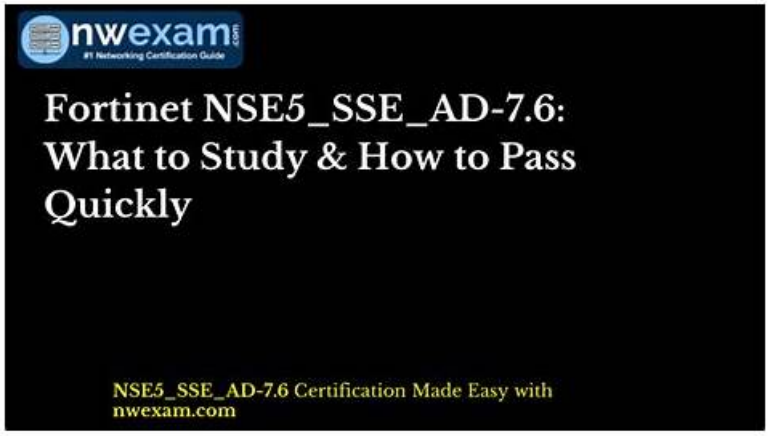
NSE5_SSE_AD-7.6 Test Labs, Valid Exam NSE5_SSE_AD-7.6 Practice



2026 Latest ITPassLeader NSE5_SSE_AD-7.6 PDF Dumps and NSE5_SSE_AD-7.6 Exam Engine Free Share: https://drive.google.com/open?id=1l8CTfUPa7Gbzx47-CLvvV-Zxug4ijwm2

Nowadays the competition in the job market is fiercer than any time in the past. If you want to find a good job， you must own good competences and skillful major knowledge. So owning the NSE5_SSE_AD-7.6 certification is necessary for you because we will provide the best study materials to you. Our NSE5_SSE_AD-7.6 exam torrent is of high quality and efficient, and it can help you pass the test successfully. The product we provide with you is compiled by professionals elaborately and boosts varied versions which aimed to help you learn the NSE5_SSE_AD-7.6 Study Materials by the method which is convenient for you. They check the update every day, and we can guarantee that you can get a free update service from the date of purchase.

Fortinet NSE5_SSE_AD-7.6 Exam Syllabus Topics:

Topic	Details
Topic 1	• Decentralized SD-WAN: This domain covers basic SD-WAN implementation including configuring members, zones, and performance SLAs to monitor network quality.
Topic 2	• SASE Deployment: This domain covers FortiSASE administration settings, user onboarding methods, and integration with SD-WAN infrastructure.
Topic 3	• Secure Internet Access (SIA) and Secure SaaS Access (SSA): This section focuses on implementing security profiles for content inspection and deploying compliance rules to managed endpoints.
Topic 4	• Rules and Routing: This section addresses configuring SD-WAN rules and routing policies to control and direct traffic flow across different links.
Topic 5	• Analytics: This domain covers analyzing SD-WAN and FortiSASE logs to monitor traffic behavior, identify security threats, and generate reports.

>> NSE5_SSE_AD-7.6 Test Labs <<

Valid Exam NSE5_SSE_AD-7.6 Practice - New NSE5_SSE_AD-7.6 Exam Guide

Fortinet NSE 5 - FortiSASE and SD-WAN 7.6 Core Administrator (NSE5_SSE_AD-7.6) PDF dumps are the third and most convenient format of the Fortinet NSE5_SSE_AD-7.6 PDF questions prep material. This format is perfect for busy test takers who prefer to study for the Fortinet NSE 5 - FortiSASE and SD-WAN 7.6 Core Administrator (NSE5_SSE_AD-7.6) exam on the go. Questions bank in the ITPassLeader Fortinet NSE5_SSE_AD-7.6 Pdf Dumps is accessible via all smart devices. We also update

Fortinet NSE 5 - FortiSASE and SD-WAN 7.6 Core Administrator (NSE5_SSE_AD-7.6) PDF questions regularly to ensure they match with the new content of the NSE5_SSE_AD-7.6 exam.

Fortinet NSE 5 - FortiSASE and SD-WAN 7.6 Core Administrator Sample Questions (Q26-Q31):

NEW QUESTION # 26
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 passively monitors the member if ICMP traffic is passing through the member.
- B. FortiGate passively monitors the member if TCP traffic is passing through the member.
- C. During passive monitoring, the SLA performance rule cannot detect dead members.
- D. FortiGate can offload the traffic that is subject to passive monitoring to hardware.
- E. After FortiGate switches to active mode, the SLA performance rule falls back to passive monitoring after 3 minutes.

Answer: B,C

Explanation:
When "Prefer Passive" is set, FortiGate attempts to passively monitor the health of SD-WAN members using real application traffic like TCP sessions, collecting statistics such as latency, jitter, and packet loss from actual observed flows.
Passive monitoring does not generate probe packets; it relies entirely on existing traffic. If there is no matching traffic, health check data is unavailable, meaning dead members may go undetected when only passive monitoring is active.

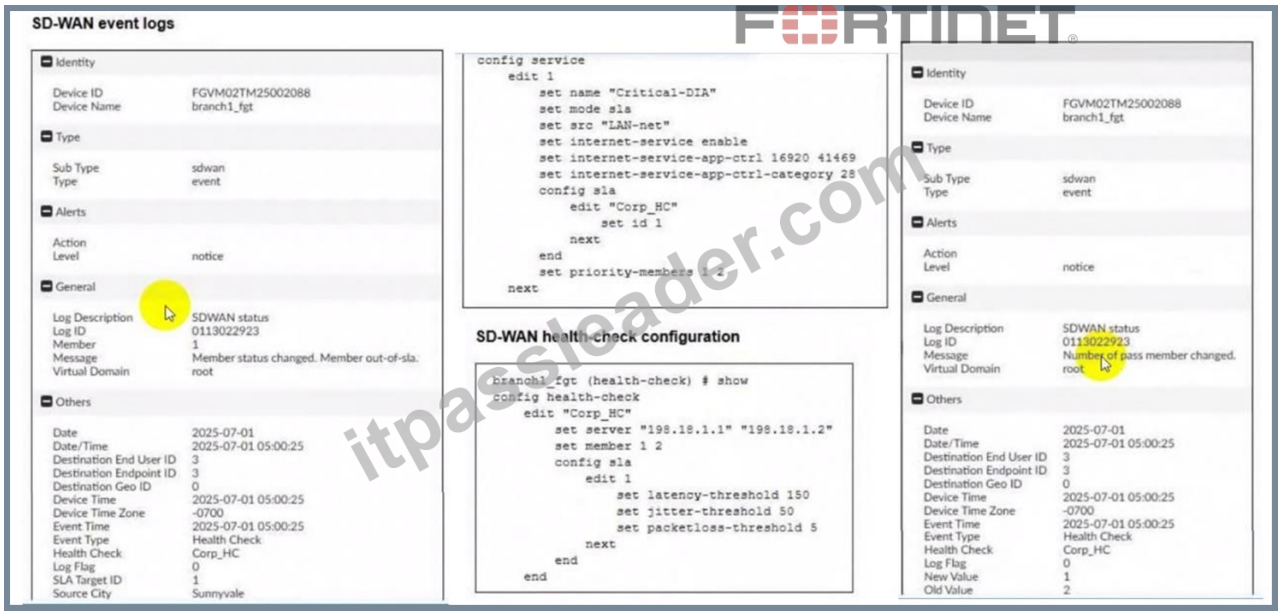
NEW QUESTION # 27
What is the purpose of the on/off-net rule setting in FortiSASE?

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

Answer: B

Explanation:
The on/off-net rule setting in FortiSASE classifies endpoints as on-net (inside trusted corporate networks, like branch offices) or off-net (remote or untrusted locations, like home or public Wi-Fi).
Administrators define on-net rules using IP subnets, gateway MACs, or other criteria to trigger behaviors such as exempting on-net endpoints from FortiSASE auto-connect or applying different profiles.

NEW QUESTION # 28
Refer to the exhibits. 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

Explanation:
According to the SD-WAN 7.6 Core Administrator curriculum and the provided exhibits, the traffic steering decision is determined by the interaction between the Lowest Cost (SLA) strategy and the link health status reported in the event logs.
Rule Strategy (Lowest Cost SLA): The SD-WAN rule configuration for ID 1 (named Critical-DIA) is set to mode sla. In this mode, the FortiGate will only steer traffic through member interfaces that satisfy the assigned Performance SLA targets.
Member Preference: The rule defines priority-members 1 2. This means that under normal conditions (where both links are healthy), Member 1 (port1) is the preferred interface because it is listed first.
Event Log Analysis:
The first log message explicitly states: "Member status changed. Member out-of-sla." for Member
1. This indicates that port1 has exceeded one of the thresholds (latency, jitter, or packet loss) defined in the Corp_HC health check.
The second log confirms: "Number of pass member changed. New Value: 1, Old Value: 2". This verifies that while there were previously two links passing the SLA, now only one link (Member
2/port2) remains in a passing state.
Steering Decision: Because the rule strategy is mode sla and the primary preferred member (port1) is now out-of-sla, the FortiGate immediately disqualifies Member 1 from the selection pool for this specific rule. It then moves to the next available member in the priority list that does satisfy the SLA, which is Member 2 (port2).

NEW QUESTION # 29
You have configured the performance SLA with the probe mode as Prefer Passive.
What are two observable impacts of this configuration? (Choose two.)

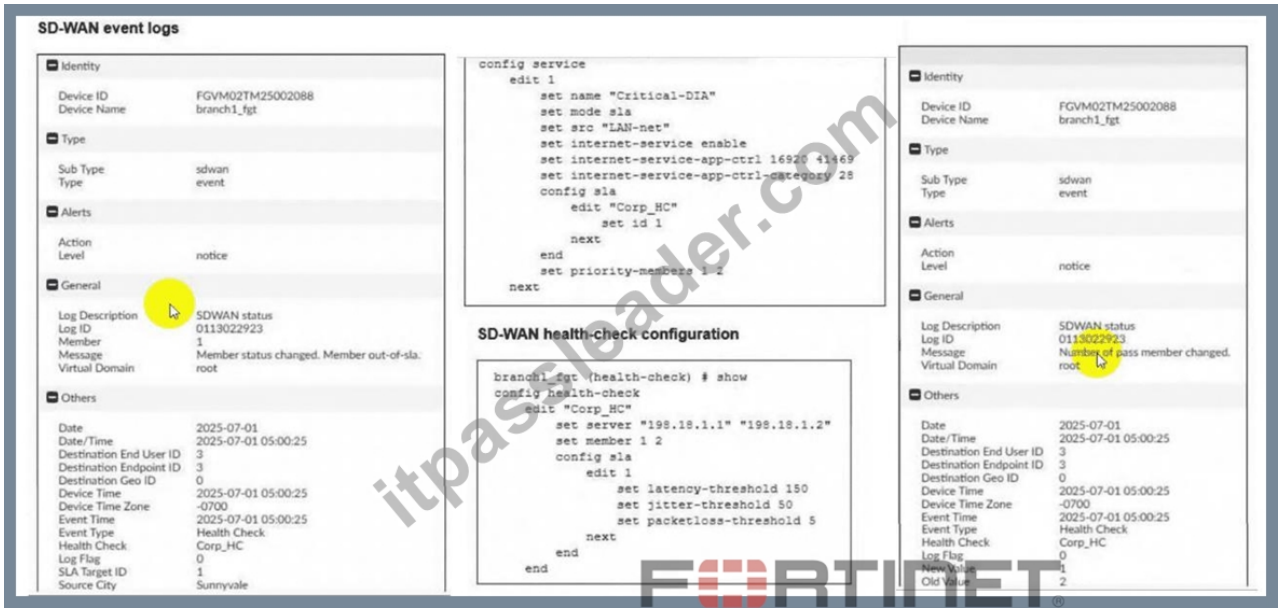
- A. FortiGate passively monitors the member if ICMP traffic is passing through the member.
- B. FortiGate passively monitors the member if TCP traffic is passing through the member.
- C. During passive monitoring, the SLA performance rule cannot detect dead members.
- D. FortiGate can offload the traffic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

Answer: B,C

Explanation:
In theSD-WAN 7.6 Core Administratorcurriculum, the "Prefer Passive" probe mode is a hybrid monitoring strategy designed to minimize the overhead of synthetic traffic (probes) while maintaining link health visibility. According to theFortiOS 7.6 Administration Guideand theSD-WAN Study Guide, the behavior and impacts are as follows:

* TCP Traffic Requirement (Option E):Passive monitoring relies on the FortiGate's ability to inspect actual user traffic to calculate health metrics such as Latency, Jitter, and Packet Loss. Specifically, it usesTCP traffic(by analyzing TCP sequence numbers and timestamps to calculate Round Trip Time - RTT). If user traffic is flowing through the member interface, the FortiGate uses those real-world sessions for SLA calculations instead of sending its own probes.
* Inability to Detect Dead Members (Option C):A significant limitation of passive monitoring is that it cannot distinguish between a "dead" link and an "idle" link. If there is no traffic, the passive monitor has no data to analyze. Consequently, while in passive mode, the SD-WAN enginecannot detect a dead member. To mitigate this, "Prefer Passive" includes a fail-safe: if no traffic is detected for a specific period (typically3 minutes), the FortiGate will automatically switch toActive mode(sending ICMP/TCP pings) to verify if the link is actually alive.
Why other options are incorrect:
* Option A:Passive monitoring generallydisables hardware offloading (ASIC)for the monitored traffic.
This is because the CPU must inspect every packet header to calculate performance metrics; if the traffic were offloaded to the Network Processor (NP), the CPU would not see the packets, rendering passive monitoring impossible.
* Option B:While active probes often use ICMP,passive monitoringis specifically designed forTCP trafficbecause the TCP protocol's ACK structure allows for accurate RTT and loss calculation without synthetic packets.
* Option D:The "3-minute" timer is actually the trigger to switchfrom passive to activewhen traffic is absent, not the fallback timer to return to passive. The fallback to passive happens as soon as valid TCP traffic is detected again.
According to theFortiSASE 7.6 Administration Guideand theFCP - FortiSASE 24/25 Administratorstudy materials, FortiSASE supports three primary external (remote) authentication sources to verify the identity of remote users (SIA and SPA users). These sources allow organizations to leverage their existing identity infrastructure for seamless onboarding and policy enforcement:
* Security Assertion Markup Language (SAML) (Option A):This is the most common and recommended method for modern SASE deployments. FortiSASE acts as aSAML Service Provider (SP)and integrates withIdentity Providers (IdP)such as Microsoft Entra ID (formerly Azure AD), Okta, or FortiAuthenticator. This enables Single Sign-On (SSO) and Multi-Factor Authentication (MFA).
* Lightweight Directory Access Protocol (LDAP) (Option C):FortiSASE can connect to on-premises or cloud-based LDAP servers (such as Windows Active Directory). This allows the administrator to map existing AD groups to FortiSASE user groups for granular security policy application.
* Remote Authentication Dial-in User Service (RADIUS) (Option E):RADIUS is supported for organizations that use centralized authentication servers or traditional MFA solutions (like RSA SecurID). FortiSASE can query a RADIUS server to validate user credentials before granting access to the SASE tunnel.
Why other options are incorrect:
* OpenID Connect (OIDC) (Option B):While OIDC is a modern authentication protocol similar to SAML, FortiSASE's primary integration for external Identity Providers is currently standardized on SAML 2.0.
* TACACS+ (Option D):Terminal Access Controller Access-Control System Plus is primarily used for administrative access(AAA) to network devices (like logging into a FortiGate CLI or FortiManager).
It is not used for end-user VPN or SASE authentication in the Fortinet ecosystem.

NEW QUESTION # 30
Refer to the exhibits.



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

Explanation:
According to the SD-WAN 7.6 Core Administrator curriculum and the provided exhibits, the traffic steering decision is determined by the interaction between the Lowest Cost (SLA) strategy and the link health status reported in the event logs.
Rule Strategy (Lowest Cost SLA): The SD-WAN rule configuration for ID 1 (named Critical-DIA) is set to mode sla. In this mode, the FortiGate will only steer traffic through member interfaces that satisfy the assigned Performance SLA targets.
Member Preference: The rule defines priority-members 1 2. This means that under normal conditions (where both links are healthy), Member 1 (port1) is the preferred interface because it is listed first.
Event Log Analysis:
The first log message explicitly states: "Member status changed. Member out-of-sla." for Member 1. This indicates that port1 has exceeded one of the thresholds (latency, jitter, or packet loss) defined in the Corp_HC health check.
The second log confirms: "Number of pass member changed. New Value: 1, Old Value: 2". This verifies that while there were previously two links passing the SLA, now only one link (Member 2/port2) remains in a passing state.
Steering Decision: Because the rule strategy is mode sla and the primary preferred member (port1) is now out- of-sla, the FortiGate immediately disqualifies Member 1 from the selection pool for this specific rule. It then moves to the next available member in the priority list that does satisfy the SLA, which is Member 2 (port2).
Why other options are incorrect:
Option A: FortiGate will not load balance or choose between both links because port1 is currently ineligible due to the SLA failure.
Option B: Steering to port1 would violate the "Lowest Cost (SLA)" rule logic, as that link is no longer meeting the required health standards.
Option D: FortiGate does not "skip" the rule unless no members meet the SLA and there is no fallback configured; in this scenario, port2 is still passing and available.

NEW QUESTION # 31
.....

7.6 Test Blueprint □ Search for ➡ NSE5_SSE_AD-7.6 □□□ on ➠ www.troytecdumps.com □ immediately to obtain a free download □Pass4sure NSE5_SSE_AD-7.6 Pass Guide

- NSE5_SSE_AD-7.6 Exam Labs ◴ NSE5_SSE_AD-7.6 PDF Dumps Files □ Exam NSE5_SSE_AD-7.6 Blueprint □ Open “ www.pdfvce.com ” enter □ NSE5_SSE_AD-7.6 □ and obtain a free download □Exam NSE5_SSE_AD-7.6 Blueprint
- 100% NSE5_SSE_AD-7.6 Exam Coverage □ Valid Braindumps NSE5_SSE_AD-7.6 Ebook □ Certification NSE5_SSE_AD-7.6 Questions □ Easily obtain free download of （ NSE5_SSE_AD-7.6 ） by searching on ➡ www.troytecdumps.com □□□ □NSE5_SSE_AD-7.6 PDF Dumps Files
- Pass-Sure Fortinet NSE5_SSE_AD-7.6 Test Labs - NSE5_SSE_AD-7.6 Free Download □ Download 《 NSE5_SSE_AD-7.6 》 for free by simply entering □ www.pdfvce.com □ website □NSE5_SSE_AD-7.6 Exam Labs
- Avail Trustable NSE5_SSE_AD-7.6 Test Labs to Pass NSE5_SSE_AD-7.6 on the First Attempt □ Open “ www.prep4away.com ” enter ➠ NSE5_SSE_AD-7.6 □ and obtain a free download □Latest NSE5_SSE_AD-7.6 Dumps
- lululeuq397639.wikienlightenment.com, ammarqbxn255841.estate-blog.com, deniseivr912718.ziblogs.com, brendazcsx472373.ssnblog.com, joshlziv511502.wikiannouncing.com, siobhanaqdv566266.blogpayz.com, hannaimqx532724.blog-gold.com, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, imogenuwvx124187.blogdeazar.com, louiseleak154919.wikiworldstock.com, Disposable vapes

BONUS!!! Download part of ITPassLeader NSE5_SSE_AD-7.6 dumps for free: https://drive.google.com/open?id=1l8CTfUPa7Gbzx47-CLvvV-Zxug4ijwm2