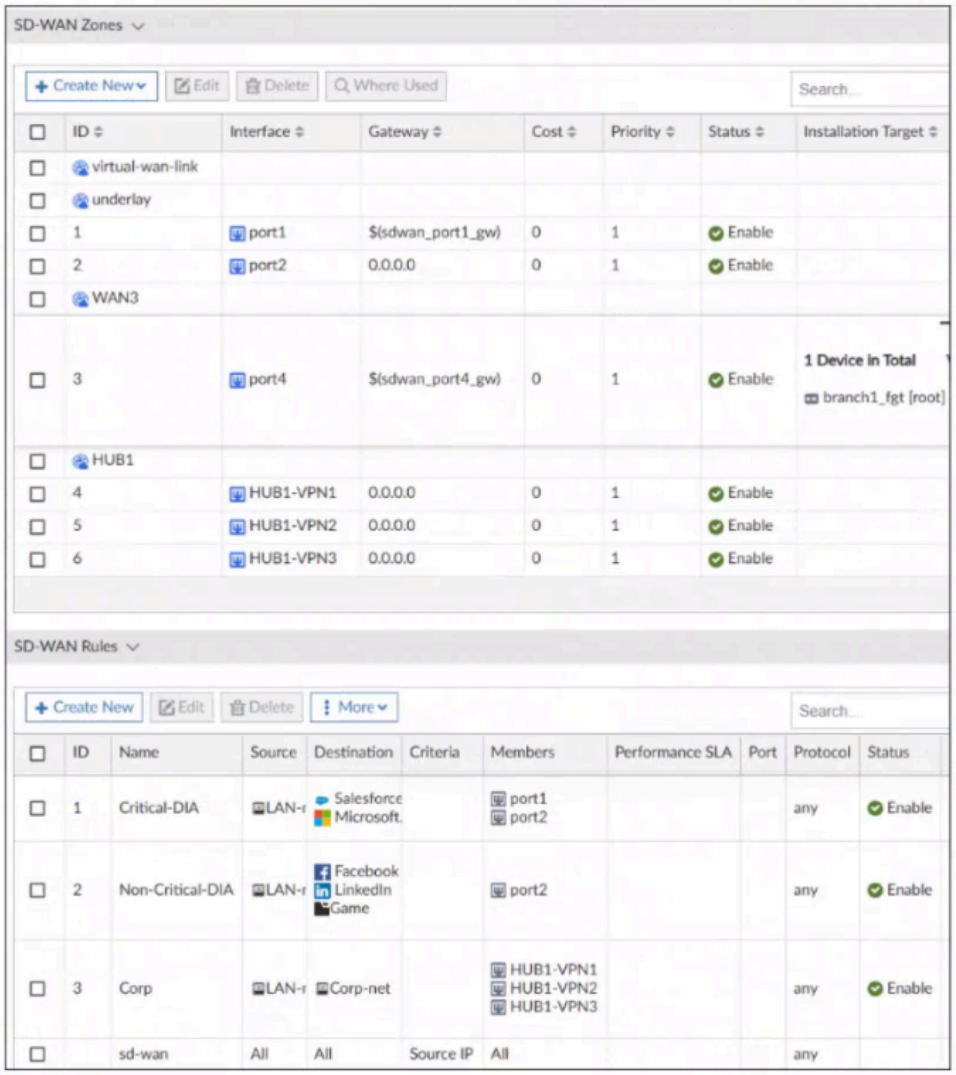
**Selected Answer: BCE**

BCE are correct: BC are correct because these two cases are applicable to implicit rule whenever they are met. Policy routes have precedence over SD-WAN rules.

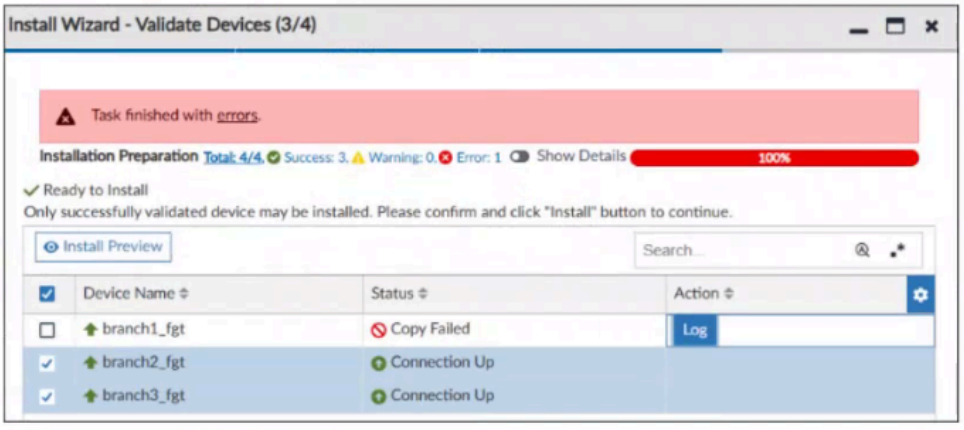
upvoted 1 times

Refer to the exhibits.

**SD-WAN template zones and rules configuration**




**FortiManager error message**




**View Install Log**

```
Copy device global objects

Copy objects for vdom root

Commit failed:
error -999 - - (from Template Group Corp-SOT_Branch) (in Template branches)
invalid ip - prop[gateway]: ip4class($(sdwan_port1_gw)) invalid ip addr
```

You use FortiManager to configure SD-WAN on three branch devices.

When you install the device settings, FortiManager prompts you with the error “Copy Failed” for the device branch1_fgt. When you click the log button, FortiManager displays the message shown in the exhibit.
Based on the exhibits, which statement best describes the issue and how you can resolve it?

A. Remove the installation target for the SD-WAN member porta. You cannot combine metadata variable and installation targets.

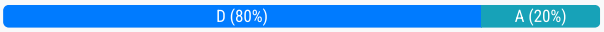
B. Check the connection between branch1_fgt and FortiManager.

C. Gateways for all members in a zone must be defined the same way. Specify the gateway of the SD-WAN member port1 without metadata variables.

D. Check the metadata variable definitions, and review the per-device mapping configuration.

**Suggested Answer:** *D*

*Community vote distribution*




**jajajaf342** 3 weeks, 4 days ago

**Selected Answer: D**

D is the correct answer.

The error relates to an improperly defined metadata variable for $(sdwan_port1_gw). This could mean the definition isn't in an IP address format, or the definition isn't configured properly for the installation target.

If you work with FortiManager regularly, you'll catch these errors frequently.

upvoted 4 times

**felixcater** 1 month, 1 week ago

**Selected Answer: A**

A is correct.

upvoted 1 times

**altres** 1 month ago

Where is this stated and why is the error stating port1 gw? Most likely the MV is not correct.

upvoted 1 times

Question #23 *Topic 1*

You manage an SD-WAN topology. You will soon deploy 50 new branches.
Which three tasks can you do in advance to simplify this deployment? (Choose three.)

A. Create a ZTP template.

B. Define metadata variables value for each device.

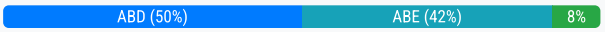
C. Update the DHCP server configuration.

D. Create policy blueprint.

E. Create model devices.

**Suggested Answer:** *ABD*

*Community vote distribution*




**bd46e16** 1 week, 6 days ago

**Selected Answer: BCE**

ZTP not exist
Blueprint policy not exist
B- OK we need variables
C- DHCP option for FMG
E- import 50 model devices by csv
upvoted 1 times

**471dfbf** 3 weeks, 3 days ago

**Selected Answer: ABE**

They are refering to the ZTP templete.. Based on this, page 85 of the PDF says...

After the administrator completes the preparation work, which includes

1. preparing templates,
2. defining blueprints, and
3. loading the model devices with a CSV file,

the ZTP process can start.

I think is ABE
upvoted 1 times

**jajajaf342** 3 weeks, 4 days ago

**Selected Answer: ABD**

This question was not formulated properly. There's no such thing as a "ZTP Template" or a "Policy Blueprint" - there are BGP, CLI, etc. templates, Policy Packages, and Device Blueprints.

Because of this, it's unclear what the intended answer is, but my best guess is ABD.

Refer to page 86 of SD-WAN 7.4 Architect - in the slide, under "Preparation", the list is:
- Define Metadata Variables (B)
- CLI Templates
- IPsec Templates
- BGP Templates (possibly all 3 refer to "ZTP" template?) (A)
- Firewall objects
- SD-WAN Templates
- Policy Packages (D)

C is incorrect, because using DHCP options is not the only way to do ZTP.

E is PROBABLY incorrect because when creating model devices, you do need serial numbers - in this situation, you may not have those on hand yet or know what they are. You could, however, create a device blueprint as part of preparation, but this isn't an available answer.

upvoted 3 times

**altres** 1 month ago

**Selected Answer: ABE**

ABE. We need the Template and atleast the Metadata Variables Name, SN and Device Blueprint which also explains E, the Model Device for the Device Blueprint

upvoted 4 times

**one_1996** 1 month, 1 week ago

**Selected Answer: ABD**

ABD are correct

upvoted 3 times

Question #24 *Topic 1*

Refer to the exhibit.

```
config vpn ipsec phase1-interface
     edit "VPN1"
          set interface "port1"
          set ike-version 2
          set peertype any
          set exchange-interface-ip enable
          set mode-cfg disable
          set proposal aes256-sha256
          …
     end
end
```

The administrator configured the IPsec tunnel VPN1 on a FortiGate device with the parameters shown in exhibit.
Based on the configuration, which three conclusions can you draw about the characteristics and requirements of the VPN tunnel? (Choose three.)

A. The remote end can be a third-party IPsec device.

B. The remote end must support IKEv2.

C. This configuration allows user-defined overlay IP addresses.

D. The tunnel interface IP address on the spoke side is provided by the hub.

E. The administrator must manually assign the tunnel interface IP address on the hub side.

**Suggested Answer:** *BCE*

*Community vote distribution*

BCE (100%)

**471dfbf** 3 weeks, 3 days ago

**Selected Answer: BCE**

Agreed, BCE

Forget about the guide there..

1. When mode-cfg is disabled, there is no exchange of IP address information within the IKE negotiation. A tunnel can exist without IP, but using interface-exchange IP will force you to use a user defined IP address on the interface. This also rules out third party (A can't Be) (C and E match for this)

2. They are using IKEv2 (Clearly defined) ... B

upvoted 1 times

**jajajaf342** 3 weeks, 4 days ago

**Selected Answer: BCE**

Answer is BCE.

Refer to page 263 of SD-WAN 7.4 Architect:

B - both sides must support/use IKEv2

C - "Instead of using IKE mode config to assign addresses automatically, you manually assign the address on the spoke and hub sides..."

E - "Administrator manually assigns the IP address on the spoke and hub sides..."

A is incorrect, since this is Fortinet proprietary extension of IKE

D is incorrect, since the addresses are manually assigned on hub and spoke

upvoted 1 times

**altres** 1 month ago

**Selected Answer: BCE**

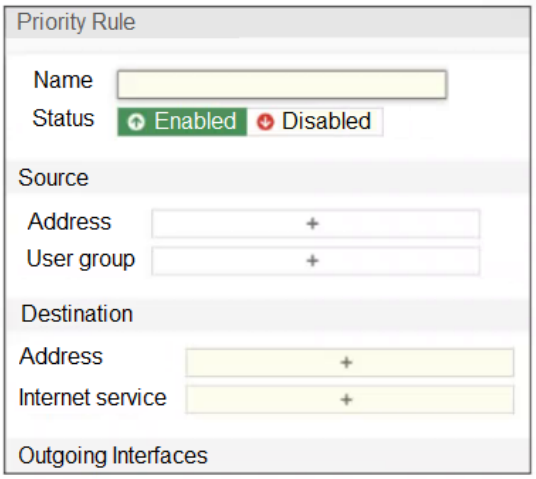
A: No, because Exchange-interface-ip is FNT propietary

D: Also no, you have to manually define the Ip addresses on spoke and hube side

upvoted 1 times

Question #25 *Topic 1*

Refer to the exhibit.




An administrator configures SD-WAN rules for a DIA setup using the FortiGate GUI. The page to configure the source and destination part of the rule looks as shown in the exhibit. The GUI page shows no option to configure an application as the destination of the SD-WAN rule. Why?

A. You must enable the feature first using the GUI menu System > Feature Visibility.

B. FortiGate allows the configuration of applications as the destination of SD-WAN rules only on the CLI

C. You must enable the feature on the CLI.

D. You cannot use applications as the destination when FortiGate is used for a DIA setup.

**Suggested Answer:** *C*

*Community vote distribution*

C (86%) 14%

**7abc0bc** 3 weeks, 6 days ago

**Selected Answer: C**

It could be enabled by GUI in the Feature visibility or by CLI.
But Study Guide P23 mentioned that the Criteria MUST be enabled by CLI, so I will go with Option C

upvoted 3 times

**eaguilera** 4 weeks, 1 day ago

**Selected Answer: A**

Feature Visibility > Application Detection-Based SD-WAN

upvoted 1 times

**fernandosanchez88** 4 weeks, 1 day ago

**Selected Answer: C**

. You must enable feature visibility on the CLI using the global command set gui-app-detection-sdwan enable. Study guide page:23

upvoted 3 times

Question #26 *Topic 1*

Which statement describes FortiGate behavior when you reference a zone in a static route?

A. FortiGate installs a static route for each member in the zone.

B. FortiGate installs ECMP static routes for the first two members of the zone.

C. FortiGate ignores the static routes defined through members referenced in the zone.

D. FortiGate routes the traffic through the best performing member of the zone.

**Suggested Answer:** *A*

*Community vote distribution*

A (100%)

**jajajaf342** 3 weeks, 4 days ago

**Selected Answer: A**

A is correct - tested and verified on my equipment.

B - incorrect, there's nothing special about the first two members of the zone

C - incorrect, static routes defined through members are not ignored

D - incorrect - while this could be true, it isn't in general - for instance, a load-balancing configuration

upvoted 1 times

Question #27 *Topic 1*

An administrator is configuring SD-WAN to load balance their network traffic.
Which two things should they consider when setting up SD-WAN? (Choose two.)

A. Only the manual and best-quality strategies allow SD-WAN load balancing.

B. When applicable, FortiGate load balances the traffic through all members that meet the SLA target.

C. You can select the outbandwidth hash mode with all strategies that allow load balancing.

D. SD-WAN load balancing is possible only using the best quality and lowest cost (SLA) strategies.

**Suggested Answer:** *BC*

Currently there are no comments in this discussion, be the first to comment!

Question #28 *Topic 1*

You have a FortiGate configuration with three user-defined SD-WAN zones and two members in each of these zones. One SD-WAN member is no longer in use in health-check and SD-WAN rules. You want to delete it.
What happens if you delete the SD-WAN member from the FortiGate GUI?

A. FortiGate displays an error message. SD-WAN zones must contain at least two members.

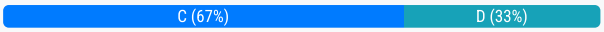
B. FortiGate displays an error message. You must use the CLI to delete an SD-WAN member.

C. FortiGate accepts the deletion and removes routes as required.

D. FortiGate accepts the deletion and paces the member in the default SWAN zone.

**Suggested Answer:** *C*

*Community vote distribution*




**471dfbf** 3 weeks, 2 days ago

**Selected Answer: D**

I just tested in the lab, version 7.4.4
I had a member part of the WAN3 zone, I went to the GUI, SDWAN Members, select UNDERLAY and delete PORT1 part of the underlay. Port 1 now is part of the default 'virtual-wan-link'

Ping the address in that rule, and still routes on the port that now belongs on the underlay.

Option C is not correct. The route is NOT removed.
branch2_fgt # diag sys sdwan service4

Service(1): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
Tie break: cfg
Shortcut priority: 2
Gen(1), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(sla), sla-compare-order
Members(2):
1: Seq_num(1 port1 virtual-wan-link), alive, sla(0x1), gid(0), cfg_order(0), local cost(0), selected <<<----- PORT1 REMOVED FROM WAN3 ZONE
2: Seq_num(2 port2 WAN3), alive, sla(0x1), gid(0), cfg_order(1), local cost(0), selected
Src address(1):
10.0.2.0-10.0.2.255

Dst address(1):
4.2.2.2-4.2.2.2
108.081158 port5 in 10.0.2.101 -> 4.2.2.2: icmp: echo request
108.081730 port1 out 192.2.0.100 -> 4.2.2.2: icmp: echo request <<-- -Packet exists port1
upvoted 1 times

**jajajaf342** 3 weeks, 4 days ago

**Selected Answer: C**

C is correct (tested on my FortiGate). You are free to delete an interface as an SD-WAN member.

A - SD-WAN zones can contain 0, 1, 2, etc. members, so this is false
B - use of the CLI is not required
D - when you delete a member, it cannot be added to a zone, and therefore it would not be placed in the default virtual-wan-link zone.
upvoted 2 times

Question #29 *Topic 1*

Refer to the exhibits.

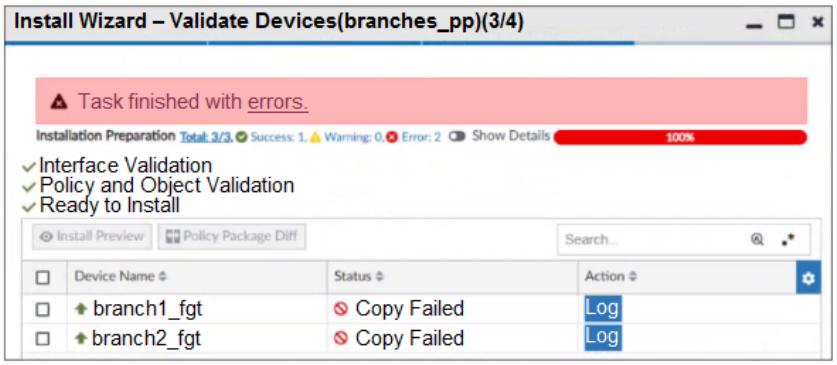
**SD-WAN template on FortiManager**

| Name | Assigned to Device/Group | Interface |
|---|---|---|
| branches | 2 Devices in Total View Details > branch1_fgt [root] branch2_fgt [root] | port1 port2 |

**Firewall policies**

| Underlay (2/3 Total:2) | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 2 | SIA | LAN | port1 | LAN-net | all | always | FTP HTTP HTTPS | Accept | no-inspection default |
| 3 | DIA | LAN | underlay | LAN-IT | all | always | ALL | Accept | default certificate-i... default |

**FortiManager error message**




You use FortiManager to manage the branch devices and configure the SD-WAN template. You have configured direct internet access (DIA) for the IT department users. Now, you must configure secure internet access (SIA) for all local LAN users and have set the firewall policies as shown in the second exhibit.

Then, when you use the install wizard to install the configuration and the policy package on the branch devices, FortiManager reports an error as shown in the third exhibit.

Which statement describes why FortiManager could not install the configuration on the branches?

A. You must direct SIA traffic to a VPN tunnel.

B. You cannot install SIA and DIA rules on the same device.

C. You cannot install firewall policies that reference an SD-WAN member.

D. You cannot install firewall policies that reference an SD-WAN zone.

**Suggested Answer:** *C*

*Community vote distribution*

C (75%) A (25%)

**jajajaf342** 3 weeks, 4 days ago

C is correct. You cannot reference an SD-WAN member in a firewall policy.

upvoted 4 times

**eaguilera** 3 weeks, 6 days ago

**Selected Answer: C**

The error is because PORT1 is associated with an SD-WAN zone, and is also associated with an access policy.

upvoted 4 times

**one_1996** 1 month, 1 week ago

**Selected Answer: A**

SIA traffic (traffic meant to go through Fortinet's Secure Internet Access cloud) must always be sent through a VPN tunnel to the SIA service.

SIA cannot be reached directly via a normal Internet interface; the traffic is encapsulated in an IPsec tunnel from the FortiGate to the SIA cloud.
upvoted 1 times

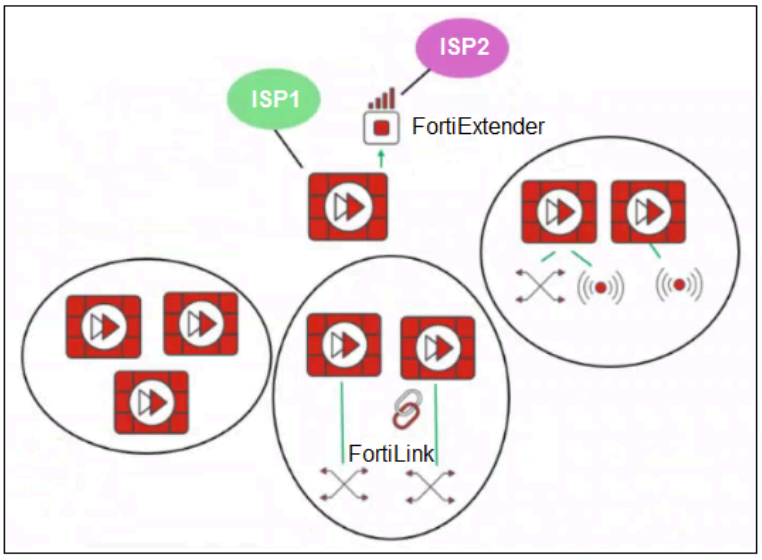
**altres** 1 month ago

In theory you are correct. But this wouldn't prevent the installation. It is more likely, that port1 is referenced as an SD-WAN Member. You cannot use SD WAN Member directly in a Firewallpolicy. Answer should be C
upvoted 3 times

Question #30 *Topic 1*

Refer to the exhibit.

**SD-WAN Network Topology**




You want to configure SD-WAN on a network as shown in the exhibit.

The network contains many FortiGate devices. Some are used as NGFW, and some are installed with extensions such as FortiSwitch, FortiAP, or FortiExtender.

What should you consider when planning your deployment?

A. You can build an SD-WAN topology that includes all devices. The hubs can be FortiGate devices with FortiExtender.

B. You must use FortiManager to manage your SD-WAN topology.

C. You can build an SD-WAN topology that includes all devices. The hubs must be devices without extensions.

D. You must build multiple SD-WAN topologies. Each topology must contain only one type of extension.

**Suggested Answer:** *A*

*Community vote distribution*

A (100%)

**jajajaf342** 3 weeks, 4 days ago

**Selected Answer: A**

A is correct - you can include FortiGates with FortiExtender.

B - incorrect, you do not need FortiManager to configure SD-WAN

C - incorrect, extensions (e.g. FortiExtender) are fine

D - incorrect, you can have a single SD-WAN topology

upvoted 1 times

Refer to the exhibits.

**Global System configuration**

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

**Interface port2 configuration**

```
config system interface
     [...]
     edit "port2"
          set vdom "root"
          set mode dhcp
          set type physical
          set snmp-index 2
     next
     [...]
```

**Routing Table on FortiGate**

```
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]

...
```

The exhibits show the source NAT (SNAT) global setting, port2 interface settings, and the routing table on FortiGate.

The administrator increases the member priority on port2 to 20.

Upon configuration changes and the receipt of new packets, which two actions does FortiGate perform on existing sessions established over port2? (Choose two.)

A. FortiGate updates the gateway information of the sessions with SNAT so that they use port1 instead of port2.

B. FortiGate continues routing all existing sessions over port2.

C. FortiGate routes only new sessions over port2.

D. FortiGate flags the SNAT session as dirty only if the administrator has assigned an IP pool to the firewall policies with NAT.

E. FortiGate flags the sessions as dirty.

**Suggested Answer:** *AE*

Currently there are no comments in this discussion, be the first to comment!

Question #32 *Topic 1*

Refer to the exhibit.

| Serial Number | name | branch_id | admin_gw | sdwan_port1_gw | sdwan_port2_gw | latitude | longitude | lan_interface_ip |
|---|---|---|---|---|---|---|---|---|
| FGVM01TM22000077 | branch1_fgt | 1 | 172.16.0.2 | 192.2.0.2 | 192.2.0.10 | 37.37610911 | -122.0260914 | 10.0.1.254 |
| FGVM01TM22000078 | branch2_fgt | 2 | 172.16.0.10 | 203.0.11.2 | 203.0.113.10 | 25.77404351 | -80.20508525 | 10.0.2.254 |
| FGT40FTK20000624 | shop1_fgt | 11 | | 198.0.1.1 | | | | 10.10.1.254 |
| FGT40FTK20003026 | shop2_fgt | 12 | | | | 48.88941 | 2.25125 | 10.10.2.254 |
| FGVM02TM24010735 | | 3 | 172.16.0.10 | 100.64.33.2 | 100.64.33.10 | 45.32482 | -75.8359 | 10.0.3.254 |

For your ZTP deployment, you review the CSV file shown in exhibit and note that it is missing important information.

Which two elements must you change before you can import it into FortiManager? (Choose two.)

A. You must associate a device blueprint with each device.

B. You must define a value for each device and each metadata variable that defines an IP address.

C. You must define a value for each device and each user-defined metadata variable.

D. You must define a name for each device.

**Suggested Answer:** *AD*

*Community vote distribution*

AD (67%) BD (17%) CD (17%)

**3101a6a** Highly Voted 1 month ago

Selected Answer: AD

Page 90 of the study guide states:

The file must contain some mandatory values, such as device serial numbers, device names, and associated blueprints.

The image doesn't show the device_blueprint tab, and the last device doesn't have a name.

So, for me, the answer is A and D.

A. You must associate a device blueprint with each device.

D. You must define a name for each device.

upvoted 5 times

**altres** Most Recent 1 month ago

Selected Answer: AD

It is AD as 3101a6a stated. Name,SN and Blueprint are required.

upvoted 3 times

**jajajaf342** 1 month, 1 week ago

Selected Answer: BD

The answer is BD - from the SD-WAN 7.4 Architect, Page 90:

"The first columns must be: serial number, device blueprint, name and, for VMs, vm_interface_number"

upvoted 2 times

**jajajaf342** 3 weeks, 4 days ago

I meant AD on this not BD lol

upvoted 1 times

**one_1996** 1 month, 1 week ago

Selected Answer: CD

The name is required.

All metadata has no default value, so the user-defined value is required.

upvoted 2 times

**jajajaf342** 1 month, 1 week ago

Wrong - metadata variables can absolutely have no user-defined value (and use the default value in the metadata variable definition).

The answer is BD - from the SD-WAN 7.4 Architect, Page 90:

"The first columns must be: serial number, device blueprint, name and, for VMs, vm_interface_number"

As you noted, "name" is required, but the CSV in the screenshot has no Device Blueprint column, hence this is the second missing piece of information.

upvoted 2 times

Question #33 *Topic 1*

When you use the command diagnose sys session list, how do you identify the sessions that correspond to traffic steered according to SD-WAN rules?

A. You identify sessions steered according to SD-WAN rules with the data vwl_mbr_seq.

B. You identify sessions steered according to SD-WAN rules with the data sdwan_service_id.

C. You cannot identify SD-WAN sessions. You must use the sdwan session filter.

D. You identify sessions steered according to SD-WAN rules with the flag vwl.

**Suggested Answer:** *B*

Currently there are no comments in this discussion, be the first to comment!

Question #34 *Topic 1*

Refer to the exhibit.

**Diagnose output**

```
fgt_A # diagnose sys sdwan service4

Service(1): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
     Tie break: cfg
     Shortcut priority: 2
      Gen(8), TOS(0x0/0x0), Protocol(0): src(1->65535), Mode(sla), sla-compare-order
      Members(3):
          1: Seq_num(4 HUB1-VPN1 HUB1), alive, sla(0x1), gid(0), cfg_order(0), local cost(0), selected
          2: Seq_num(6 HUB1-VPN3 HUB1), alive, sla(0x1), gid(0), cfg_order(1), local cost(0), selected
          3: Seq_num(5 HUB1-VPN2 HUB1), alive, sla(0x1), gid(0), cfg_order(2), local cost(0), selected
     Src address(1):
          10.0.1.0-10.0.1.255

fgt_A # diagnose sys sdwan member | grep HUB1
Member(4): transport-group: 0, interface: HUB1-VPN1, flags=0xd may_child, gateway: 100.64.1.1, peer:
192.168.1.29, source 192.168.1.1, priority: 15 1024, weight: 0
Member(5): transport-group: 0, interface: HUB1-VPN2, flags=0xd may_child, gateway: 100.64.1.9, peer:
192.168.1.61, source 192.168.1.33, priority: 10 1024, weight: 0
Member(6): transport-group: 0, interface: HUB1-VPN3, flags=0xd may_child, gateway: 172.16.1.5, peer:
192.168.1.93, source 192.168.1.65, priority: 1 1024, weight: 0

fgt_A # get router info routing-table all | grep HUB1
S          10.0.0.0/8 [10/0] via HUB1-VPN3 tunnel 172.16.1.5, [1/0]
B          10.0.3.0/24 [200/0] via 192.168.1.2 [3] (recursive is directly connected, HUB1-VPN1), 04:11:41,
[1/0]
                       [200/0] via 192.168.1.34 [3] (recursive is directly connected, HUB1-VPN2), 04:11:41,
[1/0]
B          10.1.0.0/24 [200/0] via 192.168.1.29 (recursive via HUB1-VPN1 tunnel 100.64.1.1), 04:11:42. [1/0]
                       [200/0] via 192.168.1.61 (recursive via HUB1-VPN2 tunnel 100.64.1.9), 04:11:42. [1/0]
                       [200/0] via 192.168.1.93 (recursive via HUB1-VPN3 tunnel 172.16.1.5), 04:11:42. [1/0]
```

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 HUB1-VPN1.

However, the traffic is routed over HUB1-VPN3.

Based on the output shown in the exhibit, which two reasons, individually or together, could explain the observed behavior? (Choose two.)

A.HUB1.VPN3 has a higher member configuration priority than HUB1-VPN1.

B. The traffic matches a regular policy route configured with HUB1-VPN3 as the outgoing device.

C. HUB1-VPN3 has a lower route priority value (higher priority) than HUB1-VPN1.

D. HUB1-VPN1 does not have a valid route to the destination.

**Suggested Answer:** *BD*

*Community vote distribution*

BD (58%) CD (33%) 8%

**471dfbf** 3 weeks ago

**Selected Answer: D**

For me, the only option is Option D (This question is not framed correctly)

A --- You can't compare other member priorities - diag sys sdwan member could have given this information. Or if you had another static routes using other ports in the same zone

B -- This can't be as you don't have information on PBR routes - diag firewall proute list could be a source of info for this.

C-- If CFG-ORD can be interpreted as priority criteria, then this might be ok... However, on the PDF there is no indication that this is the case. "it's a tie-breaker'

upvoted 1 times

**7abc0bc** 3 weeks, 5 days ago

**Selected Answer: BD**

Hi,

For me, option C is not correct because it mentions the priority of each member, but this priority only affects when you configure a Static route using the SD-WAN Zone, and this is not the case.

Regarding Option B you have other more specific routes, and those could be used with a Policy Route that takes precedence over the SDWAN Rule.
upvoted 2 times

**eaguilera** 3 weeks, 6 days ago

**Selected Answer: BD**

presents a specific route to the network 10.0.0.0/8 HUB1-VPN3
upvoted 2 times

**one_1996** 1 month, 1 week ago

**Selected Answer: CD**

I'm correcting myself, the correct answer is cd. There is no evidence of the existence of a policy route from the diag commands above.
upvoted 4 times

**7abc0bc** 3 weeks, 5 days ago

Hi,
For me, option C is not correct because it mentions the priority of each member, but this priority only affects when you configure a Static route using the SD-WAN Zone, and this is not the case.

Regarding Option B you have other more specific routes, and those could be used with a Policy Route that takes precedence over the SDWAN Rule.
upvoted 1 times

**one_1996** 1 month, 1 week ago

**Selected Answer: BD**

the correct answers are B D
upvoted 3 times

Question #35 *Topic 1*

You are tasked with configuring ADVPN 2.0 on an SD-WAN topology already configured for ADVPN.
What should you do to implement ADVPN 2.0 in this scenario?

A. Delete the existing ADVPN configuration and configure ADVPN 2.0.

B. Update the IPsec tunnel configurations on the hub.

C. Update the IPsec tunnel configuration on the breaches.

D. Update the SD-WAN configuration on the branches.

**Suggested Answer:** *D*

*Community vote distribution*

D (100%)

**jajajaf342** Highly Voted 1 month, 1 week ago

**Selected Answer: D**

Given answer is incorrect. The answer is D.

From SD-WAN 7.4 Architect, page 382:

"To adjust the configuration for ADVPN 2.0:
- Edit the SD-WAN template...
- IPsec templates: No changes required..."

Therefore, the configuration changes occur with the SD-WAN configuration and not the IPsec configuration.
upvoted 5 times

Question #36 *Topic 1*

Refer to the exhibit.

```
config system sdwan
     set fail-detect enable
     set fail-alert-interfaces "port5"
     config health-check
          edit "Level3_DNS"
               set update-cascade-interface enable
               set members 1 2
          next
          edit "HQ"
               set update- cascade-interface enable
               set members 3
          next
     end
end
```

Which action will FortiGate take if it detects SD-WAN members as dead?

A. FortiGate bounces port5 after it detects all SD-WAN members as dead.

B. FortiGate fails over to the secondary device after it detects port5 as dead.

C. FortiGate sends alert messages through port5 when it detects all SD-WAN members as dead.

D. FortiGate brings down port5 after it detects all SD-WAN members as dead.

**Suggested Answer:** *D*

*Community vote distribution*

D (100%)

**jajajaf342** 1 month, 1 week ago

Selected Answer: D

As is common with this exam, the given answer is incorrect - the real answer is D.

The cascade interface port5 will shutdown in order to force traffic behind it in order to (potentially) find a different route.

Source: https://community.fortinet.com/t5/FortiGate/Technical-Tip-Functionality-of-set-update-cascade-interface/ta-p/193015

upvoted 3 times

**felixcater** 1 month, 1 week ago

Selected Answer: D

Dis correct. Fortigate brings down port5 when it detected that all members are dead.

upvoted 1 times

**one_1996** 1 month, 1 week ago

Selected Answer: D

this answer is D

upvoted 1 times

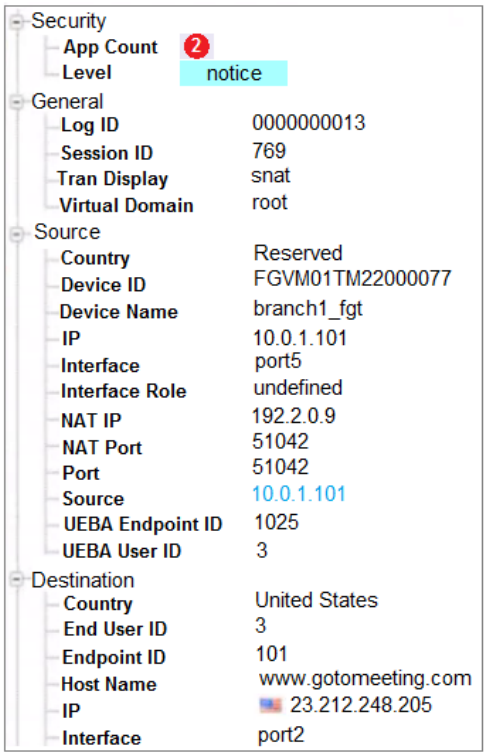
Refer to the exhibits.

**SD-WAN service details**

```
branch_fgt # diagnose sys sdwan service4

Service(1): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(2), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode
(manual)
  Members(2):
     1: Seq_num(1 port1 underlay), alive selected
     2: Seq_num(2 port2 underlay), alive selected
 Application Control(3): Microsoft.Portal(41469,0) Salesforce(16920,0)
Collaboration(0,28)
 Src address(1):
10.0.1.0-10.0.1.255

Service(2): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(2), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode
(manual)
  Members(1):
     1: Seq_num(2 port2 underlay), alive selected
     Application Control(3): Facebook(15832,0) LinkedIn(16331,0) Game(0,8)
 Src address(1):
10.0.1.0-10.0.1.255

branch_fgt # diagnose sys sdwan internet-service-app-ctrl-list
List App Ctrl Database Entry(IPv4) in Kernel:

Max_App_Ctrl_Size=32768 Num_App_Ctrl_Entry=6

Microsoft.Portal (41469 28): IP=184.27.181.201 6 443
MSN.Game(16135 8): IP=13.107.246.36 6 443
Salesforce(16920 29): IP=23.205.255.92 6 443
GoToMeeting (16354 28): IP=23.205.106.86 6 443
GoToMeeting (16354 28): IP=23.212.249.144 6 443
Facebook(15832 23): IP=31.13.80.36 6 443

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]
…
```

**GoToMeeting traffic log on FortiAnalyzer**

| Destination IP | Service | Application | Security Event List | SD-WAN Rule Name | Destination Interface |
|---|---|---|---|---|---|
| 23.212.248.205 | HTTPS | GoToMeeting | APP 2 | | 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 | | port2 |
| 23.205.106.86 | HTTPS | GoToMeeting | APP 2 | | port2 |




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

After generating GoToMeeting test traffic, the administrator examined the corresponding traffic log on FortiAnalyzer, which is shown in the second exhibit.

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 some log messages show that the traffic matched the implicit SD-WAN rule? (Choose two.)

A. The session 3-tuple did not match any of the existing entries in the ISDB application cache.

B. FortiGate could not refresh the routing information on the session after the application was detected.

C. Full SSL inspection is not enabled on the matching firewall policy.

D. No configured SD-WAN rule matches the traffic related to the collaboration application GoToMeeting.

**Suggested Answer:** *AB*

*Community vote distribution*

AB (100%)

**jajajaf342** 3 weeks, 1 day ago

**Selected Answer: AB**

The answer is AB - see SD-WAN 7.4 Architect page 221:

A - "...a session may match an unexpected rule and member when the session 3-tuple doesn't have an entry in the ISDB application cache, or when the session 3-tuple has an entry in the ISDB application cache, but the detected application is different."

B - "That is, if a session is subject to SNAT, then, by default, FortiGate doesn't flush the routing information of the session after the application is detected—the session is not flagged as dirty" - i.e. this particular could remain routing out of port1, though subsequent sessions will route over port2.

C is incorrect, because while this COULD be the case, we see that app control for GoToMeeting is working correctly - in other words, GoToMeeting is an application that can be detected without full SSL inspection.

D is incorrect, because clearly GoToMeeting matches the Collaboration category (since we can see traffic matching the SD-WAN rule)

upvoted 1 times

**3101a6a** 1 month ago

**Selected Answer: AB**

AB are correct

upvoted 2 times