

Fortinet

Exam Questions NSE5_SSE_AD-7.6

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



NEW QUESTION 1

For a small site, an administrator plans to implement SD-WAN and ensure high network availability for business-critical applications while limiting the overall cost and the cost of pay-per-use backup connections.

Which action must the administrator take to accomplish this plan?

- A. Use a mid-range FortiGate device to implement standalone SD-WAN.
- B. Implement dynamic routing.
- C. Set up a high availability (HA) cluster to implement standalone SD-WAN.
- D. Configure at least two WAN links.

Answer: D

NEW QUESTION 2

Refer to the exhibits.

SD-WAN event logs

Identity	
Device ID	FGVM02TM25002088
Device Name	branch1_fgt
Type	
Sub Type	sdwan
Type	event
Alerts	
Action	
Level	notice
General	
Log Description	SDWAN status
Log ID	0113022923
Member	1
Message	Member status changed. Member out-of-sla.
Virtual Domain	root
Others	
Date	2025-07-01
Date/Time	2025-07-01 05:00:25
Destination End User ID	3
Destination Endpoint ID	3
Destination Geo ID	0
Device Time	2025-07-01 05:00:25
Device Time Zone	-0700
Event Time	2025-07-01 05:00:25
Event Type	Health Check
Health Check	Corp_HC
Log Flag	0
SLA Target ID	1
Source City	Sunnyvale

```
config service
edit 1
set name "Critical-DIA"
set mode sla
set src "LAN-net"
set internet-service enable
set internet-service-app-ctrl 16920 41469
set internet-service-app-ctrl-category 28
config sla
edit "Corp_HC"
set id 1
next
end
set priority-members 1 2
next
```

SD-WAN health-check configuration

```
branch1_fgt (health-check) # show
config health-check
edit "Corp_HC"
set server "198.18.1.1" "198.18.1.2"
set member 1 2
config sla
edit 1
set latency-threshold 150
set jitter-threshold 50
set packetloss-threshold 5
next
end
end
```

Identity	
Device ID	FGVM02TM25002088
Device Name	branch1_fgt
Type	
Sub Type	sdwan
Type	event
Alerts	
Action	
Level	notice
General	
Log Description	SDWAN status
Log ID	0113022923
Message	Number of pass member changed.
Virtual Domain	root
Others	
Date	2025-07-01
Date/Time	2025-07-01 05:00:25
Destination End User ID	3
Destination Endpoint ID	3
Destination Geo ID	0
Device Time	2025-07-01 05:00:25
Device Time Zone	-0700
Event Time	2025-07-01 05:00:25
Event Type	Health Check
Health Check	Corp_HC
Log Flag	0
New Value	1
Old Value	2

Two SD-WAN event logs, the member status, the SD-WAN rule configuration, and the health-check configuration for a FortiGate device are shown. Immediately after the log messages are displayed, how will the FortiGate steer the traffic based on the information shown in the exhibits? (Choose one answer)

- A. FortiGate uses port1 or port2 to steer the traffic for SD-WAN rule ID 1.
- B. FortiGate uses port1 to steer the traffic for SD-WAN rule ID 1.
- C. FortiGate uses port2 to steer the traffic for SD-WAN rule ID 1.
- D. FortiGate skips SD-WAN rule ID 1.

Answer: C

NEW QUESTION 3

A FortiGate device is in production. To optimize WAN link use and improve redundancy, you enable and configure SD-WAN.

What must you do as part of this configuration update process? (Choose one answer)

- A. Replace references to interfaces used as SD-WAN members in the firewall policies.
- B. Replace references to interfaces used as SD-WAN members in the routing configuration.
- C. Disable the interface that you want to use as an SD-WAN member.
- D. Purchase and install the SD-WAN license, and reboot the FortiGate device.

Answer: A

NEW QUESTION 4

What is the purpose of the on/off-net rule setting in FortiSASE?

- A. To enable or disable user authentication for external network access.
- B. To define different traffic routing rules for on-premises and cloud-based resources.
- C. To determine if an endpoint is connecting from a trusted network or untrusted location.
- D. To configure different access policies for users based on their geographical location.

Answer: C

NEW QUESTION 5

You have a FortiGate configuration with three user-defined SD-WAN zones and one or two members in each of these zones. One SD-WAN member is no longer used in health-check and SD-WAN rules. This member is the only member of its zone. You want to delete it.

What happens if you delete the SD-WAN member from the FortiGate GUI?

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

Answer: B

NEW QUESTION 6

Refer to the exhibit.

SD-WAN rule configuration

Name

Corp_HC

Probe mode ⓘ

Active

Passive

Prefer Passive

Protocol

Ping

HTTP

DNS

Servers

198.18.1.1

×

198.18.1.2

×

Participants

All SD-WAN Members

Specify

SLA Targets

➕ Add Target

Link Status

Check Interval

500

ms

Failures before inactive ⓘ

5

Restore link after ⓘ

5

check(s)

Actions when Inactive

Update static route ⓘ

🔘

OK

Cancel

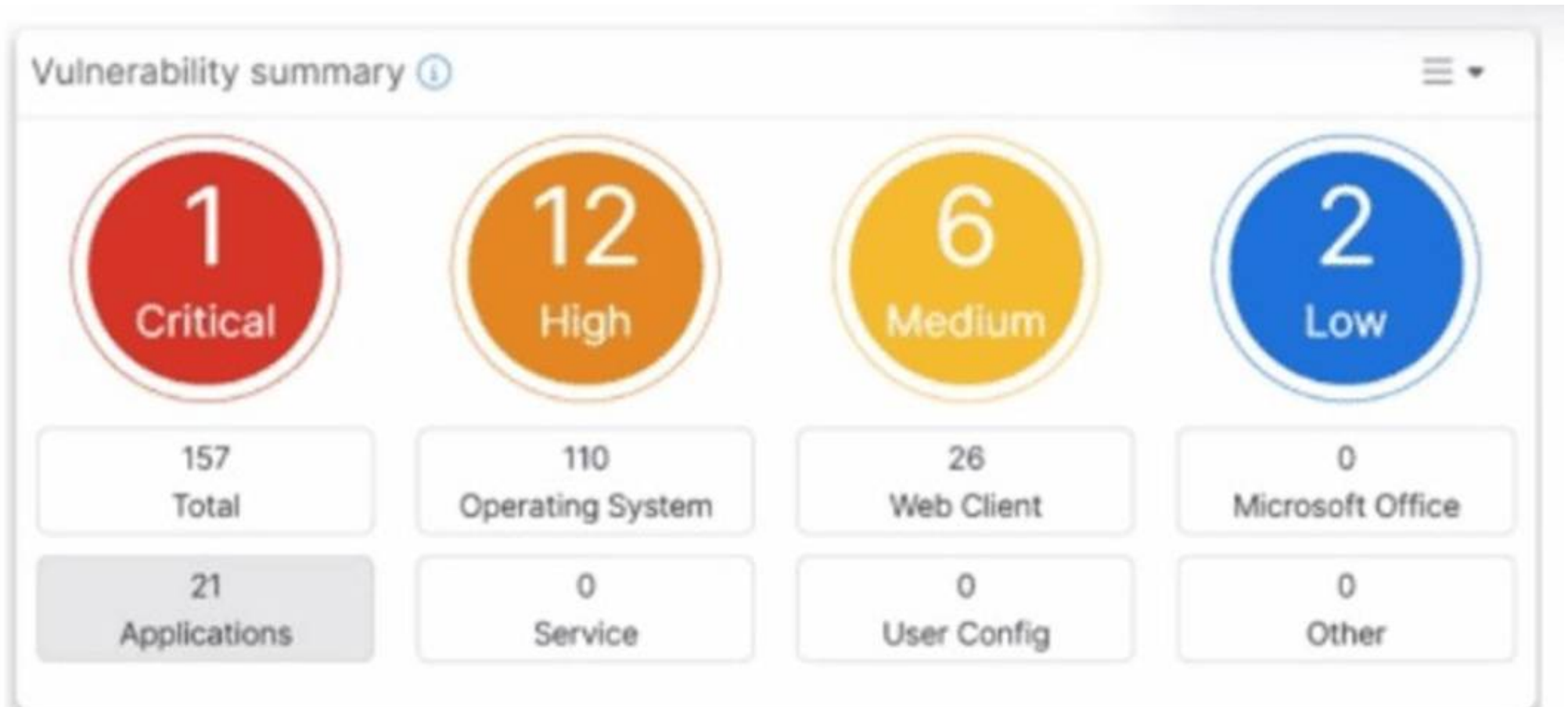
You want the performance service-level agreement (SLA) to measure the jitter of each member. Which configuration change must you make to achieve this result?

- A. No change is required.
- B. Add an SLA target and define a jitter threshold.
- C. Specify the participant members.
- D. Set the protocol to HTTP.

Answer: A

NEW QUESTION 7

Refer to the exhibit.



Which two statements about the Vulnerability summary dashboard in FortiSASE are correct? (Choose two.)

- A. The dashboard shows the vulnerability score for unknown applications.
- B. Vulnerability scan is disabled in the endpoint profile.
- C. The dashboard allows the administrator to drill down and view CVE data and severity classifications.
- D. Automatic vulnerability patching can be enabled for supported applications.

Answer: CD

NEW QUESTION 8

Which three FortiSASE use cases are possible? (Choose three answers)

- A. Secure Internet Access (SIA)
- B. Secure SaaS Access (SSA)
- C. Secure Private Access (SPA)
- D. Secure VPN Access (SVA)
- E. Secure Browser Access (SBA)

Answer: ABC

NEW QUESTION 9

You have configured the performance SLA with the probe mode as Prefer Passive. What are two observable impacts of this configuration? (Choose two.)

- A. FortiGate can offload the traffic that is subject to passive monitoring to hardware.
- B. FortiGate passively monitors the member if ICMP traffic is passing through the member.
- C. During passive monitoring, the SLA performance rule cannot detect dead members.
- D. After FortiGate switches to active mode, the SLA performance rule falls back to passive monitoring after 3 minutes.
- E. FortiGate passively monitors the member if TCP traffic is passing through the member.

Answer: CE

NEW QUESTION 10

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

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

Answer: BE

NEW QUESTION 10

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 must you configure before FortiGate can steer traffic according to SD-WAN rules? (Choose three.)

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

Answer: ACD

Explanation:

According to the SD-WAN 7.6 Core Administrator study guide and the FortiOS 7.6 Administration Guide, for the FortiGate SD-WAN engine to successfully steer traffic using SD-WAN rules, three fundamental configuration components must be in place. This is because the SD-WAN rule lookup occurs only after certain initial conditions are met in the packet flow:

Interfaces (Option C): You must first define the physical or logical interfaces (such as ISP links, LTE, or VPN tunnels) as SD-WAN members. These members are then typically grouped into SD-WAN Zones. Without designated member interfaces, there is no "pool" of links for the SD-WAN rules to select from.

Routing (Option D): For a packet to even be considered by the SD-WAN engine, there must be a matching route in the Forwarding Information Base (FIB). Usually, this is a static route where the destination is the network you want to reach, and the gateway interface is set to the SD-WAN virtual interface (or a specific SD-WAN zone). If there is no route pointing to SD-WAN, the FortiGate will use other routing table entries (like a standard static route) and bypass the SD-WAN rule-based steering logic entirely.

Firewall Policies (Option A): In FortiOS, no traffic is allowed to pass through the device unless a Firewall Policy permits it. To steer traffic, you must have a policy where the Incoming Interface is the internal network and the Outgoing Interface is the SD-WAN zone (or the virtual-wan-link). The SD-WAN rule selection happens during the "Dirty" session state, which requires a policy match to proceed with the session creation.

Why other options are incorrect:

Security Profiles (Option B): While mandatory for Application-level steering (to identify L7 signatures), basic SD-WAN steering based on IP addresses, ports, or ISDB objects does not require security profiles to be active.

Traffic Shaping (Option E): This is an optimization feature used to manage bandwidth once steering is already determined; it is not a prerequisite for the steering engine itself to function.

NEW QUESTION 12

Which two statements about configuring a steering bypass destination in FortiSASE are correct? (Choose two.)

- A. Subnet is the only destination type that supports the Apply condition
- B. Apply condition allows split tunneling destinations to be applied to On-net
- C. off-net
- D. or both types of endpoints
- E. You can select from four destination types: Infrastructure, FQDN, Local Application, or Subnet
- F. Apply condition can be set only to On-net or Off-net
- G. but not both

Answer: BC

Explanation:

According to the FortiSASE 7.6 Feature Administration Guide, steering bypass destinations (also known as split tunneling) allow administrators to optimize bandwidth by redirecting specific trusted traffic away from the SASE tunnel to the endpoint's local physical interface.

Destination Types (Option C): When creating a bypass destination, administrators can select from four distinct types: Infrastructure (pre-defined apps like Zoom/O365), FQDN (specific domains), Local Application (identifying processes on the laptop), or Subnet (specific IP ranges).

Apply Condition (Option B): The "Apply" condition is a flexible setting that allows the administrator to choose when the bypass is active. It can be applied to endpoints that are On-net (inside the office), Off-net (remote), or Both. This ensures that if a user is in the office, they don't use the SASE tunnel for local resources, but if they are home, they might still bypass high-bandwidth sites like YouTube to preserve tunnel capacity.

Why other options are incorrect:

Option A: Subnet is one of four types and is not the only type supporting these conditions.

Option D: The system explicitly supports "Both" to ensure consistency across network transitions.

NEW QUESTION 16

Which two delivery methods are used for installing FortiClient on a user's laptop? (Choose two.)

- A. Use zero-touch installation through a third-party application store.
- B. Download the installer directly from the FortiSASE portal.
- C. Send an invitation email to selected users containing links to FortiClient installers.
- D. Configure automatic installation through an API to the user's laptop.

Answer: BC

NEW QUESTION 20

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

- 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.

Answer: BDE

NEW QUESTION 23

DRAG DROP

In which order does a FortiGate device consider the following elements shown in the left column during the route lookup process?

Select the element in the left column, hold and drag it to a blank position in the column on the right. Place the four correct elements in order, placing the first element in the first position at the top of the column. Once you place an element, you can move it again if you want to change your answer before moving to the next question. You need to drop four elements in the work area.

Select and drag the screen divider to change the viewable area of the source and work areas.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 28

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

NSE5_SSE_AD-7.6 Practice Exam Features:

- * NSE5_SSE_AD-7.6 Questions and Answers Updated Frequently
- * NSE5_SSE_AD-7.6 Practice Questions Verified by Expert Senior Certified Staff
- * NSE5_SSE_AD-7.6 Most Realistic Questions that Guarantee you a Pass on Your First Try
- * NSE5_SSE_AD-7.6 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The NSE5_SSE_AD-7.6 Practice Test Here](#)