Question #1 *Topic 1*

Refer to the exhibit.

```
config router bgp
     set as 65000
     set router-id 10.1.0.1
     set ibgp-multipath enable
     set additional-path enable
     set additional-path-select 3
     config neighbor-group
        edit "Branches_INET_0"
           set interface "T_INET_0"
           set remote-as 65000
           set update-source "T_INET_0"
        next
        edit "Branches_INET_1"
           set interface "T_INET_1"
           set remote-as 65000
           set update-source "T_INET_1"
        next
        edit "Branches_MPLS"
           set interface "T_MPLS"
           set remote-as 65000
           set update-source "T_MPLS"
        next
     end
     config neighbor-range
        edit 1
           set prefix 10.201.1.0 255.255.255.0
           set neighbor-group "Branches_INET_0"
        next
        edit 2
           set prefix 10.202.1.0 255.255.255.0
           set neighbor-group "Branches_INET_1"
        next
        edit 3
           set prefix 10.203.1.0 255.255.255.0
           set neighbor-group "Branches_MPLS"
        next
     end
...
end
```

The exhibit shows the BGP configuration on the hub in a hub-and-spoke topology. The administrator wants BGP to advertise prefixes from spokes to other spokes over the IPsec overlays, including additional paths. However, when looking at the spoke routing table, the administrator does not see the prefixes from other spokes and the additional paths.

Based on the exhibit, which three settings must the administrator configure inside each BGP neighbor group so spokes can learn other spokes prefixes and their additional paths? (Choose three.)

A. Enable soft-reconfiguration

B. Enable route-reflector-client

C. Set additional-path to send

D. Set adv-additional-path to the number of additional paths to advertise

E. Set advertisement-interval to the number of additional paths to advertise

Suggested Answer: *BCD*

Community vote distribution

BCD (100%)

Slikings 1 month, 3 weeks ago

Selected Answer: BCD

A: is wrong because soft reconfiguration was not mentioned in the 7.2 SG. The only mention of it was in the context of soft clear. Soft reconfiguration is a method in which fortigate stores BGP routing information using hardware resources.

B: Is correct because by default IBGP does not pass on learned routes between spokes, it can however when you enable the route reflector command. When this is enabled on the neighbor group it will forward routes of its peers to other spokes from the hub.

C: is correct, this is because this setting enables the ability to identify 2 additional paths and select them.

D: is correct, this is because the neighbor groups need to be assigned how many paths they can send on that neighbor.
E: is incorrect, this is because the advertisement interval is used in regards to route failover. It is used to speed up convergence by lowering the time that it Fortigate waits between BGP updates by reducing the advertisement interval for dead peers.
upvoted 1 times

romartinedg 9 months, 3 weeks ago
B: enable route-reflector-client | Guia 7.2 pag. 240
C: additional-path to send | Guia 7.2 pag. 254
D: adv-additional-path | Guia 7.2 pag. 254
upvoted 4 times

mitkotest 11 months, 3 weeks ago
B & C & D are correct
upvoted 1 times

nse_student 11 months, 3 weeks ago
Selected Answer: BCD
BCD are correct!
upvoted 1 times

TTOG 11 months, 4 weeks ago
I wanted to share with you my experience (sadly the exam comment section is removed) : I passed the exam a couple of days ago. There were 40 questions 5-6 of them not from here. A friend of mine failed it, most of his questions were not from here, some of them were from 7.0 he found out later.
upvoted 4 times

ipv84 11 months, 3 weeks ago
Hi TTOG, so if I understand correctly what you have said, the questions for the 7.2 exam is a mix of questions between these and those of 7.0 ?
upvoted 1 times

J_Olin 10 months, 3 weeks ago
That is very typical in Fortinet exams. They aren't going to rewrite a whole new test when really only about 5% of the content changed (the part related to new features). Always study at least the current exam version and the one previous.
upvoted 3 times

alejandrofern43 1 year ago
Selected Answer: BCD
Enable route-reflector-client (pag 239 Sd WAN Study guide for fortios-72)
set additional-path to send (pag 252/290 Sd WAN Study guide for fortios-72)
set adv-additional-path to the number of addional paths to advertise (pag 290 Sd WAN Study guide for fortios-72)
upvoted 3 times

KavinT 1 year ago
Selected Answer: BCD
B & C & D are correct
upvoted 1 times

ac89l 1 year ago
Selected Answer: BCD
correct
upvoted 1 times

IBB90704 1 year ago
B,C y D son correctas
upvoted 2 times

Question #2 *Topic 1*

What are two advantages of using an IPsec recommended template to configure an IPsec tunnel in an hub-and-spoke topology? (Choose two.)

A. It ensures consistent settings between phase1 and phase2.

B. It guides the administrator to use Fortinet recommended settings.

C. The VPN monitor tool provides additional statistics for tunnels defined with an IPsec recommended template.

D. It automatically install IPsec tunnels to every spoke when they are added to the FortiManager ADOM.

Suggested Answer: *AB*

Community vote distribution

AB (100%)

alejandrofern43 Highly Voted 1 year ago

Selected Answer: AB

2) What are two advantages of using an IPsec recommended template to configure an IPsec tunnel in an hub-and-spoke topology? (Choose two.)

A. It ensures consistent settings between phase1 and phase2.
B. It guides the administrator to use Fortinet recommended settings.
(pag 57 Sd WAN Study guide for fortios-72)

upvoted 5 times

Slikings Most Recent 1 month, 3 weeks ago

Selected Answer: AB

A: is correct, this is because IPsec templates do
ensure consistent settings between phase 1 and 2.
B: is correct, it guides the admin to use Fortinet
recommended settings.
C: is Incorrect, this is because VPN monitor is available for setups
using VPN manager and is not completely correlated with templates
according to the study guide.
D: is incorrect, this is because while it makes vpn setup easier, you
still have to define the network information with the template and
member configuration.

upvoted 1 times

romartinedg 9 months, 3 weeks ago

A,B | Guia 7.2 pag. 59

upvoted 1 times

KavinT 1 year ago

Selected Answer: AB

AB correct

upvoted 1 times

ac89l 1 year ago

Selected Answer: AB

AB correct

upvoted 1 times

IBB90704 1 year ago

A, B y D son correctas

upvoted 1 times

Question #3 *Topic 1*

Refer to the exhibit.

```
config system interface
    edit "port2"
        set vdom "root"
        set ip 192.2.0.9 255.255.255.248
        set allowaccess ping
        set type physical
        set role wan
        set snmp-index 2
        set preserve-session-route enable
    next
end
```

A. FortiGate does not change the routing information on existing sessions that use a valid gateway, after a route change.

B. FortiGate always blocks all traffic, after a route change.

C. FortiGate performs routing lookups for new sessions only, after a route change.

D. FortiGate flushes all routing information from the session table, after a route change.

Suggested Answer: *A*

Community vote distribution

A (100%)

Slikings 1 month, 3 weeks ago

Selected Answer: A

A: is correct, this is because the set_preserve_session_route enabled command makes a sticky interface. Not allowing the session to reroute due to best path change. Only new sessions will route through the better interface.

B. Fortigate does not always block traffic it will continue the session and only start new sessions through the new interface.

C. fortigate will ALSO check routing on a downed interface. it does not re-evaluate with stickiness enabled.

D. in this case it will not flush routing for the SESSION because stickiness is enabled.

upvoted 1 times

ccie8122 5 months ago

Selected Answer: A

A is absolutely correct.

The reason C is incorrect is the word "only." The FortiGate does not "only" check routing table for new sessions. It will ALSO check routing table for existing sessions when the session gateway is down/invalid!

upvoted 2 times

Mellon 5 months, 4 weeks ago

Selected Answer: C

C is correct, A is incorrect. Routing is not depending on a session, it's a session that is depending on routing.

upvoted 1 times

ccie8122 5 months ago

You are incorrect. See my response above.

upvoted 1 times

cgilvi 6 months, 3 weeks ago

I suppose that C would be right only if the traffic is NOT SNATed

upvoted 1 times

ccie8122 5 months ago

Incorrect. C is never correct, because routing is evaluated for existing session if the gateway becomes invalid. The problem with C is the word "only" makes it incorrect.

upvoted 1 times

KZM 6 months, 3 weeks ago

Selected Answer: A

Based on the exhibit, which two actions does FortiGate perform on traffic passing through port2? (Choose two.)
Correct answers: A, C
upvoted 1 times

ccie8122 5 months ago
C is incorrect for the reason i state above.
upvoted 1 times

lucient 11 months, 1 week ago
Selected Answer: A
A is correct. But also C. Page 154.
upvoted 1 times

ccie8122 5 months ago
Nope, "only" make C incorrect.
upvoted 1 times

truserud 11 months, 1 week ago
Selected Answer: A
A is correct
upvoted 1 times

nse_student 11 months, 3 weeks ago
Selected Answer: A
C is not correct, just A.
upvoted 1 times

alejandrofern43 1 year ago
Selected Answer: A
through port2. Hub2 drops any already established TCP sessions.
• With preserve-session-route enable, FortiGate does not reevaluate the session, and the session remains established through port1 and hub1. Active TCP sessions do not change. FortiGate routes new sessions through port2. pag 153 sdwan study 7.2. Y posiblemente algo de la D
upvoted 3 times

KavinT 1 year ago
A & C are correct, 2 answers
upvoted 1 times

ccie8122 5 months ago
C is incorrect. See my response above as to why.
upvoted 1 times

truserud 11 months, 1 week ago
Nope, for checking of new routes and tagging them as "dirty" you also have to configure config firewall policy
set firewall-session-dirty check-new
end

as stated here https://community.fortinet.com/t5/FortiGate/Technical-Tip-Information-about-firewall-session-dirty/ta-p/195802

Thus only A is correct.
upvoted 1 times

lucient 11 months, 1 week ago
C is correct too. Page 154. "With preserve-session-route enable, FortiGate does not reevaluate the session, and the session remains established through port1 and hub1. Active TCP sessions do not change. FortiGate routes new sessions through port2."

It says "FortiGate performs routing lookups for NEW SESSIONS only, after a route change. " and that's true. After the route change, old sessions stay with the old route. But for new sessions, Fortigate performs a route lookup.
upvoted 1 times

ccie8122 5 months ago
Incorrect. With preserve-session-route enabled, FortiGate will evaluate routing not "only" for new sessions, but it WILL ALSO reevaluate routing for existing sessions if the gateway is invalid for any reason!
upvoted 1 times

ac89l 1 year ago

Selected Answer: A

AC. There should be two answers

upvoted 2 times

IBB90704 1 year ago

A y C son correctas

upvoted 1 times

ccie8122 5 months ago

C no es correcta. La razon es que el FortiGate reevaluara "routing" por sesiones existentes que todavia no tienen "gateway" valido -- no solo por sesiones nuevas.

upvoted 1 times

Question #4 *Topic 1*

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

A. It provides the benefits of a full-mesh topology in a hub-and-spoke network.

B. It enables spokes to establish shortcuts to third-party gateways.

C. It provides direct connectivity between spokes by creating shortcuts.

D. It enables spokes to bypass the hub during shortcut negotiation.

Suggested Answer: *AC*

Community vote distribution

AC (100%)

Slikings 1 month, 3 weeks ago

Selected Answer: AC

A: is correct, this is because spokes create shortcuts through hub and spoke topologies giving the benefit of full mesh in a hub and spoke environment. page 266

B: is incorrect, this is because it does not need third party gateways to establish the short cut.

C: is correct for the same reason A is.

D: is incorrect because it still needs to pass the hub to establish the shortcut.

upvoted 1 times

KavinT 6 months, 3 weeks ago

A & C are correct

upvoted 3 times

JP0421 6 months, 3 weeks ago

Selected Answer: AC

Correct Answer is A & C

upvoted 1 times

ac89l 6 months, 3 weeks ago

Selected Answer: AC

AC correct

upvoted 1 times

IBB90704 6 months, 3 weeks ago

A y C son correctas

upvoted 1 times

Question #5 *Topic 1*

Refer to the exhibit.

```
fgt_1 # diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
  Tie break: cfg
   Gen(7), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(priority), link-cost-factor(latency), link-cost-
threshold(10), heath-check(HQ_Servers)

   Members(2):
     1: Seq_num(1 port1), alive, latency: 2.672, selected
     2: Seq_num(2 port2), alive, latency: 2.570, selected
   Internet Service(2): Facebook(4294836714,0,0,0,0 15832) Twitter(4294838045,0,0,0,0 16001)
   Src address(1):
         10.0.1.0-10.0.1.255

Service(2): Address Mode(IPV4) flags=0x200 use-shortcut-sla
  Tie break: cfg
   Gen(6), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(manual)
   Members(1):
    1: Seq_num(2 port2), alive, selected
   Internet Service(2): Business(0,29,0,0,0) Industrial(0,26,0,0,0)
   Src address(1):
         10.0.1.0-10.0.1.255

Service(3): Address Mode(IPV4) flags=0x200 use-shortcut-sla
  Tie break: cfg
   Gen(7), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(sla), sla-compare-order
   Members(3):
     1: Seq_num(3 T_HQ1), alive, alive, sla(0x3), gid(0), cfg_order(0), local cost(0), selected
     2: Seq_num(4 T_HQ2), alive, alive, sla(0x2), gid(0), cfg_order(1), local cost(0), selected
     3: Seq_num(5 T_HQ3), alive, alive, sla(0x1), gid(0), cfg_order(2), 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
```

The exhibit shows output of the command diagnose sys sdwan service collected on a FortiGate device.
The administrator wants to know through which interface FortiGate will steer the traffic from local users on subnet 10.0.1.0/255.255.255.192 and with a destination of the business application Salesforce located on HQ servers 10.0.0.1.
Based on the exhibits, which two statements are correct? (Choose two.)

A. There is no service defined for the Salesforce application, so FortiGate will use the service rule 3 and steer the traffic through interface T_HQ1.

B. FortiGate steers traffic to HQ servers according to service rule 1 and it uses port1 or port2 because both interfaces are selected.

C. When FortiGate cannot recognize the application of the flow it steers the traffic destined to server 10.0.0.1 according to service rule 3.

D. FortiGate steers traffic for business application according to service rule 2 and steers traffic through port2.

Suggested Answer: *AC*

Community vote distribution

CD (60%) AC (40%)

ee0808 Highly Voted 1 year ago

C & D
Salesforce = Business category -> D is correct
C is a general rule
upvoted 13 times

theklee 4 months, 2 weeks ago

Yes, Salesforce = business category, but the service sd-wan service 3 rule says "Internet Services" which are application specific. If they wanted to catch Salesforce as a business application, the rule should say Application Control instead of Internet Service.
upvoted 1 times

BoostBoris 1 week, 4 days ago

Just tested on my FGT v7.2.10. When you configure SD-WAN rule with application "business" and "industrial", command diag sys sdwan service returns "Internet Service(2): Business(0,29,0,0,0) Industrial(0,26,0,0,0)"
upvoted 1 times

mader Most Recent 2 weeks, 3 days ago

Selected Answer: C

C is correct

D is incorrect - The Internet Service Database is public IP address database that comes from the FortiGuard service system. The server define with private IP located at HQ, which is unlikely to be recognized by FortiGuard

upvoted 1 times

BoostBoris 1 week, 4 days ago

It is not Internet Service configured in SD-WAN rule, it is Application. Salesforce is part of Business category. diag sys sdwan service outputs showing "Internet Service" can be confusing

upvoted 1 times

Slikings 1 month, 3 weeks ago

Selected Answer: CD

Answers C and D are correct

A: is incorrect because, there is a service defined for salesforce. It is considered under the category of business rather than the application specifically being called out.

B: is incorrect because, there is no correlation between the application ID and the interface it is coming out from other than the source address.

C: is correct because, it could use rule 3 if it did not have the category already selected in rule 2. However, if the service was not defined in service 2 it would use 3

D: is correct because, service (2) uses port 2 and the application ID falls into the business category.

upvoted 1 times

cannoe 2 months, 1 week ago

Selected Answer: AD

Option C oversimplifies the process. When Fortigate cannot recognize the application, FortiGate will try to match the traffic based on the available rules. Rule 3 is chosen when no other specific rules match the traffic due to the default fallback behavior. For me, C is incorrect since it suggests that Rule 3 is selected only when Fortigate cannot recognize the application.

upvoted 1 times

theklee 4 months, 3 weeks ago

In terms of sdwan service, Business is an application category, not an Internet Service. The Salesforce application is an internet service. At least in 7.4.5. Therefore A is correct - no service is defined for Salesforce and C is also correct. D would be correct if the diag sys sdwan service showed Application Control: Business but it shows Internet Service instead.

upvoted 1 times

ccie8122 5 months ago

Selected Answer: CD

A is incorrect because Salesforce is in category Business and with the matching source IP address, the traffic will match Service 2, thus making D correct. C is correct as a general catch-all rule logic (absent application matching)--even though not applicable as the application does match in this case.

upvoted 1 times

rac_sp 6 months ago

Selected Answer: CD

Guys I just confirmed in the Fortiguard Labs that the Sales Force traffic belongs to the category BUSINESS. Therefore, answer is C and D

upvoted 1 times

evdw 7 months ago

Selected Answer: CD

rule 2 match is not based ISDB but on application category (category 29 = Business)

If Application Control is activated on the security policy, traffic can be matched and sdwan service rule can be matched

So I would go for C,D

upvoted 2 times

geroboamo 7 months ago

Selected Answer: AC

the question states that salesforce is hosted on a private server, so sdwan rule 2 is not matched since it uses Internet Services DataBase. So traffic will be managed by rule 3

upvoted 2 times

luismanzanero 8 months, 1 week ago

Selected Answer: CD

C & D are correcte

upvoted 1 times

fottyfan 9 months, 1 week ago

Question is, would Salesforce traffic be recognized if it is to private servers?

upvoted 3 times

[Removed] 8 months, 3 weeks ago

I agree with your reasoning that's why I would go for option A and C considering the business runs on the private HQ servers and they are not available over the internet

upvoted 2 times

tibrad4 9 months, 3 weeks ago

Selected Answer: CD

C&D

I originally thought A and C but after looking at it this question is very misleading. Answer D is not saying that the specific server traffic is going to use port2, it is saying Salesforce traffic will use it. Since Salesforce is in the business category, A becomes invalid and D becomes true.

upvoted 1 times

sugar12 10 months ago

Selected Answer: CD

A is wrong because Salesforce is part of the business category

B is wrong because rule 1 doesnt cover salesforce

therefore C & D are correct

upvoted 1 times

VLAN_G 10 months, 2 weeks ago

Selected Answer: CD

CD for sure.

upvoted 1 times

truserud 11 months, 1 week ago

Selected Answer: CD

Forgot to mark answers. See my other comment below.

upvoted 1 times

truserud 11 months, 1 week ago

C & D are correct.

C is the dirst correct answer in this scenario.

D is the second correct answer: Salesforce is indeed identified as a Business Category. Just check up your Application Control profile on your Fortigate and view entries, then search for Salesforce. Thus it will hit Rule (Service) 2. As we all know; SD-WAN rules are handled the same way as Firewall Policies, from top to bottom. Thus D is correct.

upvoted 1 times

ginmco 11 months, 1 week ago

The answer is C & D

When you go under "View Application Signatures" Salesforce = Business category -> D is correct

C is a general rule

upvoted 2 times

Question #6 *Topic 1*

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

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

B. By default. SD-WAN rules are skipped if the best route to the destination is not an SD-WAN member.

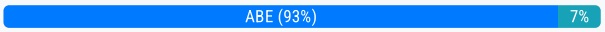
C. FortiGate performs route lookups for new sessions only.

D. SD-WAN rules have precedence over ISDB routes.

E. Regular policy routes have precedence over SD-WAN rules.

Suggested Answer: *ABD*

Community vote distribution



Slikings 1 month, 3 weeks ago

Selected Answer: ABE

A: this is correct

B: this is correct

C: this is incorrect because dirty sessions can get a new route lookup if sticky interface is disabled

D: incorrect, ISDB takes precedence over SD-WAN rules

E: is correct

upvoted 1 times

ccie8122 5 months ago

Selected Answer: ABE

D is incorrect (and E is correct) as per the route-selection hierarchy on p 130:

Policy route > ISDB route > SD-WAN rules > route cache > RIB/FIB

(i.e., both policy routes and ISDB routes take precedence over SD-WAN rules).

A is correct because this is general routing logic -- if there is not valid route through an interface, the member is not a candidate path.

B is a direct quote from principle 4 on page 126

C is incorrect, because FortiGate will recalc routes on existing sessions if preserve-session-route is disabled, or if the gateway through the current session's member goes down

upvoted 1 times

ipv84 12 months ago

Selected Answer: ABE

A & B & E - Study guide page 126

upvoted 3 times

iantra123 1 year ago

Selected Answer: ABE

ABE

Regular Policy have precedence over sd-wan rules

upvoted 2 times

Tommy_S 1 year ago

Selected Answer: ABE

A,B,E are correct

upvoted 1 times

alejandrofern43 1 year ago

Selected Answer: ABE

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

B. By default. SD-WAN rules are skipped if the best route to the destination is not an SD-WAN member.

E. Regular policy routes have precedence over SD-WAN rules.

(pag 124 Sd WAN Study guide for fortios-72)

upvoted 1 times

ee0808 1 year ago

ABE

ISDB routes have preference over SD-WAN rules

upvoted 1 times

Tommy_S 1 year ago

Selected Answer: ABE

A,B and E are Correct.

Study guide p126

upvoted 4 times

Johnwoo3201 1 year ago

Selected Answer: BDE

BDE might make more sense.

upvoted 1 times

ccie8122 5 months ago

No, D is incorrect for the reasons I state above.

upvoted 1 times

KavinT 1 year ago

Selected Answer: ABE

page 126 SD WAN 7.2

upvoted 1 times

IBB90704 1 year ago

A, B y E son correctas

upvoted 2 times

FreddyM 1 year ago

Selected Answer: ABE

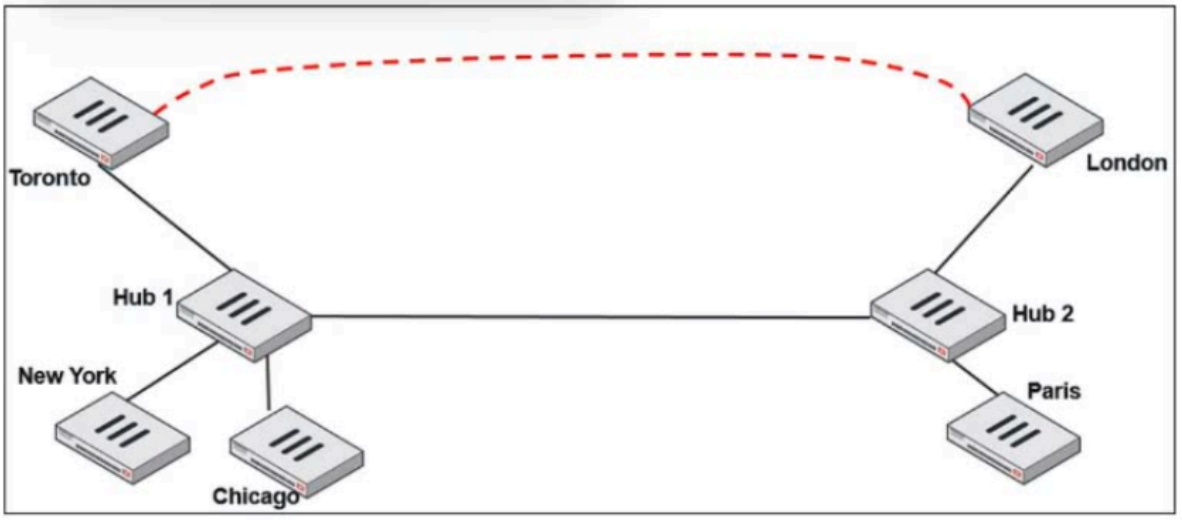
study guide

E: page 126

upvoted 2 times

Question #7 *Topic 1*

Refer to the exhibit.



Two hub-and-spoke groups are connected through a site-to-site IPsec VPN between Hub 1 and Hub 2.
Which two configuration settings are required for Toronto and London spokes to establish an ADVPN shortcut? (Choose two.)

A. On the hubs, net-device must be enabled on all IPsec VPNs.

B. auto-discovery-forwarder must be enabled on all IPsec VPNs.

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

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

Suggested Answer: *CD*

Community vote distribution

CD (100%)

alejandrofern43 Highly Voted 6 months, 1 week ago

Selected Answer: CD

(pag 269 Sd WAN Study guide for fortios-72)
C. On the spokes, auto-discovery-receiver must be enabled on the IPsec VPN to the hub.
D. On the hubs, auto-discovery-sender must be enabled on the IPsec VPNs to spokes.
upvoted 5 times

Slikings Most Recent 1 month, 3 weeks ago

Selected Answer: CD

A: incorrect, net device is only enabled on overlays configured as dial up.
B: incorrect, auto discovery forwarder is used on the hub to communicate with other hubs, it does not need to be enabled on all spokes.
C: correct, receiver is enabled on the spokes
D: correct sender is enabled on the hub

Page 270
This question is asking about the configuration of auto-discovery
it is important to understand the difference between receiver, sender and forwarder.
upvoted 1 times

ee0808 6 months, 1 week ago

Selected Answer: CD

CD
auto-disovery-forwarder only between hubs
upvoted 3 times

KavinT 6 months, 3 weeks ago

Selected Answer: CD

CD are correct, Refer to AD VPN section

upvoted 1 times

ac89l 6 months, 3 weeks ago

Selected Answer: CD

CD correct

upvoted 1 times

IBB90704 6 months, 3 weeks ago

C y D son correctas

upvoted 1 times

Question #8 *Topic 1*

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

A. get router info routing-table all

B. get ipsec tunnel list

C. diagnose vpn tunnel list

D. diagnose debug application ike

Suggested Answer: *D*

Community vote distribution

D (100%)

Slikings 1 month, 3 weeks ago

Selected Answer: D

A: is incorrect because it is a route lookup command

B: is incorrect

C: is incorrect this will show tunnel names and ID

D: is correct because diag debugging commands show real time troubleshooting.

upvoted 1 times

alejandrofern43 6 months, 1 week ago

Selected Answer: D

diagnose debug application ike pag 278 study_guie

upvoted 3 times

ee0808 6 months, 1 week ago

Selected Answer: D

D is correct

upvoted 1 times

KavinT 6 months, 3 weeks ago

Selected Answer: D

D is correct

upvoted 1 times

IBB90704 6 months, 3 weeks ago

D es correcta

upvoted 1 times

Question #9 *Topic 1*

What are two common use cases for remote internet access (RIA)? (Choose two.)

A. Provide internet access through the hub.

B. Centralize security inspection on the hub.

C. Provide thorough inspection on spokes.

D. Provide direct internet access on spokes.

Suggested Answer: *AB*

Community vote distribution

AB (100%)

iantra123 Highly Voted 1 year ago

Selected Answer: AB

A & B

Remote internet access (RIA) = through the Hub

upvoted 5 times

Slikings Most Recent 1 month, 3 weeks ago

Selected Answer: AB

RIA is where internet passes through the hub. SD-WAN can use RIA to steer traffic through overlays to centralize traffic on the hub for inspection and improved performance if DIA is poor or unavailable.

A: Correct

B:Correct

C: Incorrect, it can but spokes could be using DIA and have adequate inspection already.

D: incorrect, this would be DIA (direct internet access)

upvoted 1 times

Gilmarcio 7 months, 3 weeks ago

P. 12 Study Guide

upvoted 1 times

alejandrofern43 1 year ago

Selected Answer: AB

A. Provide internet access through the hub.

B. Centralize security inspection on the hub.

pag 13 guide 7.2

upvoted 3 times

KavinT 1 year ago

Selected Answer: AB

AB are correct

upvoted 1 times

IBB90704 1 year ago

A y B son correctas

upvoted 1 times

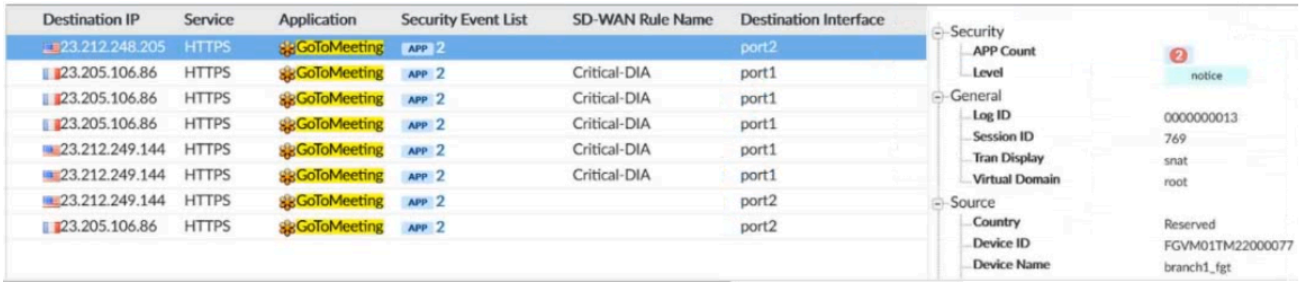
Question #10 *Topic 1*

Refer to the exhibits.

Exhibit A.

```
branch1_fgt # diagnose sys sdwan service

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

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

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

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

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

Exhibit B.



Destination IP	Service	Application	Security Event List	SD-WAN Rule Name	Destination Interface
23.212.248.205	HTTPS	GoToMeeting	APP 2		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 exhibit A.

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

The administrator noticed that the traffic matched the implicit SD-WAN rule, but they expected the traffic to match rule ID 1.

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

A. Port1 and port2 do not have a valid route to the destination.

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

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

D. FortiGate did not refresh the routing information on the session after the application was detected.

Suggested Answer: *BD*

Community vote distribution

BD (100%)

lucient Highly Voted 11 months, 1 week ago

Selected Answer: BD

B: There is no 3-tuple with IP 23.212.248.205

D: Page 156 of the study guide. "By default, SNAT sessions are not flagged as dirty following a routing change that impacts the session". So, the first routing match is the default sd wan rule. After identifying the app, the match is now rule ID 1. However, because there is SNAT to the Internet, the session is not marked as "dirty". It is not re-evaluated and traffic keeps going through port2.

upvoted 5 times

Gilmarcio Most Recent 7 months, 3 weeks ago

Study Guide P. 320

upvoted 1 times

romartinedg 9 months, 3 weeks ago

B, D | Guía 7.2 pág. 192

upvoted 2 times

Lomik29 1 year ago

D is correct when the session is subject to SNAT (by default, guide page 191)

upvoted 1 times

alejandrofern43 1 year ago

Selected Answer: BD

B (pag 191 study_guide 7.2)

D descarte

upvoted 1 times

KavinT 1 year ago

Selected Answer: BD

B & D are correct

upvoted 1 times

ac89l 1 year ago

why D is correct ?

upvoted 1 times

IBB90704 1 year ago

B y D correctas

upvoted 1 times

Question #11 *Topic 1*

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

A. diagnose sys sdwan member

B. diagnose sys sdwan interface

C. diagnose sys sdwan zone

D. diagnose sys sdwan service

Suggested Answer: *C*

Community vote distribution

C (100%)

Slikings 1 month, 3 weeks ago

Selected Answer: C

A: incorrect, this command only shows its members and not zones assigned to it.

B: incorrect, cannot find info on this command

C: Correct, diagnose sys sdwan zone shows zones and assigned members.

D: incorrect, this command shows service of the rule, this indicates matching criteria, rule modes and how it determines preferred members.

upvoted 1 times

romartinedg 9 months, 3 weeks ago

C | Guía 7.2 pág. 313

upvoted 2 times

alejandrofern43 1 year ago

Selected Answer: C

C is correct. pag 312 guide 7.2

upvoted 2 times

Tommy_S 1 year ago

Selected Answer: C

C is correct

upvoted 1 times

KavinT 1 year ago

Selected Answer: C

C is correct

upvoted 1 times

IBB90704 1 year ago

C es la correcta

upvoted 1 times

Question #12 *Topic 1*

Which statement is correct about SD-WAN and ADVPN?

A. SD-WAN can steer traffic to ADVPN shortcuts only for rules defined with strategy manual or best quality.

B. SD-WAN does not monitor the health and performance of ADVPN shortcuts.

C. SD-WAN cannot steer traffic to ADVPN shortcuts established over IPSec overlays if the zone contains physical interfaces.

D. SD-WAN can steer traffic to ADVPN shortcuts established over IPsec overlays configured as SD-WAN members.

Suggested Answer: *D*

Community vote distribution

Slikings 1 month, 3 weeks ago

Selected Answer: D

D: is correct due to the wording of answer C

upvoted 1 times

ccie8122 5 months ago

Selected Answer: D

D is correct per page 266 of the guide:

"SD-WAN supports ADVPN shortcuts. For this, SD-WAN automatically steers the traffic through shortcuts and monitors their health and performance. You add the parent tunnel as member, and after the shortcut is negotiated, SD-WAN automatically starts steering traffic through the shortcut."

C is INCORRECT for the same reason D is correct: "you add the parent tunnel as member." There is no discussion of (nor is there any need to) add the physical interface to the overlay zone -- only the tunnel interface need be added.

upvoted 2 times

ccie8122 5 months ago

Correction ^^

There is no discussion that adding the physical interface will prevent SD-WAN from steering traffic over the member tunnel interface. I agree it is an incorrect configuration (physical interface SHOULD NOT be a member), but ADVPN/SD-WAN shortcut steering will still work.

upvoted 1 times

GCISystemIntegrator 9 months, 2 weeks ago

Selected Answer: D

need to listen the audio and in the ADVPN slite the voice tell exactely the "D" answer

upvoted 3 times

sugar12 10 months ago

Selected Answer: C

A - Wrong

B - Wrong

D - Wrong - SD-WAN supports ADVPN shortcuts. For this, SD-WAN automatically steers the traffic through shortcuts and monitors their health and performance. You add the parent tunnel as member, and after the shortcut is negotiated, SD-WAN automatically starts steering the traffic through the shortcut

Lets say that the parent interface is called ADVPN and an example of a shortcut will be ADVPN1_0 . You do not add in the zone the ADVPN1_0 as described on choice D you add the parent tunnel. I am not really sure how all people gave as an answer D as correct. Its a tricky one as they play with words.

C is the correct one. SD-WAN ADVPN is an overlay solution so it not expected to use the physical interfaces as members when specifically at C it says "established over IPSEC overlays"

upvoted 1 times

ccie8122 5 months ago

Just because it is not expected to have the physical interface in the zone does not mean it will not work. C is INCORRECT because it states that "SD-WAN cannot steer traffic" if the zone contains physical interfaces. This is not true. You could have a physical interface in the zone.

Since there is no valid route out that interface, that member will never be used, but the SD-WAN will still steer traffic over the IPSec overlay.

upvoted 1 times

stbb 9 months, 1 week ago

Answer D, the ipsec overlays are configured as SD-WAN members meaning in your example the "ADVPN".

upvoted 1 times

truserud 11 months, 1 week ago

Selected Answer: D

D is correct

upvoted 1 times

alejandrofern43 1 year ago

Selected Answer: D

D is correct

upvoted 1 times

KavinT 1 year ago

Selected Answer: D

D is correct

upvoted 1 times

IBB90704 1 year ago

D es la correcta

upvoted 1 times

Question #13 *Topic 1*

Refer to the exhibit.

```
branch1_fgt # diagnose sys sdwan service 3

Service(3): Address Mode(IPV4) flags=0x200 use-shortcut-sla
  Gen(5), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(priority), link-cost-
factor(latency), link-cost-threshold(10), heath-check(VPN_PING)
  Members(3):
    1: Seq_num(3 T_INET_0_0), alive, latency: 101.349, selected
    2: Seq_num(4 T_INET_1_0), alive, latency: 151.278, selected
    3: Seq_num(5 T_MPLS_0), alive, latency: 200.984, selected
  Src address(1):
        10.0.1.0-10.0.1.255

  Dst address(1):
        10.0.0.0-10.255.255.255


branch1_fgt (3) # show
config service
    edit 3
        set name "Corp"
        set mode priority
        set dst "Corp-net"
        set src "LAN-net"
        set health-check "VPN_PING"
        set priority-members 3 4 5
    next
end
```

The exhibit shows the SD-WAN rule status and configuration.

Based on the exhibit, which change in the measured latency will make T_MPLS_0 the new preferred member?

A. When T_INET_0_0 has a latency of 250 ms.

B. When T_MPLS_0 has a latency of 80 ms.

C. When T_INET_0_0 and T_MPLS_0 have the same latency.

D. When T_MPLS_0 has a latency of 100 ms.

Suggested Answer: *B*

Community vote distribution

B (100%)

8666239 Highly Voted 6 months, 3 weeks ago

Page 204 in the 7.2 Study guide.

link-cost-threshhold(10) which means you need a 10% improvement over the highest selected member (T_INET_0_0). 101.349 / 1.10 (110%) = 92.135. That means that T_MPLS_0 would have to be lower than that value to be selected.

Answer B sets the latency to 80ms which is less than 92.135ms.

upvoted 5 times

Slikings Most Recent 1 month, 3 weeks ago

Selected Answer: B

A: incorrect, this would make it last

B: correct, the adjusted value of T_INET_0_0 is 92.135 bringing it above a latency of 80

C: incorrect, if it was the same then it would use priority as its metric

D: incorrect because the adjusted value of 0_0 is still lower.

upvoted 1 times

JTGUTI 8 months, 4 weeks ago

One question. What formula is made to give this result? 80ms.

Thanks,

upvoted 1 times

sugar12 10 months ago

Selected Answer: B

A. - wrong because INET_1_0 will still win MPLS_0

B. correct because 80ms will be better from the corrected metric of INET_0_0

C. Wrong because INET_0_0 has better priority

D. wrong because 100ms will be worst from the corrected metric of inter_0_0

upvoted 2 times

alejandrofern43 1 year ago

Selected Answer: B

13) The exhibit shows the SD-WAN rule status and configuration.

Based on the exhibit, which change in the measured latency will make T_MPLS_0 the new preferred member?

pag 203 guide 7.2

B. When T_MPLS_0 has a latency of 80 ms. Latenci en inet_0 is 101.349/1.10=92.14

upvoted 3 times

KavinT 1 year ago

Selected Answer: B

B is correct. Refer to Link Cost Threshold section in SD WAN 7.2

upvoted 1 times

IBB90704 1 year ago

B es la correcta

upvoted 1 times

Question #14 *Topic 1*

What is a benefit of using application steering in SD-WAN?

A. The traffic always skips the regular policy routes.

B. You do not need to configure firewall policies that accept the SD-WAN traffic.

C. You steer traffic based on the detected application.

D. You do not need to enable SSL inspection.

Suggested Answer: *C*

Community vote distribution

C (100%)

Slikings 1 month, 3 weeks ago

Selected Answer: C

C is correct, very easy question

upvoted 1 times

iantra123 6 months, 1 week ago

Selected Answer: C

C : steer based on application

upvoted 2 times

alejandrofern43 6 months, 1 week ago

Selected Answer: C

pag 188 guide 7.2

C. You steer traffic based on the detected application.

upvoted 1 times

KavinT 6 months, 3 weeks ago

Selected Answer: C

C is correct

upvoted 1 times

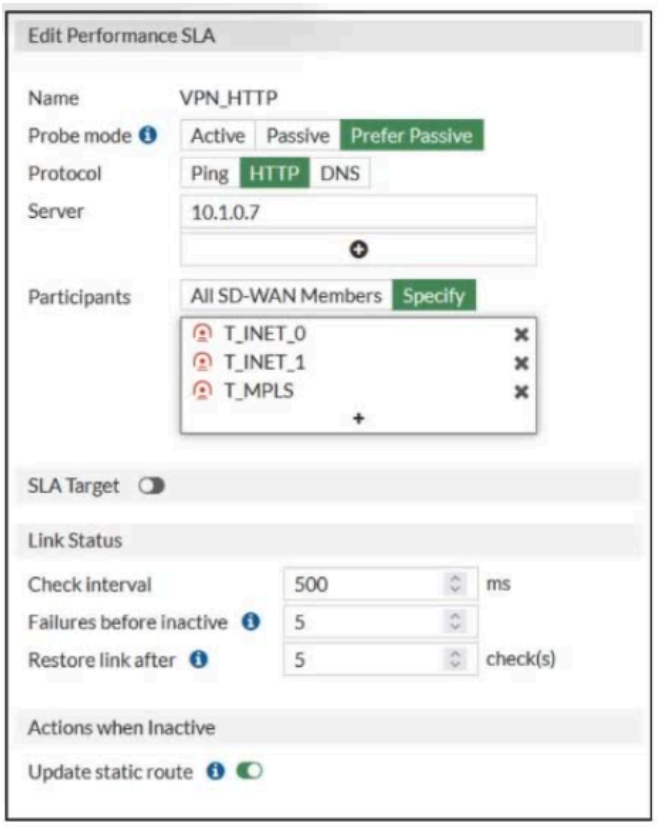
IBB90704 6 months, 3 weeks ago

C es la correcta

upvoted 1 times

Question #15 *Topic 1*

Refer to the exhibit.



Based on the exhibit, which two statements are correct about the health of the selected members? (Choose two.)

A. After FortiGate switches to active mode, the SLA performance rule never fallsback to passive monitoring.

B. FortiGate passively monitors the member if TCP traffic is passing through the member.

C. FortiGate can offload the traffic that is subject to passive monitoring to hardware.

D. During passive monitoring, the SLA performance rule cannot detect dead members.

Suggested Answer: *BD*

Community vote distribution

BD (100%)

Slikings 1 month, 3 weeks ago

Selected Answer: BD

A: is incorrect, the point is to preferr passive monitoring

B: is correct, passive monitoring works only on traffic passing through

C: incorrect page 106 states you must have passive wan health measurement on which consequently results in auto-asic-offload being disabled

D: correct passive monitor does not detect dead members prefer passive only detects after 3 min of no traffic.

upvoted 1 times

truserud 5 months ago

Selected Answer: BD

B & D are correct as stated in the study guide for SD-WAN 7.2 on page 106.

upvoted 1 times

alejandrofern43 6 months, 1 week ago

Selected Answer: BD

pag 105 study_guide 7.2

B. FortiGate passively monitors the member if TCP traffic is passing through the member.

D. During passive monitoring, the SLA performance rule cannot detect dead members.

upvoted 4 times

Tommy_S 6 months, 2 weeks ago

Selected Answer: BD

B & D are correct

upvoted 1 times

KavinT 6 months, 3 weeks ago

Selected Answer: BD

B & D are correct. Refer to Prefer Passive Section in SD WAN 7.2

upvoted 1 times

IBB90704 6 months, 3 weeks ago

B y D correctas

upvoted 1 times

Question #16 *Topic 1*

Which two statements about the SD-WAN members are true? (Choose two.)

A. Interfaces of type virtual wire pair can be used as SD-WAN members.

B. You can manually define the SD-WAN members sequence number.

C. An SD-WAN member can belong to two or more SD-WAN zones.

D. Interfaces of type VLAN can be used as SD-WAN members.

Suggested Answer: *BD*

Community vote distribution

BD (100%)

Slikings 1 month, 3 weeks ago

Selected Answer: BD

B and D are correct. B is obvious, D is correct based off the list on page 84

vlan interfaces can be part of the underlay, as a member including physical ports, lags and wireless.

upvoted 1 times

truserud 5 months ago

Selected Answer: BD

B & D are correct.

upvoted 1 times

alejandrofern43 6 months, 1 week ago

Selected Answer: BD

pag 83 y 85 guide 7.2

B and D are correct

upvoted 2 times

KavinT 6 months, 3 weeks ago

Selected Answer: BD

B & D are correct

upvoted 1 times

IBB90704 6 months, 3 weeks ago

B y D correctas

upvoted 1 times

Question #17 *Topic 1*

Refer to the exhibit.

```
branch1_fgt # diag sys sdwan service 1

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
  Tie break: cfg
   Gen(14), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(sla), sla-compare-order
   Members(4):
      1: Seq_num(3 T_INET_0), alive, sla(0x1), gid(0), cfg_order(0), local cost(0), selected
      2: Seq_num(4 T_INET_1), alive, sla(0x1), gid(0), cfg_order(1), 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

branch1_fgt # diagnose sys sdwan member | grep T_INET_
Member(3): interface: T_INET_0, flags=0xd may_child, gateway: 100.64.1.1, peer: 10.201.1.254, priority:
10 1024, weight: 0
Member(4): interface: T_INET_1, flags=0xd may_child, gateway: 100.64.1.9, peer: 10.202.1.254, priority:
1 1024, weight: 0

branch1_fgt # get router info routing-table all | grep T_INET_
S        10.0.0.0/8 [1/0] via T_INET_1 tunnel 100.64.1.9, [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 T_INET_0. However, the traffic is routed over T_INET_1. Based on the output shown in the exhibit, which two reasons can cause the observed behavior? (Choose two.)

A. T_INET_1 has a lower route priority value (higher priority) than T_INET_0.

B. The traffic matches a regular policy route configured with T_INET_1 as the outgoing device.

C. T_INET_1 has a higher member configuration priority than T_INET_0.

D. T_INET_0 does not have a valid route to the destination.

Suggested Answer: *AB*

Community vote distribution

BD (55%) AD (40%) 5%

sven22 1 month, 2 weeks ago

Selected Answer: BD

A is definitely incorrect as the member priority is what is used in Lowest Cost (SLA) and T_INET_0 has higher priority over T_INET_1 as that is how they are configured in order.

upvoted 1 times

ccie8122 5 months ago

Selected Answer: BD

SD-WAN strategy is Lowest Cost (SLA) as indicated by the "Mode(sla)" flag. Cost SLA uses SLA target, cost, and priority (i.e., interface preference - or order of config unless manually overridden by admin config) as the criteria -- in that order. Both members meet the target, both have 0 cost, and therefore member 3 (T_INET_0) wins the "priority" tiebreaker. So if there is a valid route to the destination through member 3, it will win. The fact that it does not has nothing to do with the configured static route/member priority, which according to SG page 197 "is used as a tiebreaker for ECMP routes when matching implicit SD-WAN rule." That is not the case here, so A is INCORRECT.

C is patently incorrect as T_INET_0 clearly has the higher priority (3) than T_INET_1 (4).

upvoted 2 times

bestboy120 6 months, 4 weeks ago

This priority value will be used in the static route created for the SD-WAN's member interface. This routing priority is mainly effective against traffic matching SD-WAN implicit rules where it can be used to prioritize certain SD-WAN's member interface. The lower the value the higher the priority is.

upvoted 1 times

bestboy120 6 months, 4 weeks ago

and rule from exihibit is not IMPLICIT RULE

upvoted 1 times

evdw 7 months ago

Selected Answer: BD

B&D is correct

upvoted 2 times

Fanny1493 7 months, 3 weeks ago

Selected Answer: AD

A because INET_1 have best priority

upvoted 2 times

ad7eddd 8 months, 2 weeks ago

Selected Answer: BD

BD correct

upvoted 1 times

Alkaa 9 months, 2 weeks ago

B et D is best anser. In fact, priority is not use on SD-WAN rules just in implicit SD-WAN rule.

upvoted 1 times

Kippie036 9 months, 2 weeks ago

Selected Answer: BD

These are the correct answers, just passed the exam with a 100% score.

upvoted 2 times

KamelVelizy 3 weeks, 6 days ago

Hi, Would you please share the all your responses?

upvoted 1 times

Kippie036 9 months, 2 weeks ago

It is B and D, just passed the exam with a 100% score so must be B and D on de Exam

upvoted 2 times

sugar12 10 months ago

B - Wrong There is no PBR details anywhere while there is a static route to
T_INET_1 and definitely SDWAN rules. PBR is an assumption
C - Wrong the member configuration priority refers to which interface added first
in the rule and as you see the first one at the top of service(1) is T_INET_0
therefore that option is wrong as INET_1 has lower member configuration priority
than INET_0 as is added later

upvoted 3 times

sugar12 10 months ago

Selected Answer: AD

D - Correct We see only a static route to T-INET_1 so there is no valid route to INET_0
therefore this is correct
A - Correct if you have a fortigate go to SDWAN-> SDWAN ZONES ->
click to a zone you configured and check which interfaces you added
in that zone. if you click any interfaces you will see an the option to specify
"priority". Go on the exclamation mark and see what it says. The lower the value
the higher the route priority. T_INET_1 has priority 1 while T_INET_0 has priority 10
therefore T-INET_1 has a higher route priority as it has lower value/
Therefore C & B are wrong.

upvoted 1 times

stbb 9 months, 1 week ago

A is not correct. Priority is only used for the implicit rule which is not the case in this question.

upvoted 2 times

lucient 11 months ago

Selected Answer: BD

After reading once and again this question, I've found this: the commando get router info routing-table all user "grep T_INET_"

So, grep should lists entries for T_INET_0 and T_INTE_1. However, there is only one entry for T_INET_1

This means:

A) Wrong. Even if it matchet sdwan rule 1, the only valid member is 2: T_INET_1

B) Can be right. A regular policy with T_INET_1 would work because there is a route in the routing table.

C) Wrong. Same as "A".

D) It's 100% right. T_INET_0 does not have a valid route.
upvoted 2 times

lucient 11 months, 1 week ago

Selected Answer: BD

"A" can't be right. Page 197: "Do not confuse the member configuration priority with the Priority setting available on the SD-WAN member configuration. The latter is used for the priority of static routes for members when you configure static routes for zones. The former refers to the member priority based on the Interface Preference list configuration. Members that are configured first in the list have higher priority over those configured last. The Priority setting is used as a tiebreaker for ECMP routes when matching the implicit SD-WAN rule."

Priority SETTING is not relevant in this case because there is no static route for zone, so there is NOT ECMP. There is only one route to 10.0.0.0/8 pointing to T_INET_1.

"B" is a possible reason even if there is no exhibit. Policy routes come before ISDB rules and SDWAN rules. If there is a policy route pointing to T_INET_1 it has precedence over sdwan rules. And will work because there is a valid route through T_INET_1.
upvoted 1 times

lucient 11 months, 1 week ago

"C" can't be right. Page 87: "cfg-order instructs FortiGate to use the member configuration order as the tiebreaker for the selected member. That is, members that are configured first, have higher priority."

There is not tie because there is NO route through T_INET_0. So, even when the tie break is "cfg", member configuration priority is not relevant.

"D" is right. There is no route to 10.0.0.0/8 pointing to T_INET_0
upvoted 1 times

truserud 11 months, 1 week ago

Selected Answer: AD

A&D must be the correct answers based on the exhibition:
A because that is an actual fact with regards to the router info output
D because T_INET_0 is not listed in the routing info output, and there are no places in the exhibition showing anything related to policy based routing
upvoted 3 times

nse_student 11 months, 3 weeks ago

Selected Answer: BD

Priority not used for this purpose.
upvoted 1 times

83e48be 12 months ago

Selected Answer: AD

AD is correct
upvoted 1 times

83e48be 12 months ago

If I try to put in the explanation it gives a cloudflare error.
really short version :
D, route no exist on T_INET_0
A, 1 lower prio over 0 , yes, but only implicit rule
B , could be , but nothing showing PBR

on exam pick A+D
upvoted 1 times

83e48be 12 months ago

This is a bad question/example.
We don't know the source besides "branch1_fgt", which has no reference to a subnet.
We have to assume this is source 10.0.1.0/24.
Info regarding PBR and other SDWAN config is missing as well.

T_INET_1 has a lower route priority value (higher priority) than T_INET_0.
This is technically true and this answer could be correct if the traffic would not match the SDWAN rule.
We have to assume no other rules would match and it would hit the implicit ruleset.
The implicit ruleset uses the FIB to determine the outgoing interface.
Now the route in the FIB with lowest priority will get selected.
Answer A could be correct, we are missing some relevant info.
upvoted 1 times

83e48be 12 months ago

Because there is no output shown regarding PBR it is not known if PBR could interface.
PBR is performed before SDWAN so anything in SDWAN becomes irrelevant.
Answer B could be correct, we are missing relevant info.

Route priority difference has no impact on the route added to the active routing table.
(Distance and weight will and only the best one will be added)
Both T_INET_0 and T_INET_1 should show in the output.
In this output only T_INET_1 is shown as a valid destination for 10.0.0.0/8.
SDWAN members don't have a specific subnet as destination, rather 0.0.0.0/0.
The presence of a more specific subnet implies the use of addditional config beyond what is shown.
Ex. set default / set gateway , static route etc.
Because T_INET_0 is not mentioned at all , all we know is there is no valid route to 10.0.0.0/8.
Answer D is correct.
upvoted 1 times

83e48be 12 months ago

The only one we can safely count as wrong is C.
There is nothing in the SDWAN rule that leads to T_INET_1 preferred over T_INET_0.

Once again....poor question/example.
On an actual exam my best bet would be A+D.
There is nothing shown about PBR, thus would be the least valid answer.
At least A has some relevance...
upvoted 1 times

83e48be 12 months ago

Here , if examtopics wont allow a long comment I will just cut it into smaller sections =D
upvoted 1 times

ipv84 1 year ago

I think too... right answers are B & D.
upvoted 2 times

Question #18 *Topic 1*

Within IPsec tunnel templates available on FortiManager, which template will you use to configure static tunnels for a hub and spoke topology?

A. Hub_IPsec_Recommended

B. Static_IPsec_Recommended

C. IPsec Fortinet Recommended

D. Branch IPsec Recommended

Suggested Answer: *A*

Community vote distribution

D (88%) 13%

SuperK Highly Voted 1 year ago

Selected Answer: D

Recommended templates will allow you to prepare a template for IPsec tunnels using Fortinet recommended settings for phase1 and phase2 parameters.

• The IPsec_Fortinet_Recommended template defines a template for a static point-to-point tunnel

• The BRANCH_IPsec_Recommended template defines a template for a static tunnel (with a known remote IP address)

• The HUB_IPsec_Recommended template defines a template for a dynamic tunnel (an IPsec hub for dial-up tunnels)

upvoted 6 times

Slikings Most Recent 1 month, 3 weeks ago

Selected Answer: D

A: Hub IPSEC template is a template that creates dynamic ipsec VPN with OI, PSK, and IP range.

B: Does not exists, its to throw you off with the term static.

C: IPSEC fortinet recommended template defines a static point to point tunnel.

D: correct, branch IPSEC defines a template for a static tunnel. Think branch as in branch locations.

upvoted 1 times

ccie8122 5 months ago

Selected Answer: D

"The HUB_IPsec_Recommended template defines a template for a dynamic tunnel"

upvoted 1 times

rac_sp 6 months ago

Selected Answer: D

branch ipsec recommended is the template correct

upvoted 1 times

Fanny1493 7 months, 3 weeks ago

Selected Answer: D

D is correct

upvoted 3 times

truserud 11 months, 1 week ago

Selected Answer: D

D is correct. See page 59 in the 7.2 Study Guide which explains that Branch_ipsec_recommended is what defines a template for a STATIC tunnel.

upvoted 3 times

alejandrofern43 1 year ago

Selected Answer: D

D is correct. Page 58 stududy guide 7.2 For Static tunnel is The BRANCH_IPsec_Recommended template defines a template for a static tunnel (with a known

remote IP address)

upvoted 3 times

f194908 1 year ago

Selected Answer: D

According Study Guide 7.2 page 59:

The Branch_IPsec_Recommended template defines a template for a static tunnel

upvoted 3 times

ee0808 1 year ago

Selected Answer: D

D

Dynamic tunnels on hub

Static tunnels on spokes

upvoted 3 times

Tommy_S 1 year ago

Selected Answer: A

A is correct

upvoted 1 times

Tommy_S 1 year ago

D is the correct one.

Study guid p59

upvoted 2 times

Manilo 1 year ago

Selected Answer: D

Should be D.... Question says: "to configure static tunnels for a hub and spoke topology"

According Study Guide 7.2 page 59:

The Branch_IPsec_Recommended template defines a template for a static tunnel

upvoted 3 times

KavinT 1 year ago

Selected Answer: A

A is correct.

Refer to below link

https://docs.fortinet.com/document/fortimanager/7.4.2/administration-guide/959026/recommended-ipsec-templates

upvoted 1 times

JP0421 1 year ago

Selected Answer: A

HUB_IPSec_Recommended - Fortinet's recommended template for hub IPSec tunnels.

Branch_IPSec_Recommended - Fortinet's recommended template for IPSec branch device configurations.

IPSec_Fortinet_ Recommended - Fortinet's recommended template for IPSec configurations.This template is not used for SD-WAN configuration.

upvoted 1 times

Question #19 *Topic 1*

The administrator uses the FortiManager SD-WAN overlay template to prepare an SD-WAN deployment. With information provided through the SD-WAN overlay template wizard, FortiManager creates templates ready to install on spoke and hub devices.
Select three templates created by the SD-WAN overlay template for a spoke device. (Choose three.)

A. IPsec tunnel template

B. BGP template

C. Overlay template

D. System template

E. CLI template

Suggested Answer: *ABE*

Community vote distribution

ABE (100%)

alejandrofern43 Highly Voted 6 months ago

Selected Answer: ABE

pag 74 Study_guide7.2
A. IPsec tunnel template
B. BGP template
E. CLI template
upvoted 5 times

lucient 5 months ago

But it's page 75.
upvoted 1 times

KavinT Most Recent 6 months, 3 weeks ago

Selected Answer: ABE

A & B & E are correct.

Refer to the below link
https://docs.fortinet.com/document/fortimanager/7.4.2/administration-guide/28292/objects-and-templates-created-by-the-sd-wan-overlay-template
upvoted 4 times

Question #20 *Topic 1*

Refer to the exhibit.

```
branch1_fgt # diagnose firewall proute list
list route policy info(vf=root):

id=1 dscp_tag=0xff 0xff flags=0x0 tos=0x00 tos_mask=0x00 protocol=17 sport=0-65535 iif=7
dport=53 path(1) oif=3(port1)
source wildcard(1): 0.0.0.0/0.0.0.0
destination wildcard(1): 4.2.2.1/255.255.255.255
hit_count=0 last_used=2022-03-25 10:53:26

id=2131165185(0x7f070001) vwl_service=1(Critical-DIA) vwl_mbr_seq=1 2 dscp_tag=0xff 0xff
flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 sport=0-65535 iif=0 dport=1-65535 path(2)
oif=3(port1) oif=4(port2)
source(1): 10.0.1.0-10.0.1.255
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(3): GoToMeeting(4294836966,0,0,0, 16354)
Microsoft.Office.365.Portal(4294837474,0,0,0, 41468) Salesforce(4294837976,0,0,0, 16920)
hit_count=0 last_used=2022-03-24 12:18:16

id=2131165186(0x7f070002) vwl_service=2(Non-Critical-DIA) vwl_mbr_seq=2 dscp_tag=0xff
0xff flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 sport=0-65535 iif=0 dport=1-65535
path(1) oif=4(port2)
source(1): 10.0.1.0-10.0.1.255
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(2): Facebook(4294836806,0,0,0, 15832) Twitter(4294838278,0,0,0, 16001)
hit_count=0 last_used=2022-03-24 12:18:16

id=2131165187(0x7f070003) vwl_service=3(all_rules) vwl_mbr_seq=1 dscp_tag=0xff 0xff
flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 sport=0-65535 iif=0 dport=1-65535 path(1)
oif=3(port1)
source(1): 0.0.0.0-255.255.255.255
destination(1): 0.0.0.0-255.255.255.255
hit_count=0 last_used=2022-03-25 10:58:12
```

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

A. Entry 1 (id=1) is a regular policy route.

B. There is more than one SD-WAN rule configured.

C. The SD-WAN rules take precedence over regular policy routes.

D. The all_rules rule represents the implicit SD-WAN rule.

Suggested Answer: *AB*

Community vote distribution

AB (100%)

mader 2 weeks, 3 days ago

Selected Answer: AB

A & B correct

D not correct, implicit rule has service id=0, https://community.fortinet.com/t5/FortiGate/Troubleshooting-Tip-Implicit-SD-WAN-Rule-ID-not-showing-on/ta-p/299366

upvoted 1 times

sugar12 4 months ago

Selected Answer: AB

C & D are wrong therefore A & B are correct because for A there is no VWL_Service which makes it no SDWAN proute while for B there is more than one VWL_Service rules with ID >6535

upvoted 1 times

truserud 5 months, 1 week ago

Selected Answer: AB

A & B are correct - detailed on pages through 127 - 129 in the 7.2 Study Guide.

upvoted 2 times

KavinT 6 months, 3 weeks ago

Selected Answer: AB

A & B are correct

upvoted 2 times

IBB90704 6 months, 3 weeks ago

A y B son correctas

upvoted 2 times

Question #21 *Topic 1*

What are two benefits of using forward error correction (FEC) in IPsec VPNs? (Choose two.)

A. FEC can leverage multiple IPsec tunnels for parity packets transmission.

B. FEC transmits parity packets that can be used to reconstruct packet loss.

C. FEC improves reliability of noisy links.

D. FEC supports hardware offloading.

Suggested Answer: *BC*

Community vote distribution

BC (100%)

amadeu 9 months, 1 week ago

Underlay: Refers to the physical infrastructure of the network

Overlay: Refers to a virtual network layer that is built on top of the underlay infrastructure.

R=>D= Therefore there are 4 virtual overlay interfaces

upvoted 1 times

sugar12 10 months ago

Selected Answer: BC

A. wrong - doesn't make sense

B. correct - that is the main reason of using FEC on ipsec overlays

C. correct - that is the main reason of using FEC on ipsec overlays

D. wrong - once you enable FEC on a policy offloading is automatically disabled

upvoted 1 times

alejandrofern43 1 year ago

Selected Answer: BC

B y C PAG 256 SDWAN 7.2

upvoted 2 times

KavinT 1 year ago

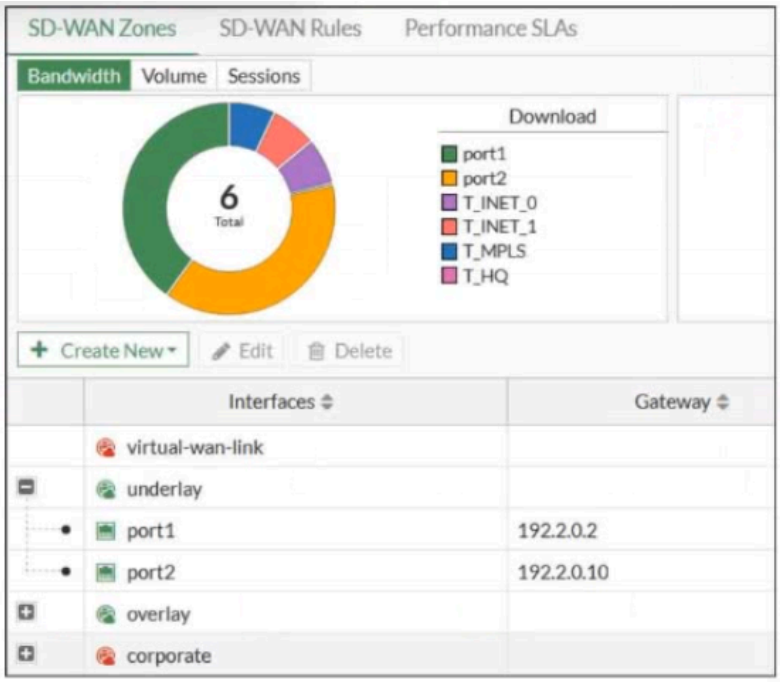
Selected Answer: BC

Refer to Page 257 in SD WAN 7.2

upvoted 2 times

Question #22 *Topic 1*

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



Based on the exhibit, which statement is true?

A. You can move port1 from the underlay zone to the overlay zone.

B. You can delete the virtual-wan-link zone because it contains no member.

C. The corporate zone contains no member.

D. The overlay zone contains four members.

Suggested Answer: *D*

Community vote distribution

A (90%) 10%

Slikings 1 month, 1 week ago

Selected Answer: A

SD-Wan zone cannot be deleted. The only information we have to confirm how many members are in each zone is that there has to be 1 therefore we can subtract from the ones we know to be true and it could not add up to be correct.

Therefore answer A is correct because members can be moved

upvoted 1 times

ccie8122 5 months ago

Selected Answer: A

D is incorrect since of the 6 members, 2 are in the "underlay" zone, that means the remaining four must be split between the "overlay" and "corporate" zones. Since members can only exist in one zone, and since both "corporate" and "overlay" must each have at least one member. Thus member distribution must either be "corporate" = 1, "overlay" = 3; OR "corporate" = 2, "overlay" = 2; OR "corporate" = 3, "overlay" = 1.

From this logic, C cannot be true, and D cannot be true. And since the v-w-l is used for upgrades and new links, it cannot be deleted - B must be false.

Only A is left . . .

upvoted 2 times

truserud 11 months, 1 week ago

Selected Answer: A

A is correct. Tested in lab, also check the details provided in my othe comment here to provide further comment on why the other alternatives are wrong.

upvoted 3 times

Tommy_S 1 year ago

Selected Answer: A

A is correct. Also tested it.

upvoted 3 times

ee0808 1 year ago

Selected Answer: A

A

It is possible to move port, have just tested it - Edit on port 1, change SD-WAN zone to overlay

Since there is a plus sign next to corporate, it contains member(s) - so the overlay zone can not contain all the remaining 4 members

upvoted 3 times

KavinT 1 year ago

Selected Answer: D

A. not true - you cannot move port 1 since it is referenced in a rule.

B. not true - you cannot delete default virtual-wan-link zone

C. not true - Corporate may have members but are not active. Thus the red colour.

D. TRUE - The 4 tunnels are in the overlay zone.

upvoted 1 times

truserud 11 months, 1 week ago

You can actually move the interface between zones, as the zone is what is referenced in firewall rules.

D is wrong, as there are 6 members in total, 2 of which are in the underlay zone. As the Corporate zone has the "+" icon, it indicates that there are in fact members in this zone. Thus D is incorrect, as there can't be 4 members in the overlay zone because of the 6 total members.

upvoted 4 times

Question #23 *Topic 1*

Refer to the exhibit.

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

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

A. FortiGate terminates the old sessions.

B. FortiGate evaluates new sessions.

C. FortiGate does not change existing sessions.

D. FortiGate flushes all sessions.

Suggested Answer: *BC*

Community vote distribution

BC (100%)

mader 2 weeks, 2 days ago

Selected Answer: BC

pg 162 study guide 7.2

upvoted 2 times

Slikings 1 month, 1 week ago

Selected Answer: BC

check-new = new sessions are flagged as dirty however existing sessions are not affected.

check-all all sessions are dirty

upvoted 1 times

sugar12 4 months ago

Selected Answer: BC

check-new: New sessions are flagged as dirty. Existing sessions are not affected.

If the firewall handles a huge number of sessions, flagging all sessions as dirty, and performing a firewall policy lookup for the sessions may result in high CPU utilization. To prevent this, you can configure FortiGate to flag only new sessions as dirty by setting firewall-session-dirty to check-new. The result is that FortiGate evaluates only new sessions against the new firewall policy configuration.

upvoted 2 times

KavinT 6 months, 3 weeks ago

Selected Answer: BC

B & C are correct.

upvoted 4 times

Question #24 *Topic 1*

Refer to the exhibit.

```
# diagnose sys session list

session info: proto=6 proto_state=01 duration=39 expire=3593 timeout=3600 flags=00000000
socktype=0 sockport=0 av_idx=0 use=4
state=may_dirty npu
orgin->sink: org pre->post, reply pre->post dev=7->5/5->7 gwy=10.10.10.1/10.9.31.160
hook=pre dir=org act=noop 10.9.31.160:7932->10.0.1.7:22(0.0.0.0:0)
hook=post dir=reply act=noop 10.0.1.7:22->10.9.31.160:7932(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00045e02 tos=ff/ff app_list=0 app=0 url_cat=0
sdwan_mbr_seq=1 sdwan_service_id=1
rpdb_link_id=80000000 rpdb_svc_id=0 ngfwid=n/a
npu_state=0x4000c00
npu info: flag=0x81/0x81, offload=8/8, ips_offload=0/0, epid=64/76, ipid=76/64,
vlan=0x0000/0x0000
vlifid=76/64, vtag_in=0x0000/0x0000 in_npu=1/1, out_npu=1/1, fwd_en=0/0, qid=2/2
reflect info 0:
dev=7->6/6->7
npu_state=0x4000800
npu info: flag=0x00/0x81, offload=0/8, ips_offload=0/0, epid=0/76, ipid=0/65, vlan=0x0000/0x0000
vlifid=0/65, vtag_in=0x0000/0x0000 in_npu=0/1, out_npu=0/1, fwd_en=0/0, qid=0/2
total reflect session num: 1
total session 1

# diagnose netlink interface list

if=port1 family=00 type=1 index=5 mtu=1500 link=0 master=0
if=port2 family=00 type=1 index=6 mtu=1500 link=0 master=0
if=port3 family=00 type=1 index=7 mtu=1500 link=0 master=0
```

The exhibit shows the details of a session and the index numbers of some relevant interfaces on a FortiGate appliance that supports hardware offloading.

Based on the information shown in the exhibits, which two statements about the session are true? (Choose two.)

A. The main session cannot be offloaded to hardware.

B. The original direction of the symmetric traffic flows from port3 to port2.

C. The reply direction of the asymmetric traffic flows from port2 to port3.

D. The auxiliary session can be offloaded to hardware.

Suggested Answer: *CD*

Community vote distribution

CD (100%)

2c34985 4 days, 20 hours ago

Selected Answer: CD

A- wrong : traffic can be offloaded

B- must be wrong : 7>5 means port 3 to 1

and B +C CANNOT be true at the same time overwise traffic became symmetrical 3-2 2-3

C- correct : 6>7 means port 2 to 3

D- correct : all the session can be offloaded

upvoted 1 times

4aeb5f8 2 months, 2 weeks ago

Selected Answer: CD

Per Study Guide page 160, C and D are the correct answeres

upvoted 1 times

sugar12 3 months, 4 weeks ago

Selected Answer: CD

A - wrong both sessions can be offloaded to hardware

B - wrong the orogonial direction is from 7 to 5 which is translated from port 3 to port 1

C - Correct reply is from 6 to 7 which is port 2 to port 3

D - correct - offload 0/8

upvoted 2 times

truserud 5 months, 1 week ago

Selected Answer: CD

C & D are correct. Check out page 160 in the 7.2 Study guide.

upvoted 3 times

KavinT 6 months, 3 weeks ago

Selected Answer: CD

C & D are correct.

upvoted 3 times

Question #25 *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 three mandatory post-run tasks that must be performed? (Choose three.)

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

B. Assign a branch_id metadata variable to each branch device.

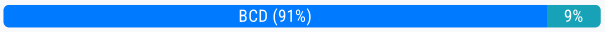
C. Create policy packages for branch devices.

D. Configure SD-WAN rules.

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

Suggested Answer: *BDE*

Community vote distribution



ccie8122 5 months ago

Selected Answer: BCD

SG page 76:
"you must define a unique branch ID value for each branch device"
"Mandatory . . .
- Configure the SD-WAN rules by editing the SD-WAN template
- Create policy packages for branch and hub devices"
upvoted 1 times

sugar12 10 months ago

Selected Answer: BCD

BCD page 75
upvoted 1 times

truserud 11 months, 1 week ago

Selected Answer: BCD

B, C & D are correct. This is detailed on page 76 in the Study Guide.
upvoted 2 times

alejandrofern43 1 year ago

Selected Answer: BCD

B,C,D pag 75 study guide 7.2
upvoted 3 times

gogudindeal 1 year ago

BCD
Page 76 study guide
upvoted 2 times

ee0808 1 year ago

Selected Answer: BCD

BCD
Policy packages are not created with SD-WAN overlay template
Routing is provided by BGP templates created with SD-WAN overlay template
upvoted 2 times

LoukasR 1 year ago

B,C,D pg 76 study guide
upvoted 3 times

Tommy_S 1 year ago

Selected Answer: BCD

B,C,D are correct. See study guide p76

upvoted 2 times

KavinT 1 year ago

Selected Answer: BCD

Answer is B, C, D

upvoted 1 times

KavinT 1 year ago

Selected Answer: BDE

B & D & E are correct.

A is not correct - SD WAN ID cannot be assigned.
B is not correct - Routing needs to be done first.

upvoted 1 times

truserud 11 months, 1 week ago

You answered that BDE is correct, but then you are saying that B is not correct? B is also correct as the metafield branch_id is created by the overlay template as stated on page 76 in the study guide. E is incorrect, as that is created with the BGP template created by the SD-WAN overlay template.

upvoted 1 times

Question #26 *Topic 1*

Refer to the exhibit.

```
config firewall policy
    edit 1
        set anti-replay disable
    next
end
```

In a dual-hub hub-and-spoke SD-WAN deployment, which is a benefit of disabling the anti-replay setting on the hubs?

A. It instructs the hub to skip content inspection on TCP traffic, to improve performance.

B. It instructs the hub to not check the ESP sequence numbers on IPsec traffic, to improve performance.

C. It instructs the hub to disable TCP sequence number check, which is required for TCP sessions originated from spokes to fail over back and forth between the hubs.

D. It instructs the hub to disable the reordering of TCP packets on behalf of the receiver, to improve performance.

Suggested Answer: *B*

Community vote distribution

C (100%)

Fanny1493 7 months, 3 weeks ago

Selected Answer: C

Answer C

upvoted 2 times

OrioN88 8 months, 3 weeks ago

Selected Answer: C

100% C

upvoted 2 times

sugar12 10 months ago

Selected Answer: C

c - by disabling the anti-replay setting. When you disable anti-replay,
FortiGate doesn't check sequence numbers of TCP packets

upvoted 3 times

nse_student 11 months, 3 weeks ago

Selected Answer: C

C is ok

upvoted 2 times

alejandrofern43 1 year ago

Selected Answer: C

C is correct Page: 164 on 7.2 Guide

upvoted 2 times

Tommy_S 1 year ago

Selected Answer: C

C is Correct

upvoted 2 times

KavinT 1 year ago

Selected Answer: C

Refer to below explanation from JP0421

upvoted 2 times

JP0421 1 year ago

Selected Answer: C

Page: 164 on 7.2 Guide

upvoted 3 times

Question #27 *Topic 1*

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

A. The session information output displays no SD-WAN-specific details.

B. All SD-WAN rules have the default and gateway setting enabled.

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

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

Suggested Answer: *AC*

Community vote distribution

ccie8122 4 months, 4 weeks ago

Selected Answer: AC

D is incorrect. SG p 180: "when you enable SD-WAN on FortiGate, FortiOS hides the v4-ecmp-mode setting and replaces it with the load-balance-mode setting"

C is correct. SG p 311: Order of route lookup precedence = Policy Routes > ISDB routes > SD-WAN rules > route-cache > RIB/FIB. THus, if traffic matches any proute, the traffic would be routed by proute, not by SD-WAN rule.

upvoted 1 times

Fanny1493 7 months, 3 weeks ago

Selected Answer: AD

Answer A and D

upvoted 1 times

ccie8122 5 months ago

Not correct. See my response above.

upvoted 1 times

d567468 9 months, 4 weeks ago

Selected Answer: AC

The other statements, B and D, are not correct because:

B. All SD-WAN rules have the default and gateway setting enabled.

This is not necessarily true for the implicit rule, as it functions as a fallback and does not need explicit default and gateway settings enabled in the context of user-defined SD-WAN rules.

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

This statement may be partially correct in some contexts, but it does not specifically apply to traffic matching the implicit SD-WAN rule, which is more about the traffic not matching any of the defined rules rather than how it gets load balanced. The implicit rule typically uses default routing behavior rather than any special load balancing algorithm.

upvoted 2 times

sugar12 10 months ago

Selected Answer: AC

A. correct - If the session matched the SD-WAN

implicit rule, and therefore was handled using standard FIB routing, these SD-WAN fields do not appear.

page 149

C. correct - if traffic doesnt match any entry in the proute table then it will use the implicity deny SD-WAN rule

D. wrong - load-balance-mode replaces v4-ecmp-mode when SD-WAN is enabled - page 179

B. therefore B is wrong

upvoted 2 times

NaomiLimJQ 11 months, 2 weeks ago

should be C and D

upvoted 2 times

ipv84 1 year ago

Why not "D" ?

upvoted 2 times

r3n0 10 months, 3 weeks ago

Because v4-ecmp-mode is replaced by load-balance-mode when SDWAN is enable.

upvoted 3 times

gogudindeal 1 year ago

AC

Studi guide page 150

If the session matched the SD-WAN

implicit rule, and therefore was handled using standard FIB routing, these SD-WAN fields do not appear.

upvoted 1 times

KavinT 1 year ago

Selected Answer: AC

A & C are correct

upvoted 1 times

Question #28 *Topic 1*

Refer to the exhibits.

Exhibit A -

```
config duplication
    edit 1
       set srcaddr "10.0.1.0/24"
       set dstaddr "10.1.0.0/24"
       set srcintf "port5"
       set dstintf "overlay"
       set service "ALL"
       set packet-duplication force
    next
end
```

```
branch1_fgt # diag sys sdwan zone
Zone overlay index=3
     members(3): 19(T_INET_0) 20(T_INET_1) 21(T_MPLS)
Zone underlay index=2
     members(2): 3(port1) 4(port2)
Zone virtual-wan-link index=1
     members(0):
```

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

Exhibit B -

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

Exhibit A shows the packet duplication rule configuration, the SD-WAN zone status output, and the sniffer output on a FortiGate device acting as the sender. Exhibit B shows the sniffer output on a FortiGate device acting as the receiver.
The administrator configured packet duplication on both FortiGate devices. The sniffer output on the sender FortiGate shows that FortiGate forwards an ICMP echo request packet over three overlays, but it only receives one reply packet through T_INET_1.
Based on the output shown in the exhibits, which two reasons can cause the observed behavior?
(Choose two.)

A. The ICMP echo request packets sent over T_INET_0 and T_MPLS were dropped along the way.

B. On the receiver FortiGate, packet-de-duplication is enabled.

C. On the sender FortiGate, duplication-max-num is set to 3.

D. The sender FortiGate has anti-replay enabled to block duplicate ICMP replies.

Suggested Answer: *BC*

Community vote distribution

BC (100%)

FriedExams 1 month, 1 week ago

Selected Answer: BC

B and C

Yes, deduplication on the other end drops the packets. However, it is on the FortiGate and not along the way.

upvoted 1 times

sugar12 3 months, 3 weeks ago

Selected Answer: BC

b & C page260

upvoted 2 times

alejandrofern43 6 months ago

Selected Answer: BC

pag 260 guide 7.2

B y C is correct

upvoted 2 times

gogudindeal 6 months, 1 week ago

bc

page 261

upvoted 2 times

KavinT 6 months, 3 weeks ago

Selected Answer: BC

B and C are correct

upvoted 3 times

Question #29 *Topic 1*

Refer to the exhibit.

```
ike 0:T_INET_0:4: received informational request
ike 0:T_INET_0:4: processing notify type SHORTCUT_OFFER
ike 0:T_INET_0: shortcut-offer 10.0.1.101->10.0.2.101 0 psk 64 ppk 0 ver 2
mode 0, peer-addr 203.0.113.1:500
ike 0 looking up shortcut by addr 10.0.2.101, name T_INET_0, peer-addr
203.0.113.1:500
ike 0:T_INET_0: send shortcut-query 821242144571674185
e7132541b71ac3ea/0000000000000000 192.2.0.1 10.0.1.101->10.0.2.101 0 psk 64
```

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

A. This is a spoke that has received an offer from a remote hub.

B. Two spokes, 192.2.0.1 and 10.0.2.101, establish a shortcut.

C. This is a hub that has received an offer from a spoke and has forwarded it to another spoke.

D. An IKE session is established between 10.0.1.101 and 10.0.2.101 in the process of forming a shortcut tunnel.

Suggested Answer: *C*

Community vote distribution

A (95%) 5%

alejandrofern43 Highly Voted 1 year ago

Selected Answer: A

PAG 279 SDWAN 7.2

A. This is a spoke that has received an offer from a remote hub.

upvoted 5 times

ccie8122 Most Recent 5 months ago

Selected Answer: A

SG p 280:

"Spoke 1 output - spoke 1 receives shortcut offer from hub, and then sends shortcut querty to hub:

. . .

"received informational request

processing notify type SHORTCUT_OFFER

. .

send shortcut query . . ."

this is the exact debug output in this exhibit

upvoted 2 times

[Removed] 8 months, 2 weeks ago

Selected Answer: A

A. page 279

upvoted 2 times

OrioN88 8 months, 3 weeks ago

Selected Answer: A

A.

If it was a hub, it would not send a shortcut-query in response but rather forward the shortcut-offer.

upvoted 2 times

sugar12 10 months ago

Selected Answer: A

A. page 279

upvoted 2 times

ginmco 11 months, 1 week ago

Study Guide page 180.
A. This is a spoke that has received an offer from a remote hub.
upvoted 3 times

ee0808 1 year ago
Selected Answer: A
A
SHORTCUT OFFER is SENT from hub, and RECEIVED on originating spoke
upvoted 4 times

Tommy_S 1 year ago
Selected Answer: A
A is correct
upvoted 3 times

SuperK 1 year ago
I think B.
upvoted 1 times

SuperK 1 year ago
Sorry mistake The Answer is A.
Refer to Page 280, SD WAN 7.2
upvoted 3 times

KavinT 1 year ago
Please disregard below answers. Correct answer is A.

Refer to Page 280
upvoted 1 times

KavinT 1 year ago
Refer to Page 260 - SD WAN 7.2
upvoted 2 times

KavinT 1 year ago
Selected Answer: B
Answer is B.
Refer to Page 280, SD WAN 7.2
upvoted 1 times

ac89l 1 year ago
according to page 280, it is answer A
upvoted 2 times

Question #30 *Topic 1*

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

A. By default, FortiGate does not check if the selected member has a valid route to the destination.

B. You must configure each local-out feature individually, to use SD-WAN.

C. By default, local-out traffic does not use SD-WAN.

D. FortiGate does not consider the source address of the packet when matching an SD-WAN rule for local-out traffic.

Suggested Answer: *BC*

Community vote distribution

sugar12 3 months, 3 weeks ago

Selected Answer: BC

B and C page 175

upvoted 1 times

alejandrofern43 6 months ago

Selected Answer: BC

PAG 175 SDWAN 7.2

upvoted 1 times

gogudindeal 6 months, 1 week ago

BC

page 176

upvoted 1 times

KavinT 6 months, 3 weeks ago

Selected Answer: BC

B and C are correct

upvoted 2 times

Question #31 *Topic 1*

Refer to the exhibits.

Exhibit A -

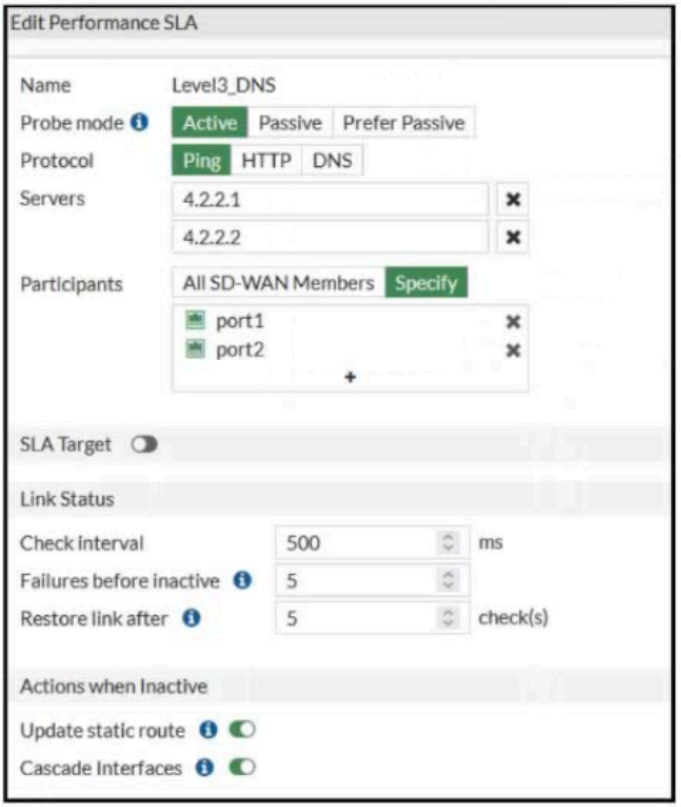


Exhibit B -

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

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

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

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

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

A. Host 8.3.8.8 is reachable through port1 and port2.

B. Port2 becomes alive after three successful probes are detected.

C. The administrator manually restores the static routes for port2, if port2 becomes alive.

D. FortiGate disables all static routes for port2.

Suggested Answer: *D*

Community vote distribution

D (100%)

alejandrofern43 6 months ago

Selected Answer: D

d is correct

upvoted 1 times

IBB90704 6 months, 2 weeks ago

La D es correcta

upvoted 1 times

KavinT 6 months, 3 weeks ago

Selected Answer: D

D is correct

upvoted 2 times

Question #32 *Topic 1*

In which SD-WAN template field can you use a metadata variable?

A. You can use metadata variables only to define interface members and the gateway IP.

B. Any field identified with a dollar sign (S) in a magnifying glass.

C. Any field identified with an "M" in a circle.

D. All SD-WAN template fields support metadata variables.

Suggested Answer: *C*

Community vote distribution

B (100%)

alejandrofern43 6 months ago

Selected Answer: B

pag 47

B. Any field identified with a dollar sign (S) in a magnifying glass.

upvoted 2 times

ee0808 6 months, 1 week ago

Selected Answer: B

B is correct

upvoted 2 times

Tommy_S 6 months, 1 week ago

Selected Answer: B

B is correct

upvoted 2 times

IBB90704 6 months, 2 weeks ago

La B es correcta

upvoted 2 times

JP0421 6 months, 3 weeks ago

Selected Answer: B

Page 48: 7.2 Study Guide

upvoted 2 times

KavinT 6 months, 3 weeks ago

Selected Answer: B

Correct answer is B.

Refer to Page 48 - SD WAN 7.2

upvoted 3 times

Question #33 *Topic 1*

Refer to the exhibit.

```
# get router info routing-table all
...
B    10.0.2.0/24 [200/0] via 10.201.1.2 [3] (recursive is directly connected, VPN0), 00:26:48, [1/0]
                 [200/0] via 10.202.1.2 [3] (recursive is directly connected, VPN1), 00:26:48, [1/0]
                 [200/0] via 10.203.1.1 [3] (recursive is directly connected, VPN2), 00:26:48, [1/0]
...
```

The device exchanges routes using IBGP.

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

A. Each BGP route is three hops away from the destination.

B. ibgp-multipath is disabled.

C. You can run the get router info routing-table database command to display the additional paths.

D. additional-path is enabled.

Suggested Answer: *CD*

Community vote distribution

CD (100%)

mader 1 week, 6 days ago

Selected Answer: CD

pg 241

upvoted 1 times

alejandrofern43 6 months ago

Selected Answer: CD

pag 239

C. You can run the get router info routing-table database command to display the additional paths.

D. additional-path is enabled.

upvoted 4 times

KavinT 6 months, 3 weeks ago

Selected Answer: CD

C & D are correct

upvoted 1 times

KavinT 6 months, 3 weeks ago

C and D are correct

upvoted 1 times

Question #34 *Topic 1*

Refer to the exhibit, which shows output of the command diagnose sys sdwan health-check status collected on a FortiGate device.

```
# diagnose sys sdwan health-check status

Health Check(Level3_DNS):
Seq(1 port1): state(alive), packet-loss(0.000%) latency(22.129), jitter(0.201), mos(4.393),
bandwidth-up(10235), bandwidth-dw(10235), bandwidth-bi(20470) sla_map=0x0
Seq(2 port2): state(alive), packet-loss(7.000%) latency(42.394), jitter(0.912), mos(4.378),
bandwidth-up(10236), bandwidth-dw(10237), bandwidth-bi(20473) sla_map=0x0
Health Check(VPN_PING):
Seq(5 T_MPLS): state(alive), packet-loss(0.000%) latency(131.336), jitter(0.199), mos(4.330),
bandwidth-up(9999999), bandwidth-dw(9999999), bandwidth-bi(19999998) sla_map=0x2
Seq(4 T_INET_1): state(alive), packet-loss(11.000%) latency(1.465), jitter(0.226), mos(4.398),
bandwidth-up(10239), bandwidth-dw(10239), bandwidth-bi(20478) sla_map=0x1
Seq(3 T_INET_0): state(alive), packet-loss(0.000%) latency(1.440), jitter(0.245), mos(4.403),
bandwidth-up(10239), bandwidth-dw(10239), bandwidth-bi(20478) sla_map=0x3
```

Which two statements are correct about the health check status on this FortiGate device? (Choose two.)

A. The interface T_INET_0 missed three SLA targets.

B. The interface T_INET_1 missed one SLA target.

C. There is no SLA criteria configured for the health-check Level3_DNS.

D. The health-check VPN_PING orders the members according to the measured jitter.

Suggested Answer: *BC*

Community vote distribution

CD (59%) BC (36%) 5%

Lomik29 Highly Voted 12 months ago

B & C are correct, guide p.227. 0x1 means that only SLA target #1 passed. 0x2 means SLA target #2 passed/ 0x3 means both SLA targets passed

upvoted 11 times

sugar12 Highly Voted 9 months, 3 weeks ago

Selected Answer: CD

A. wrong T_INET_0 0x3 that means it passed 2 sla targets. If it missed then it
missed 1 SLA target which is the 3bit in the SLA_MAP binary 3rd bit 4(0 off) 2nd bit 2(1bit on) first 1(1bit on)

B. wrong T_INET_1 0x1 that means it passed 1 sla target. if it missed then it missed
2 2nd and 3rd bit in the sla_MAP

therefore what is left is C,D correct

upvoted 7 times

woodyrj Most Recent 2 days, 6 hours ago

Selected Answer: CD

This question depends how many targets were set which is not mentioned. If 3 targets were set then B is incorrect as 0x3 means it failed two targets, as one of the answers says that an interface missed three targets, in this rate I would have to choose CD

upvoted 1 times

mader 1 week, 6 days ago

Selected Answer: CD

A-missed 1

B-missed 2

C-correct, 0x0, pg 316

upvoted 1 times

sven22 1 month, 2 weeks ago

Selected Answer: BC

This could be C&D, but the question is more around the health check and what has and has not passed, therefore I feel that B&C are correct, B could also be stated that T_MPLS has missed 1 target as well, that is if the assumption is there are 2 targets.