FCSS SD-WAN 7.6 Architect

FCSS SD-WAN 7.6 Architect is the role-specific Fortinet Certified Solution Specialist examination for designing, deploying, and troubleshooting Fortinet SD-WAN with FortiOS 7.6. It is worth your time because it tests whether you can translate business requirement into a resilient design. *Memorising interface steps alone is not enough.*

1. Decoding the Exam and the Architect Mindset

Plain explanation, then precise meaning

Picture an architect approving a transport system. Every route must serve a purpose, and every failure requires a plan. The code **FCSS_SDW_AR-7-6** combines **FCSS** for Fortinet Certified Solution Specialist, **SDW** for SD-WAN, **AR** for Architect, and **7-6** for the tested FortiOS generation. The **SD-WAN Architect** exam therefore assesses design judgment alongside operational knowledge.

The published format is **60 questions in 60 minutes**; confirm current policy before booking.

Everyday example

For a retail chain, you would first map stores, data centres, applications, and recovery paths before choosing any configuration sequence.

Single common mistake

Treating the exam as a command-memorisation exercise. Design choices determine reachability and resilience, so scenario reasoning matters more.

2. Understanding the SD-WAN Architecture

Plain explanation, then precise meaning

An overlay is like a private road network carried above public highways. The **underlay** provides physical IP connectivity. The **overlay** uses logical IPsec tunnels between FortiGate devices.

Within FortiOS, a **zone** groups devices according to their architectural role. An **SD-WAN member** is an interface eligible to carry selected traffic.

Everyday example

In a three-branch design, each branch FortiGate might reach a central hub through a provider network, broadband, or cellular service.

Single common mistake

Confusing the overlay with the underlay. Changing a tunnel policy does not change the carrier circuit carrying it.

3. Selecting Paths with Rules, SLAs, and Health Checks

Plain explanation, then precise meaning

Think of a dispatcher choosing the best available vehicle for each parcel. An **SD-WAN rule** matches traffic and selects members. A **performance SLA** defines measurable latency, jitter, and packet-loss targets. A **health check** evaluates member reachability or quality. **BGP** can distribute routes.

A reachable member can still violate an SLA. Rule design must connect these mechanisms.

Everyday example

A shop sends card traffic through its low-latency private link but uses broadband when the primary path fails.

Single common mistake

Creating an SLA without applying it to a rule. The member may be healthy while receiving no matching traffic.

4. Separating Path Selection from Security Enforcement

Plain explanation, then precise meaning

Think of path selection as choosing a lane and security policy as deciding who may enter a building. An **SD-WAN rule** chooses an egress path. A **firewall policy** controls acceptance, denial, address translation, and service exposure.

IPsec protects the overlay, while central policies can provide consistent enforcement. When troubleshooting, work through the intended policy, member health, routing, tunnel state, and flow logs in that order.

Everyday example

For a branch-to-data-centre flow, an administrator checks the selected path and confirms that the application is permitted to use it.

Single common mistake

Treating an SD-WAN rule as a firewall policy. Choosing a path does not authorise the application.

5. Essential Vocabulary

- **Underlay**: the physical carrier network.
- **Overlay**: the logical tunnel network.
- **FortiGate**: Fortinet's security and SD-WAN appliance.
- **FortiOS**: the operating system running FortiGate.
- **Zone**: a logical grouping of SD-WAN devices.
- **SD-WAN member**: an interface participating in path selection.
- **Performance SLA**: measurable path-quality thresholds.
- **Health check**: a probe used to evaluate a member.
- **Application steering**: directing matched traffic towards selected members.
- **Fortinet SD-WAN Certification**: validation of role-specific SD-WAN expertise.

6. Self-Check, Conclusion, and FAQ

Five questions

1. **What does the examination code identify?**

   Answer: The Fortinet Certified Solution Specialist track, SD-WAN domain, Architect role, and FortiOS 7.6 generation.

2. **How do underlay and overlay differ?**

   Answer: The underlay supplies physical connectivity; the overlay supplies logical tunnels between sites.

3. **What connects SD-WAN rules, SLAs, and health checks?**

   Answer: Rules select members, SLAs define acceptable quality, and health checks determine usability.

4. **How does an SD-WAN rule differ from a firewall policy?**

   Answer: The rule selects a path; the firewall policy authorises and controls traffic.

5. **A failover does not occur. What should you inspect first?**

   Answer: The intended rule, member health, SLA state, routing, tunnel status, and matching logs.

Conclusion

Learn the architecture, then demonstrate steering, security, and troubleshooting in a FortiOS 7.6 lab. We prepare for the **FCSS SD-WAN 7.** **Architect** examination by reasoning from requirement to dependable design.

FAQ

Is older study material useless?

No. It explains enduring principles, but current 7.6 objectives must govern features and behaviour.

What knowledge should precede the exam?

You should be comfortable with IPv4 and IPv6, routing, BGP, IPsec, firewall policy, and FortiOS administration.

Fortinet

FCSS_SDW_AR-7.6 Exam

FCSS - SD-WAN 7.6 Architect

Thank you for Downloading FCSS_SDW_AR-7.6 exam PDF Demo

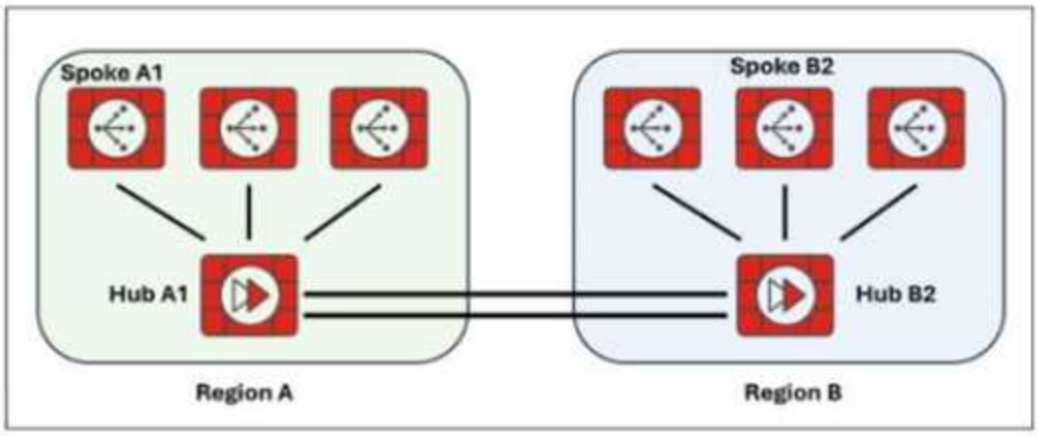
You can also try our FCSS_SDW_AR-7.6 Full Version Download

https://www.certkillers.net/Exam/FCSS_SDW_AR-7.6

Version: 4.2

Question: 1

Exhibit.



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

Which two configuration settings are required for the spoke A1 to establish an ADVPN shortcut with the spoke B2? (Choose two.)

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

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

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

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

Answer: A, D

Explanation:

To allow spokes in different hub-and-spoke groups to establish ADVPN shortcuts, the hubs must be configured to forward and send ADVPN shortcut offers. The key required settings on the hub are auto-discovery-forwarder (for VPNs to hubs) and auto-discovery-sender (for VPNs to spokes). This ensures the hub can facilitate and advertise ADVPN shortcut offers between spokes.
Reference:

[FCSS_SDW_AR-7.4 1-0.docx Q1]

Fortinet SD-WAN 7.4 ADVPN Guide (Auto-discovery settings for hub-and-spoke topologies)

Question: 2

Refer to the exhibit.

SD-WAN configuration on FortiGate

```
branch1_fgt # get router info routing-table all
...
S*      0.0.0.0/0 [1/0] via 192.2.0.2, port1, [1/0]
                  [1/0] via 192.2.0.10, port2, [10/0]
C       10.0.1.0/24 is directly connected, port5
B       10.1.0.0/24 [200/0] via 192.168.1.61 (recursive is directly connected, HUB1-VPN1), 1d03h58m, [1/0]
                    [200/0] via 192.168.1.125 (recursive is directly connected, HUB1-VPN2), 1d03h58m, [1/0]
                    [200/0] via 192.168.1.189 (recursive is directly connected, HUB1-VPN3), 1d03h58m, [1/0]
C       10.200.99.1/32 is directly connected, Branch-Lo
B       10.2.0.0/16 [200/0] via 192.168.1.61 (recursive is directly connected, HUB1-VPN1), 00:03:01, [1/0]
                    [200/0] via 192.168.1.125 (recursive is directly connected, HUB1-VPN2), 00:00:51, [1/0]
                    [200/0] via 192.168.1.189 (recursive is directly connected, HUB1-VPN3), 00:00:51, [1/0]
B       10.2.5.0/24 [200/0] via 192.168.1.61 (recursive is directly connected, HUB1-VPN3), 00:00:01, [1/0]
...


branch1_fgt # diag sys sdwan service4

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

  Dst address(1):
        10.0.0.0-10.255.255.255


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

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

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

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

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

C. SD-WAN service rule 4 and port1 or port2.

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

Answer: D

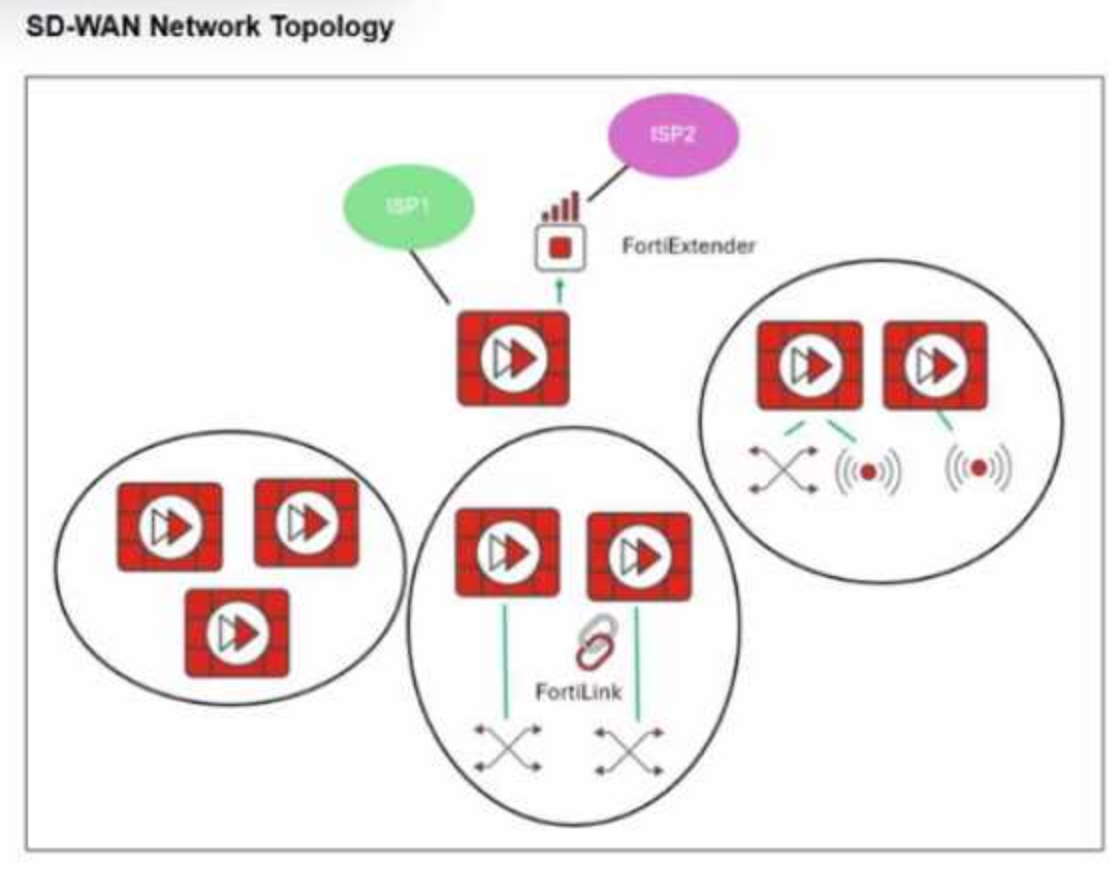
Explanation:

Traffic steering in Fortinet SD-WAN is based on defined rules and the corresponding outgoing interfaces. The exhibit (not shown here) would indicate that the traffic from the LAN subnet 10.0.1.0/24 to the server 10.2.5.254 is matched by SD-WAN rule 3 and sent out via the HUB1-VPN3 interface.
Reference:

[FCSS_SDW_AR-7.4 1-0.docx Q2]

FortiOS 7.4 SD-WAN Concept Guide – Rule Matching

Question: 3



Refer to the exhibit.

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

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

What should you consider when planning your deployment?

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

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

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

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

Answer: B

Explanation:

In Fortinet SD-WAN, hubs should not have extensions like FortiSwitch, FortiAP, or FortiExtender installed, as these can affect hub functionality and scalability. While all device types can be included in the topology, the hubs must be "clean" FortiGate devices without such extensions to ensure proper ADVPN and overlay management.
Reference:

[FCSS_SDW_AR-7.4 1-0.docx Q3]

Fortinet SD-WAN Reference Architecture Guide 7.4 – Hub requirements

Question: 4

Refer to exhibit.

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=500 locport=500 outintf="port1" srccountry="Reserved" cookies="50b8a3684ddfd2cb/af3f725d883c5585" user="10
0.64.1.1" group="N/A" useralt="N/A" xauthuser="N/A" xauthgroup="N/A" assignip=172.168.1.1 vpntunnel="VPN4_0" tunnelip=N/A 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
```

Refer to the exhibit that shows event logs on FortiGate.

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: C

Explanation:

Event logs (from the exhibit) show how traffic is matched to SD-WAN rules and routed. The log output indicates that voice traffic is being routed through the HUB1-VPN3 tunnel. This matches SD-WAN's application-aware steering, which uses dynamic performance metrics to select the optimal path.
Reference:

[FCSS_SDW_AR-7.4 1-0.docx Q4]

FortiOS 7.4 SD-WAN Application-Aware Routing Documentation

Question: 5

Exhibit.

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

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

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

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

C. FortiGate sends alert messages through poft5 when it detects all SD-WAN members as dead

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

Answer: C

Explanation:

Thank You for trying FCSS_SDW_AR-7.6 PDF Demo

To try our FCSS_SDW_AR-7.6 Full Version Download visit link below

https://www.certkillers.net/Exam/FCSS_SDW_AR-7.6

Start Your FCSS_SDW_AR-7.6 Preparation

[Limited Time Offer] Use Coupon "CKNET" for Further discount on your purchase. Test your FCSS_SDW_AR-7.6 preparation with actual exam questions.