DBCLOUD
EXAMS

QUESTIONS & ANSWERS

verified



Technology Provider: Fortinet

Exam: Fortinet NSE 5 - FortiSASE and SD-WAN 7.6 Core Administrator

Number of questions in the database: 50

Exam Version: NOV.2026

Question #1*Topic 1*

Refer to the exhibit.

FortiGate router policy and diagnose output

```
branch1_fgt # show router policy
config router policy
    edit 1
        set src "10.0.1.128/255.255.255.128"
        set dst "128.66.0.0/255.255.255.0"
        set action deny
    next
end

branch1_fgt # diagnose sys sdwan service4

Service(1): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(1), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(priority),
  link-cost-factor(latency), link-cost-threshold(10), heath-check(Corp_HC)
  Members(2):
    1: Seq_num(2 port2 underlay), alive, latency: 0.769, selected
    2: Seq_num(1 port1 underlay), alive, latency: 71.022, 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(4): Address Mode(IPV4) flags=0x24200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(1), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(sla hash-mode=round-rob)
  Members(2):
    1: Seq_num(1 port1 underlay), alive, sla(0x1), gid(2), num of pass(1), selected
    2: Seq_num(2 port2 underlay), alive, sla(0x1), gid(2), num of pass(1), selected
  Src address(1):
        10.0.1.0-10.0.1.255
  Dst address(1):
   128.66.0.0-128.66.255.255
```

How does FortiGate handle the traffic with the source IP 10.0.1.130 and the destination IP 128.66.0.125?

A. FortiGate steers the traffic flow through port2.

B. FortiGate routes the traffic flow according to the FIB.

C. FortiGate load balances the traffic flow through port1 and port2.

D. FortiGate drops the traffic flow.

Correct Answer: D

https://dbcloud.academy/

Question #2Topic 1

Which statement is true about scheduling a FortiClient upgrade using an endpoint upgrade rule?

A. When scheduled, the installation always starts immediately if the endpoint is online.

B. An endpoint upgrade rule can be assigned to a user group.

C. Scheduled upgrades automatically reboot macOS endpoints after installation.

D. If the scheduled time is already past in the local time zone of the endpoint, installation starts the next day at that time.

Correct Answer: B

Question #3Topic 1

Which three factors about SLA targets and SD-WAN rules should you consider when configuring SD-WAN rules? (Choose three.)

A. When configuring an SD-WAN rule, you can select multiple SLA targets from different performance SLAs.

B. SLA targets are used only by SD-WAN rules that are configured with a Lowest Cost (SLA) strategy.

C. Member metrics are measured only if a rule uses the SLA target.

D. SD-WAN rules can use SLA targets to check whether the preferred members meet the SLA requirements.

E. When configuring an SD-WAN rule, you can select multiple SLA targets if they are from the same performance SLA.

Correct Answer: ABD

Question #4Topic 1

Which authentication method overrides any other previously configured user authentication on FortiSASE?

A. RADIUS

B. MFA

C. Local

D. SSO

Correct Answer: D

https://dbcloud.academy/

Question #5Topic 1

Which two configurations are required for Agentless ZTNA to work? (Choose two.)

A. Proxy user single sign-on (SSO)

B. FortiClient Agent

C. FortiGate with ZTNA proxy

D. SD-WAN Private Access SPA

Correct Answer: AC

Question #6Topic 1

What is the purpose of the priority/failover connection feature in FortiSASE Geofencing for managing VPN connections?

A. It forces all remote users to connect only to the nearest security POP regardless of location.

B. It allows administrators to define rules to prioritize on-premises FortiGate connections for users in specific countries, with failover to a security POP if the FortiGate device is unavailable.

C. It restricts VPN access to users based on their geolocation without allowing failover options.

D. It automatically balances VPN traffic across all available security POPs without prioritizing on-premises devices.

Correct Answer: B

Question #7Topic 1

What is the primary purpose of implementing a dedicated IP in security POPs?

A. To provide a unique identifier for logging and monitoring user activities across multiple networks

B. To ensure consistent and reliable access for specific users or devices

C. To implement geolocation rules and source IP address anchoring

D. To improve website performance by reducing load times

Correct Answer: C

https://dbcloud.academy/