



CERTIFICATION TEST

-CertificationTest.net - Cheap & Quality Resources With Best Support

Question #1

Topic 1

In the context of SD-WAN, the terms underlay and overlay are commonly used to categorize links.

Which two statements about underlay and overlay links are correct? (Choose two.)

- A. Overlay links provide routing flexibility.
- B. Only wired connections can be used as underlay links.
- C. A VLAN is a type of overlay link.
- D. FortiLink interface is considered an underlay link.
- E. Wireless connections can be used to build overlay links.

Suggested Answer: A, E

 **Expressif** Most Recent 1 month, 2 weeks ago

Selected Answer: A,E

Overlay links provide routing flexibility by creating logical connections over one or more physical transport networks. In SD-WAN, they allow traffic to be steered across available underlay paths according to policies, performance, and reachability. Wireless connections can serve as transport for building overlay links, just as wired Internet, MPLS, or cellular links can. Underlay links are not limited to wired connections, and a VLAN is a Layer 2 segmentation mechanism rather than an SD-WAN overlay link.

upvoted 2 times

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 accepts the SD-WAN member deletion with no further action.
- B. FortiGate displays an error message. SD-WAN zones must contain at least two members.
- C. FortiGate accepts the deletion and removes static routes as required.
- D. FortiGate accepts the deletion and places the member in the default SD-WAN zone.

Suggested Answer: A

 **Expressif** Most Recent 1 month, 2 weeks ago

Selected Answer: A

FortiGate allows an unused SD-WAN member to be deleted directly from the GUI. Because the member is not referenced by health checks or SD-WAN rules, no dependent configuration needs to be changed before removal. User-defined SD-WAN zones are not required to retain two members, so the deletion succeeds without an error or automatic reassignment to the default zone.

upvoted 1 times

Refer to the exhibits.

An OSPF peer is advertising route 172.16.52.0/24. The local FortiGate is configured with an inbound distribution list that allows the 172.16.0.0/14 network to be injected into its routing table. However, the 172.16.52.0/24 subnet cannot be seen in the FIB.

Which two steps can the administrator of the local FortiGate take to ensure that the advertised 172.16.52.0/24 subnet will be injected into the routing table? (Choose two.)

OSPF configuration

```
FGT # show router ospf
config router ospf
  set router-id 0.0.0.113
  set distribute-list-in "Allow-172.16"
  config area
    edit 0.0.0.0
  ---omitted---
end
```

Prefix-list configuration

```
FGT # show router prefix-list
config router prefix-list
  edit "Allow-172.16"
  config rule
    edit 1
      set prefix 172.16.0.0 255.255.0.0
      unset ge
      unset le
  ---omitted---
end
```

- A. Modify the default prefix-list behavior from implicit deny to implicit allow.
- B. Change the ge value to 17.
- C. Add another entry to the prefix list to specifically allow the 172.16.52.0/24 network.
- D. Change the le value to 16.

Suggested Answer: B, C

 **Expressif** Most Recent 1 month, 2 weeks ago

Selected Answer: B,C

The prefix-list entry matches only the exact 172.16.0.0/16 prefix when both ge and le are unset, so it does not permit the advertised 172.16.52.0/24 route. Setting ge to 17 allows more-specific prefixes longer than /16, including the /24 advertisement. Alternatively, a separate prefix-list entry can explicitly permit 172.16.52.0/24.

upvoted 1 times

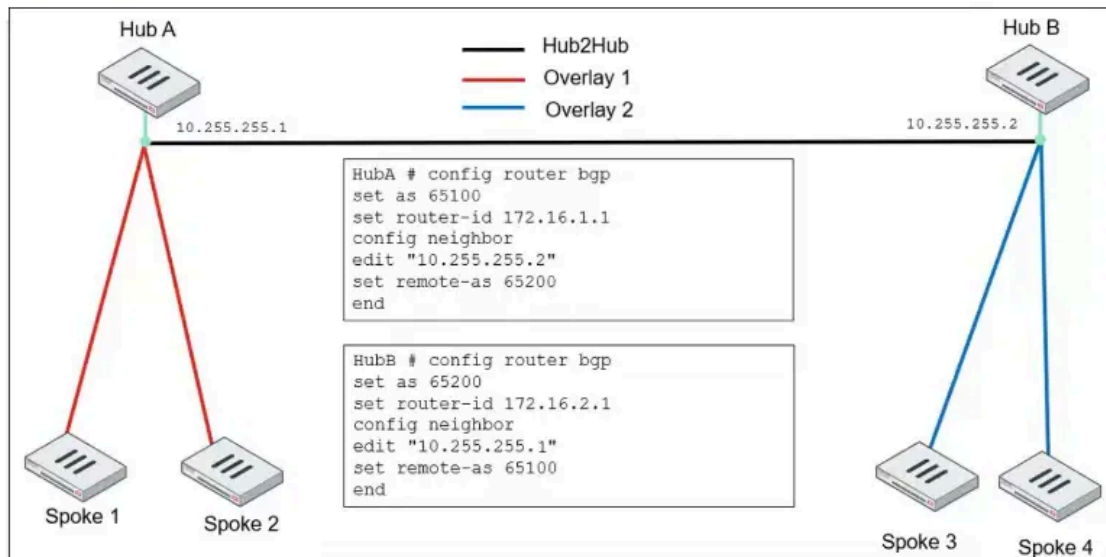
Refer to the exhibit.

An ADVPN network is shown.

You must configure an ADVPN using IBGP for each local region and EBGp across regions to connect Overlay 1 with Overlay 2.

Which two options must you configure in the Hub2Hub BGP peering? (Choose two.)

Network topology



- A. set. ebgp-enforce-multihop enable
- B. set. ibgp-enforce-multihop advpn
- C. set. attribute-unchanged next-hop
- D. set. next-hop-self enable

Suggested Answer: A, C

Expressif Most Recent 1 month, 2 weeks ago

Selected Answer: A,C

The Hub2Hub EBGp peer uses loopback-style overlay addresses rather than directly connected physical interface addresses, so ebgp-enforce-multihop must be enabled to allow the BGP session across the tunnel path. Attribute-unchanged next-hop preserves the original BGP next-hop when routes are advertised between the hubs. This allows ADVPN shortcut routing to retain the reachable overlay next-hop instead of replacing it with the advertising hub. The IBGP-specific multihop setting does not apply to this inter-region EBGp peering.

upvoted 1 times

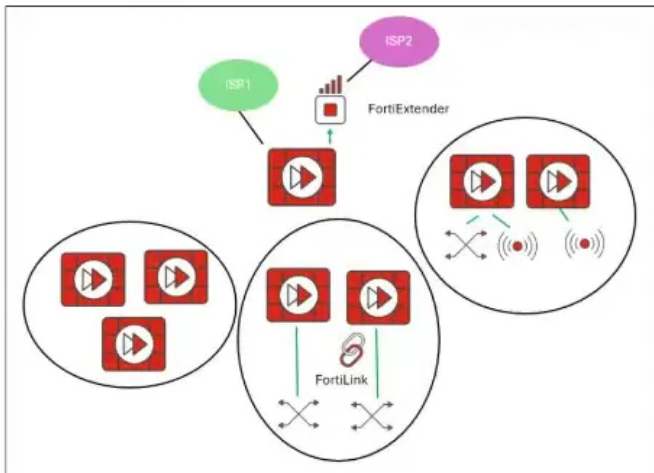
Refer to the exhibit.

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

The network contains many FortiGate devices. Some are used as next-generation firewalls (NGFW), and some are installed with extensions such as FortiSwitch, FortiAP, or FortiExtender.

Which factors should you consider when planning your deployment?

SD-WAN Network Topology



- A. You should exclude the FortiGate devices with FortiLink connection from the SD-WAN topology.
- B. You should build multiple SD-WAN topologies. Each topology should contain only one type of extension.
- C. You can build an SD-WAN topology that includes all devices. The hubs can be FortiGate devices with FortiExtender.
- D. You can build an SD-WAN topology that includes all devices. The hubs must be devices without extensions.

Suggested Answer: C

orion_son30 Most Recent 1 month, 1 week ago

Selected Answer: C

I think C is correct. I don't see any reason to not be possible to use Extender on the Hub.

upvoted 3 times

Refer to the exhibit.

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.)

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

- A. You must define a name for each device.
- B. You must define a value for each device and each user-defined metadata variable.
- C. You must associate a device blueprint with each device.
- D. You must define a value for each device and each metadata variable that defines an IP address.

Suggested Answer: A, C

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

Which two troubleshooting steps should you perform if you encounter issues with intermittent web filter behavior? (Choose two.)

- A. Check that the inspection mode configured for the web filter profile matches that of the firewall policy where it is applied.
- B. Check that the correct port is mapped to HTTP in the Protocol Options.
- C. Check that the communication between FortiGate and FortiGuard is stable.
- D. Check that FortiGate is not entering conserve mode.

Suggested Answer: *C, D*

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

Refer to the exhibit.

The output of diagnose sys session list command is shown.

If the HA ID for the primary device is 0, what happens if the primary fails and the secondary becomes the primary?

Diagnose output

```
# diagnose sys session list
session info: proto=6 proto_state=01 duration=73 expire=3597 timeout=3600
flags=00000000 sockflag=00000000 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=may_dirty synced none app_ntf
statistic (bytes/packets/allow_err): org=822/11/1 reply=9037/15/1 tuples=2
origin->sink: org pre->post, reply pre->post dev=4->2/2->4
gwy=100.64.1.254/10.0.1.10
hook=post dir=org act=snat 10.0.1.10:65464->54.192.15.182:80 (100.64.1.1:65464)
hook=pre dir=reply act=dnat 54.192.15.182:80->100.64.1.1:65464 (10.0.1.10:65464)
pos/ (before, after) 0/ (0,0), 0/ (0,0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00000098 tos=ff/ff ips view=0 app_list=0 app=0
dd_type=0 dd_mode=0
```

- A. The session state is preserved but the kernel will re-evaluate the session because the routing information will be flushed.
- B. The session is synchronized with the secondary device, however, because application control is applied, the session is marked dirty and has to be re-evaluated after failover.
- C. The session will be removed from the session table of the secondary device because the TCP session is not yet fully established.
- D. The session continues to permit traffic on the new primary device after failover, without requiring the client to restart the session with the server.

Suggested Answer: D

👤 86024a2 Most Recent 1 week ago

Selected Answer: C

Probably C because proto_state is 01 and unestablished tcp sessions are not synced
upvoted 1 times

Refer to the exhibit.

How does FortiGate handle the traffic with the source IP address 10.0.1.125 and the destination IP address 128.66.0.125?

FortiGate Diagnose Output

```
branch1_fgt # 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), health-check(Corp_HC)
Members(2):
  1: Seq_num(2 port2 underlay), alive, latency: 0.971, selected
  2: Seq_num(1 port1 underlay), alive, latency: 1.170, selected
Application Control(3): Salesforce(16920,0) Microsoft.Portals(41469,0) Microsoft.Outlook(15816,0)

Src address(1):
  10.0.1.0-10.0.1.255

Service(2): Address Mode(IPV4) flags=0x24200 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(2):
  1: Seq_num(3 port7 SiteA), alive, sla(0x1), gid(2), num of pass(1), selected
  2: Seq_num(4 port8 SiteA), alive, sla(0x1), gid(2), num of pass(1), selected
Src address(1):
  10.0.1.0-10.0.1.255
Dst address(1):
  128.66.0.0-128.66.255.255
```

FortiGate Routing Table

```
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
       V - BGP VPNv4
       * - candidate default

Routing table for VRF=0
S*    0.0.0.0/0 [5/0] via 192.2.0.2, port1, [1/0]
      [5/0] via 192.2.0.10, port2, [1/0]
C     10.0.1.0/24 is directly connected, port7
      is directly connected, port8
C     10.0.2.0/24 is directly connected, port5
S     172.16.0.0/16 [10/0] via 172.16.0.2, port4, [1/0]
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
```

- A. FortiGate routes the traffic flow according to the forwarding information base (FIB).
- B. FortiGate drops the traffic flow.
- C. FortiGate steers the traffic flow through port7.
- D. FortiGate load balances the traffic flow through port7 and port8.

Suggested Answer: D

 **blueji** Most Recent 3 weeks ago

Selected Answer: A

The default route points to port1 and port2. However, Service(2) in the SD-WAN configuration uses members port7 and port8. Since the best route to the destination (via the default route) does not point to an SD-WAN member (port7 or port8), the SD-WAN rule is skipped.

upvoted 2 times

You use the FortiManager SD-WAN overlay orchestrator to prepare an SD-WAN deployment. Using information provided through the SD-WAN overlay template wizard, FortiManager creates templates that are ready to install on the spoke and hub devices.

Which three templates are created by the SD-WAN overlay orchestrator for a spoke device? (Choose three.)

- A. CLI template
- B. Static route template
- C. Rules template
- D. BGP template
- E. IPsec tunnel template

Suggested Answer: A, D, E

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

In which order does FortiGate consider the following elements during the route lookup process?

- A. SD-WAN rules, policy routes, static routes, ISDB routes
- B. Policy routes, ISDB routes, SD-WAN rules, static routes
- C. Policy routes, SD-WAN rules, Internet Service Database (ISDB) routes, BGP routes
- D. SD-WAN rules, ISDB routes, policy routes, BGP routes

Suggested Answer: B

AI-derived guidance: Policy routes precede ISDB routes, SD-WAN rules, and routing-table routes.

🗉 **haiderzaid** Most Recent 1 month, 1 week ago

Selected Answer: C

C

<https://docs.fortinet.com/document/fortigate/8.0.0/administration-guide/144044/policy-routes>

upvoted 1 times

🗉 **orion_son30** Highly Voted 1 month, 1 week ago

Selected Answer: B

I think it's B. Route lookup can be checked on the following links:

<https://community.fortinet.com/fortigate-3/technical-tip-routing-in-fortigate-route-lookup-process-96148>

<https://community.fortinet.com/fortigate-3/troubleshooting-tip-understanding-route-prioritization-in-fortigate-a-comprehensive-guide-with-troubleshooting-commands-206870>

upvoted 5 times

While troubleshooting a FortiGate web filter issue, users report that they cannot access any websites, even though those sites are not explicitly blocked by any web filter profiles that are applied to firewall policies.

What are the three most likely reasons for this behavior? (Choose three.)

- A. The SSL/TLS deep inspection was configured but the browsers do not have the FortiGate certificate installed.
- B. The web filter cache has been cleared causing all websites to take longer to be rated.
- C. The DNS server is unreachable, preventing URL resolution.
- D. The webfilter-force-off setting has been enabled under config system fortiguard.
- E. The FortiGuard Web Filtering license has expired, causing FortiGate to apply the default block action.

Suggested Answer: A, C, E

AI-derived guidance: Inspection certificates, DNS resolution, and FortiGuard licensing can each prevent access.

🗨️ 👤 **86024a2** 1 week ago

Selected Answer: A,C,E

I think the selected answers are correct.

upvoted 1 times

🗨️ 👤 **bluejl** 1 month ago

Selected Answer: C,D,E

D:

webfilter-force-off Enable/disable turning off the FortiGuard web filtering service.

A: Wrong

This scenario would typically result in browser certificate error warnings or specific site failures, rather than a complete inability to access any websites.

upvoted 1 times

🗨️ 👤 **86024a2** **Most Recent** 1 week ago

Why would D block access to sites?

upvoted 1 times

You manage an SD-WAN topology and you will soon deploy 50 new branches.

Which two tasks can you do in advance to simplify this deployment? (Choose two.)

- A. Create model devices.
- B. Create a policy blueprint.
- C. Define metadata variable values for each device.
- D. Create a zero-touch provisioning (ZTP) template.

Suggested Answer: A, D

AI-derived guidance: Model devices and ZTP templates let you prepare branch deployments in advance.

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

You want to configure SD-WAN on a few FortiGate devices to optimize the use of WAN links and secure internet access. The devices are standalone FortiGate, already centrally managed by FortiManager.

Which statement applies?

- A. You must move the devices to the SD-WAN Manager section before you can configure SD-WAN rules.
- B. You can keep the devices in the Device Manager section, but you must place them in a dedicated device group.
- C. You can keep the devices in the Device Manager section. You can configure per-device SD-WAN settings.
- D. You must move the devices to the SD-WAN Manager section and use the SD-WAN standalone wizard.

Suggested Answer: C

AI-derived guidance: Standalone devices can remain in Device Manager with per-device SD-WAN settings.

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

Refer to the exhibit.

The VDOM configuration on a FortiGate device is shown.

You discover that web filtering stopped working in Core1 and Core2 after a maintenance window.

What are two reasons why web filtering stopped working? (Choose two.)

VDOM sessions

HQ-NGFW-2				
Dashboard	+ Create new Search			
Network				
Security Profiles				
WiFi Controller				
System				
VDOM				
Global Resources				
Administrators				
Admin Profiles				
Firmware & Registration				
Settings				
HA				

N...	Management VDOM	Type	NGFW mode
☐ Core1	No	Traffic	Profile-based
☐ Core2	No	Traffic	Profile-based
☐ root	Yes	Traffic	Profile-based

- A. The Core1 and Core2 VDOMs must also be enabled as management VDOMs to receive FortiGuard updates.
- B. The root VDOM does not have access to FortiManager in a closed network.
- C. The root VDOM does not use a VDOM link to connect with the Core1 and Core2 VDOMs.
- D. The root VDOM does not have access to any valid, public Fortinet Distribution Network (FDN).

Suggested Answer: B, D

AI-derived guidance: The root management VDOM supplies FortiGuard connectivity for the other VDOMs. Check its public FDN reachability, or its FortiManager/FortiGuard service in a closed network; other VDOMs do not each become management VDOMs.

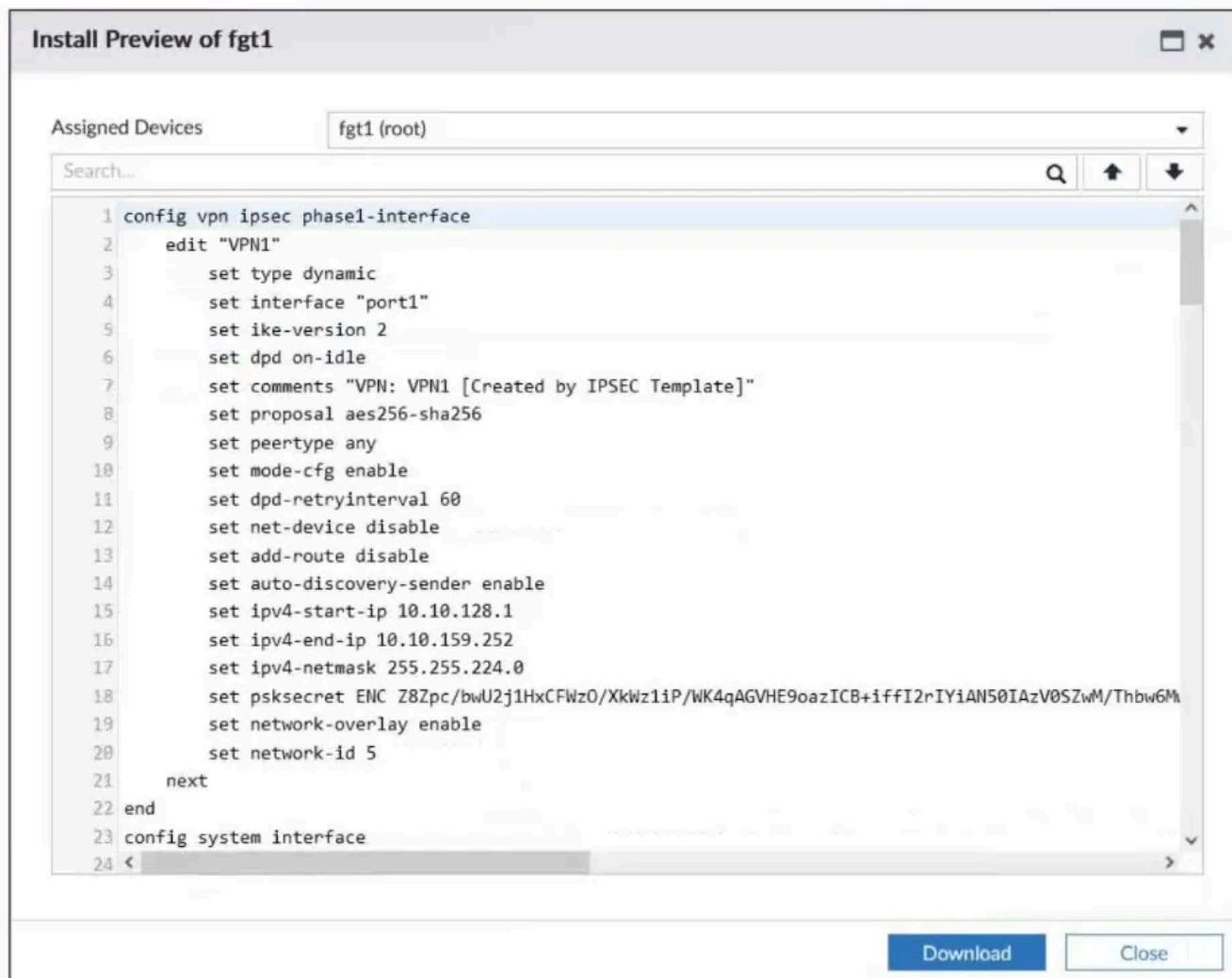
Currently there are no comments in this discussion, be the first to comment!

Refer to the exhibit.

You used the SD-WAN overlay orchestrator 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 correctly describes the configuration applied to the FortiGate device?

SD-WAN overlay template



- A. It is a hub device. It can send ADVPN shortcut offers.
- B. It is a spoke device that establishes dynamic IPsec tunnels to the hub. It can send auto-discovery VPN (ADVPN) shortcut requests.
- 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 IP sec tunnels to the hub. The local subnet range is 10.10.128.0/23.

Suggested Answer: A

AI-derived guidance: The exhibit has type dynamic, mode-cfg enable and auto-discovery-sender enable: this is a dialup hub that sends shortcut offers, not a spoke.

👤 haiderzaid Most Recent 1 month, 1 week ago

Selected Answer: A

A-set auto-discovery-sender enable

upvoted 1 times

Refer to the exhibits.

The routing tables of FortiGate A and FortiGate B are shown.

FortiGate_A and FortiGate_B are in the same autonomous system. You want to add only route 172.16.1.248/30 on FortiGate_A by updating the BGP configuration.

Which configuration must you apply?

Routing table on FortiGate_A

```
FortiGate_A # 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
       V - BGP VPNv4
       * - candidate default

Routing table for VRF=0
S*  0.0.0.0/0 [10/0] via 10.1.0.254, port1, [1/0]
C   10.1.0.0/24 is directly connected, port1
C   10.1.4.0/24 is directly connected, port3
B   100.64.1.0/24 [200/0] via 10.1.0.254 (recursive is directly connected, port1), 00:39:45, [1/0]
B   172.16.1.252/30 [200/0] via 10.1.0.1 (recursive is directly connected, port1), 00:42:48, [1/0]
C   172.16.100.0/24 is directly connected, port8
```

Routing table on FortiGate_B

```
FortiGate_B # 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
       V - BGP VPNv4
       * - candidate default

Routing table for VRF=0
S*  0.0.0.0/0 [10/0] via 10.1.0.254, port1, [1/0]
S   4.2.2.2/32 [10/0] via 10.1.5.254, port4, [1/0]
C   10.1.0.0/24 is directly connected, port1
B   10.1.4.0/24 [200/0] via 10.1.0.100 (recursive is directly connected, port1), 00:41:02, [1/0]
C   10.1.5.0/24 is directly connected, port4
B   100.64.1.0/24 [200/0] via 10.1.0.254 (recursive is directly connected, port1), 00:38:14, [1/0]
C   172.16.1.248/30 is directly connected, C0
C   172.16.1.252/30 is directly connected, A0
C   172.16.100.0/24 is directly connected, port8
```

- A. A BGP route map in for 172.16.1.248/30 on FortiGate_A
- B. The prefix 172.16.1.248/30 in the BGP Networks section on FortiGate_B
- C. A BGP route map out for 172.16.1.248/30 on FortiGate_B
- D. Enable Redistribute Connected in the BGP section on FortiGate_B

Suggested Answer: B

AI-derived guidance: Advertise the specific connected prefix by adding it to FortiGate B's BGP networks.

  **haiderzaid** Most Recent 1 month, 1 week ago

Selected Answer: B

B-since the prefix is not advertised yet

C-wrong because the prefix is not advertised, the route map will do nothing
upvoted 1 times

Refer to the exhibit.

The output of a BGP debug command is shown.

What is the most likely reason that the local FortiGate is not receiving any prefixes from its neighbors?

```
# get router info bgp summary

VRF 0 BGP router identifier 0.0.0.117, local AS number 65117
BGP table version is 3
3 BGP AS-PATH entries
0 BGP community entries

Neighbor      V      AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRcd
10.125.0.60    4    65060   1698   1756      0     0   0 never    OpenSent
10.127.0.75    4    65060   2206   2250     102     0   0 02:45:55      0
100.64.3.1     4    65061    101    115      0     0   0 never    Active

Total number of neighbors 3
```

- A. None of the three neighbors has successfully established the TCP three-way handshake with the local router.
- B. The local router is waiting for the keepalive message from the router 10.125.0.60.
- C. The router 100.64.3.1 is waiting for the OPEN message from the local router.
- D. The RIB-OUT configuration for router 10.127.0.75 prevents any route advertisement to the local router.

Suggested Answer: D

AI-derived guidance: The established 10.127.0.75 neighbor receives zero prefixes, consistent with no routes advertised.

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

FortiManager SD-WAN overlay orchestrator helps prepare SD-WAN deployments. To complete the tasks performed by the SD-WAN overlay orchestrator, you must perform some post-run tasks.

Which two mandatory post-run tasks must you perform? (Choose two.)

- A. Assign a hub_id metadata variable to each hub device.
- B. Assign an sdwan_id metadata variable to each device (branch and hub).
- C. Configure SD-WAN rules.
- D. Configure routing through the overlay tunnels created by the SD-WAN overlay template.
- E. Create policy packages and assign them to the branch devices.

Suggested Answer: C, E

AI-derived guidance: The overlay orchestrator generates the overlay and routing foundation. Configure application steering SD-WAN rules and assign the required traffic policy packages after orchestration.

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

Refer to the exhibits.

The system administrator settings configured on a root FortiGate and the Security Fabric settings configured on a downstream FortiGate are shown.

When prompted to sign in with Security Fabric to the downstream FortiGate, a user enters the single sign-on (SSO) provider credentials.

What is the result?

Root FortiGate - System Administrator configuration

System Administrator 2		
☐	AdminSSO	super_admin
☐	admin	super_admin

Downstream FortiGate - Security Fabric settings

Security Fabric role	Standalone Serve as Fabric Root Join Existing Fabric
Allow other Security Fabric devices to join	☒ port1 + ×
Upstream FortiGate IP/FQDN	10.1.0.254
Allow downstream device REST API access	☐
SAML Single Sign-On	Auto Manual
	Advanced Options
Mode	
Default login page	Normal Single Sign-On
Default admin profile	super_admin_readonly
Management IP/FQDN	Use WAN IP Specify
	10.1.0.100
Management port	Use Admin Port Specify
	443

- A. The downstream FortiGate relies on the root FortiGate and does not create an administrator account.
- B. The user is prompted to create an administrator account for AdminSSO.
- C. The downstream FortiGate creates an SSO administrator account for AdminSSO with the super_admin profile.
- D. The downstream FortiGate creates an SSO administrator account for AdminSSO with the super_admin_readonly profile.

Suggested Answer: D

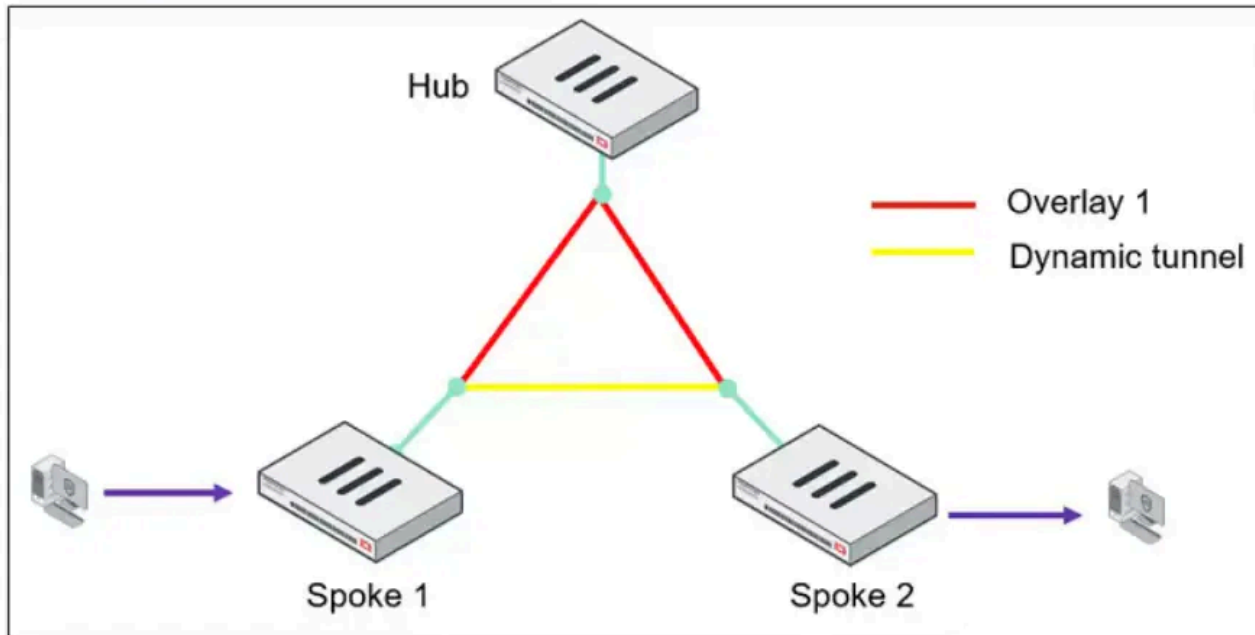
AI-derived guidance: The downstream's configured default admin profile is super_admin_readonly.

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

Refer to the exhibit.

Based on the exhibit, what is the first message that Spoke 1 replies to the hub instructing it to bring up the dynamic tunnel if a client generates traffic destined to Spoke 2?

Network topology



- A. Shortcut reply
- B. Shortcut forward
- C. Shortcut offer
- D. Shortcut query

Suggested Answer: D

AI-derived guidance: The initiating spoke responds to a shortcut offer from the hub by sending a shortcut query. The other spoke later returns the shortcut reply.

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

Refer to the exhibits.

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.)

SD-WAN service details

```
branch1_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.Portals(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

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=6

Microsoft.Portals(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

Security	APP Count	2
Level	notice	
General	Log ID	0000000013
Session ID	769	
Tran Display	snat	
Virtual Domain	root	
Source	Country	Reserved
Device ID	FGVM01TM22000077	
Device Name	branch1_fgt	
IP	10.0.1.101	
Interface	port5	
Interface Role	undefined	
NAT IP	192.2.0.9	
NAT Port	51042	
Port	51042	
Source	10.0.1.101	
UEBA Endpoint ID	1025	
UEBA User ID	3	
Destination	Country	United States
End User ID	3	
Endpoint ID	101	
Host Name	www.gotomeeting.com	
IP	23.212.248.205	
Interface	port2	

- A. No configured SD-WAN rule matches the traffic related to the collaboration application GoToMeeting.
- 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. The session 3-tuple did not match any of the existing entries in the ISDB application cache.

Suggested Answer: B, D

AI-derived guidance: Late application detection and an ISDB cache 3-tuple mismatch can leave sessions on the implicit rule.