Exam Questions FCSS_SDW_AR-7.4

FCSS - SD-WAN 7.4 Architect

https://www.2passeasy.com/dumps/FCSS_SDW_AR-7.4/

NEW QUESTION 1
Refer to the exhibits.

You use FortiManager to manage the branch devices and configure the SD-WAN template. You have configured direct internet access (DIA) for the IT department users. Now. you must configure secure internet access (SIA) for all local LAN users and have set the firewall policies as shown in the second exhibit.
Then, when you use the install wizard to install the configuration and the policy package on the branch devices, FortiManager reports an error as shown in the third exhibit.
Which statement describes why FortiManager could not install the configuration on the branches?

A. You must direct SIA traffic to a VPN tunnel.
B. You cannot install firewall policies that reference an SD-WAN zone.
C. You cannot install firewall policies that reference an SD-WAN member.
D. You cannot install SIA and DIA rules on the same device.

Answer: C

NEW QUESTION 2
SD-WAN interacts with many other FortiGate features. Some of them are required to allow SD-WAN to steer the traffic.
Which three configuration elements that you must configure before FortiGate can steer traffic according to SD-WAN rules? (Choose three.)

A. Firewall policies
B. Interfaces
C. Security profiles
D. Traffic shaping
E. Routing

Answer: ABE

NEW QUESTION 3
Which two statements correctly describe what happens when traffic matches the implicit SD-WAN rule? (Choose two.)

A. The session information output displays no SD-WAN service id.
B. Traffic is load balanced using the algorithm set for the v4-ecmp-mode setting.
C. The traffic is distributed, regardless of weight, through all available static routes.
D. Traffic does not match any of the entries in the policy route table.
E. FortiGate flags the session with may_dirty and vwl_def ault.

Answer: AD

NEW QUESTION 4
You are planning a new SD-WAN deployment with the following criteria:
- Two regions
- Most of the traffic is expected to remain within its region
- No requirement for inter-region ADVPN
To remain within the recommended best practices, which routing protocol should you select for the overlays?

A. OSPF for the routing within each region and EBGP between the regions.
B. IBGP with BGP on loopback within each region and EBGP between the regions.
C. IBGP with BGP per overlays within each region and IBGP with BGP on loopback between the regions.
D. IBGP within each region and between the regions.

Answer: B

NEW QUESTION 5
You are planning a large SD-WAN deployment with approximately 1000 spokes and want to allow ADVPN between the spokes. Some remote sites use FortiSASE to connect to the company's SD-WAN hub. Which overlay routing configuration should you use?

A. BGP on loopback with dynamic BGP for ADVPN shortcut routing.
B. BGP on loopback with IPsec phase2 selectors for ADVPN shortcut routing.
C. BGP per overlay with dynamic BGP for ADVPN shortcut routing.
D. BGP per overlay with BGP next-hop convergence for ADVPN shortcut routing.

Answer: A

NEW QUESTION 6
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. FodiGate accepts the deletion and removes routes as required.
B. FortiGate displays an error messag
C. You must use the CLI to delete an SD-WAN member.
D. FortiGate displays an error messag
E. SD-WAN zones must contain at least two members
F. FortiGate accepts the deletion and places the member in the default SD-WAN zone.

Answer: B

NEW QUESTION 7
Refer to the exhibits.

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.Portal(41469,0) Salesforce(16920,0) Collaboration(0,28)
  Src address(1):
10.0.1.0-10.0.1.255

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

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

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

branch1_fgt # get router info routing-table all
...
```

›n FortiAnalyzer

Application	Security Event List	SD-WAN Rule Name	Destination Interface
GoToMeeting	APP 2		port2
GoToMeeting	APP 2	Critical-DIA	port1
GoToMeeting	APP 2	Critical-DIA	port1
GoToMeeting	APP 2	Critical-DIA	port1
GoToMeeting	APP 2	Critical-DIA	port1
GoToMeeting	APP 2	Critical-DIA	port1
GoToMeeting	APP 2		port2
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

An administrator is testing application steering in SD-WAN. Before generating test traffic, the administrator collected the information shown in the first exhibit. After generating GoToMeeting test traffic, the administrator examined the corresponding traffic log on FortiAnalyzer, which is shown in the second exhibit.
The administrator noticed that the traffic matched the implicit SD-WAN rule, but they expected the traffic to match rule ID 1.
Which two reasons explain why some log messages show that the traffic matched the implicit SD-WAN rule? (Choose two.)

A. Full SSL inspection is not enabled on the matching firewall policy.
B. The session 3-tuple did not match any of the existing entries in the ISDB application cache.
C. FortiGate could not refresh the routing information on the session after the application was detected.
D. No configured SD-WAN rule matches the traffic related to the collaboration application GoToMeeting

Answer: BC

NEW QUESTION 8
Refer to the exhibits.

The exhibits show two IPsec templates to define Branch IPsec 1 and Branch_IPsec_2. Each template defines a VPN tunnel. The error message that FortiManager displayed when the administrator tried to assign the second template to the FortiGate device is also shown.
Which statement best describes the cause of the issue?

A. You can assign only one template with a tunnel type of static to each FortiGate device.
B. You can assign only one IPsec template to each FortiGate device.
C. You should review the branch1_fgt configuration for configured tunnels in the rootVDOM.
D. You should use the same outgoing interface of both templates.

Answer: B

NEW QUESTION 9
Refer to the exhibit that shows event logs on FortiGate.

Event log on FortiGate

```
6: date=2024-12-18 time=15:15:06 eventtime=1734563705745090691 tz="-0800" logid="0113022925" type="event" subtype="sdwan" leve
l="information" vd="root" logdesc="SDWAN SLA information" eventtype="SLA" healthcheck="HUB1_HC" slatargetid=1 interface="HUB1-
VPN3" status="up" latency="1.001" jitter="0.162" packetloss="0.000" moscodec="g711" mosvalue="4.404" inbandwidthavailable="10.
00Gbps" outbandwidthavailable="10.00Gbps" bibandwidthavailable="20.00Gbps" inbandwidthused="0kbps" outbandwidthused="0kbps" bi
bandwidthused="0kbps" slamap="0x1" msg="Health Check SLA status."

7: date=2024-12-18 time=15:14:26 eventtime=1734563666333265394 tz="-0800" logid="0101037141" type="event" subtype="vpn" level=
"notice" vd="root" logdesc="IPsec tunnel statistics" msg="IPsec tunnel statistics" action="tunnel-stats" remip=120.64.1.1 loci
p=192.2.0.1 remport=4500 locport=4500 outintf="port1" srccountry="Reserved" cookies="50b8a3684ddfd2cb/af3f725d883c5585" user="10
0.64.1.1" group="N/A" useralt="N/A" xauthuser="N/A" xauthgroup="N/A" assignip=172.168.1.1 vpntunnel="VPN4_0" tunnelip=N/A t
unnelid=3050027470 tunneltype="ipsec" duration=2968 sentbyte=245849 rcvdbyte=246456 nextstat=600 fctuid="N/A" advpnsc=0

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

9: date=2024-12-18 time=15:04:26 eventtime=1734563066334252138 tz="-0800" logid="0101037141" type="event" subtype="vpn" level=
"notice" vd="root" logdesc="IPsec tunnel statistics" msg="IPsec tunnel statistics" action="tunnel-stats" remip=172.16.1.1 loci
p=172.16.0.1 remport=500 locport=500 outintf="port4" srccountry="Reserved" cookies="ce1c2c62ecc04871/a4d93a059b8df005" user="1
72.16.1.1" group="N/A" useralt="N/A" xauthuser="N/A" xauthgroup="N/A" assignip=192.168.1.193 vpntunnel="HUB2-VPN3" tunnelip=N/
A tunnelid=3050027467 tunneltype="ipsec" duration=2367 sentbyte=195836 rcvdbyte=196492 nextstat=600 fctuid="N/A" advpnsc=0
```

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

A. The master tunnel HU82-VPN3 cannot accept ADVPN shortcuts.
B. The device steers voice traffic through the VPN tunnel HUB1-VPN3.
C. The VPN tunnel HUB1-VPN1_0 is a shortcut tunnel.
D. There is one shortcut tunnel built from master tunnel VPN4.

Answer: B

NEW QUESTION 10
Within the context of SD-WAN, what does SIA correspond to?

A. Remote Breakout
B. Local Breakout
C. Software Internet Access
D. Secure Internet Authorization

Answer: A

NEW QUESTION 10
......

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual FCSS_SDW_AR-7.4 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the FCSS_SDW_AR-7.4 Product From:

https://www.2passeasy.com/dumps/FCSS_SDW_AR-7.4/

Money Back Guarantee

FCSS_SDW_AR-7.4 Practice Exam Features:

* FCSS_SDW_AR-7.4 Questions and Answers Updated Frequently

* FCSS_SDW_AR-7.4 Practice Questions Verified by Expert Senior Certified Staff

* FCSS_SDW_AR-7.4 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* FCSS_SDW_AR-7.4 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year