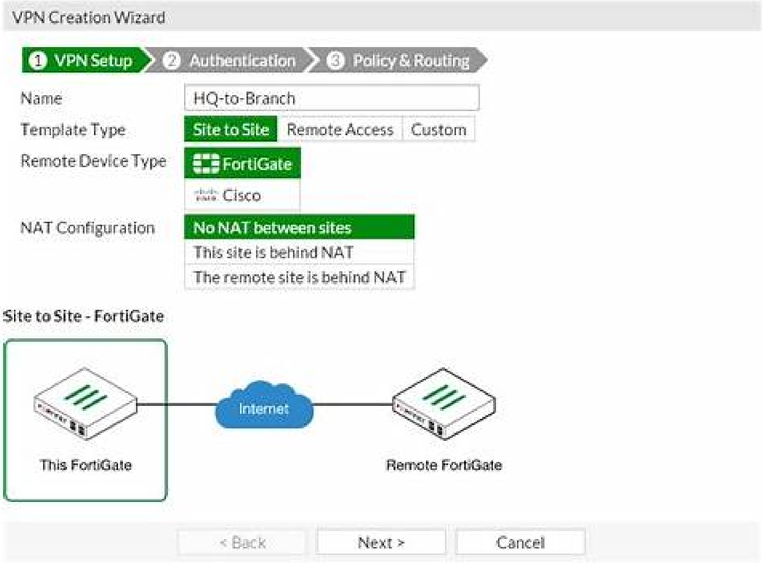
Reliable NSE5_SSE_AD-7.6 Test Guide & NSE5_SSE_AD-7.6 Latest Test Labs



VPN Creation Wizard

1 VPN Setup > 2 Authentication > 3 Policy & Routing

Name: HQ-to-Branch

Template Type: Site to Site | Remote Access | Custom

Remote Device Type: FortiGate | Cisco

NAT Configuration: No NAT between sites | This site is behind NAT | The remote site is behind NAT

Site to Site - FortiGate

The Fortinet NSE5_SSE_AD-7.6 certification exam and this will assist you to take the right decision for your career. The right decision is to enroll in the Fortinet NSE5_SSE_AD-7.6 exam and start preparation with top-notch Fortinet NSE5_SSE_AD-7.6 Exam Dumps. All Fortinet NSE5_SSE_AD-7.6 practice test questions formats are ready for quick download.

Fortinet NSE5_SSE_AD-7.6 Exam Syllabus Topics:

Topic	Details
Topic 1	• Rules and Routing: This section addresses configuring SD-WAN rules and routing policies to control and direct traffic flow across different links.
Topic 2	• 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 3	• Decentralized SD-WAN: This domain covers basic SD-WAN implementation including configuring members, zones, and performance SLAs to monitor network quality.
Topic 4	• Analytics: This domain covers analyzing SD-WAN and FortiSASE logs to monitor traffic behavior, identify security threats, and generate reports.
Topic 5	• SASE Deployment: This domain covers FortiSASE administration settings, user onboarding methods, and integration with SD-WAN infrastructure.

>> Reliable NSE5_SSE_AD-7.6 Test Guide <<

NSE5_SSE_AD-7.6 Latest Test Labs | NSE5_SSE_AD-7.6 Exam Tutorial

The price for NSE5_SSE_AD-7.6 study guide is quite reasonable, no matter you are a student or employee in the company, you can afford them. Just think that, you only need to spend some money, you can get a certificate as well as improve your ability. Besides, we also pass guarantee and money back guarantee for you fail to pass the exam after you have purchasing NSE5_SSE_AD-7.6 Exam Dumps from us. We can give you free update for 365 days after your purchasing. If you have any questions about the NSE5_SSE_AD-7.6 study guide, you can have a chat with us.

Fortinet NSE 5 - FortiSASE and SD-WAN 7.6 Core Administrator Sample Questions (Q13-Q18):

NEW QUESTION # 13
Which secure internet access (SIA) use case minimizes individual endpoint configuration? (Choose one answer)

- A. Site-based remote user internet access
- B. Agentless remote user internet access
- C. SIA for FortiClient agent remote users
- D. SIA using ZTNA

Answer: A

Explanation:
According to theFortiSASE 7.6 Architecture GuideandAdministration Guide, theSite-based remote user internet accessuse case is the only deployment model that completely eliminates the need for individual endpoint configuration.
* Centralized Enforcement: In a site-based deployment, a "thin edge" device (such as aFortiExtender or aFortiGatein LAN extension mode) is installed at the remote site. This device establishes a secure tunnel to the FortiSASE Point of Presence (PoP).
* Zero Endpoint Configuration: Because the traffic redirection happens at the network gateway level, individual devices (laptops, IoT devices, mobile phones) behind the site-based device do not require any specialized software or settings. They simply connect to the local network as they would normally, and their traffic is automatically secured by the SASE cloud.
* Comparison with Other Modes:
* Agent-based (Option B): Requires the installation and maintenance ofFortiClientsoftware on every device, often managed via MDM tools.
* Agentless (Option A): While it doesn't need an agent, it typically requires the configuration of Explicit Web Proxysettings or the distribution of aPAC (Proxy Auto-Configuration) filevia GPO or SCCM to each device's browser.
* ZTNA (Option D): Generally requires an endpoint agent (FortiClient) to perform posture checks and identity verification, involving significant endpoint-level configuration.
Why other options are incorrect:
* Option A: Agentless mode is often confused with being "configuration-free," but it still requires endpoints to be pointed toward the FortiSASE proxy.
* Option B: This is the most configuration-intensive mode, requiring full software lifecycles for every endpoint.
* Option D: ZTNA is an access methodology that adds configuration complexity (tags, certificates, posture checks) rather than minimizing it.

NEW QUESTION # 14
Which three factors about SLA targets and SD-WAN rules should you consider when configuring SD-WAN rules? (Choose three answers)

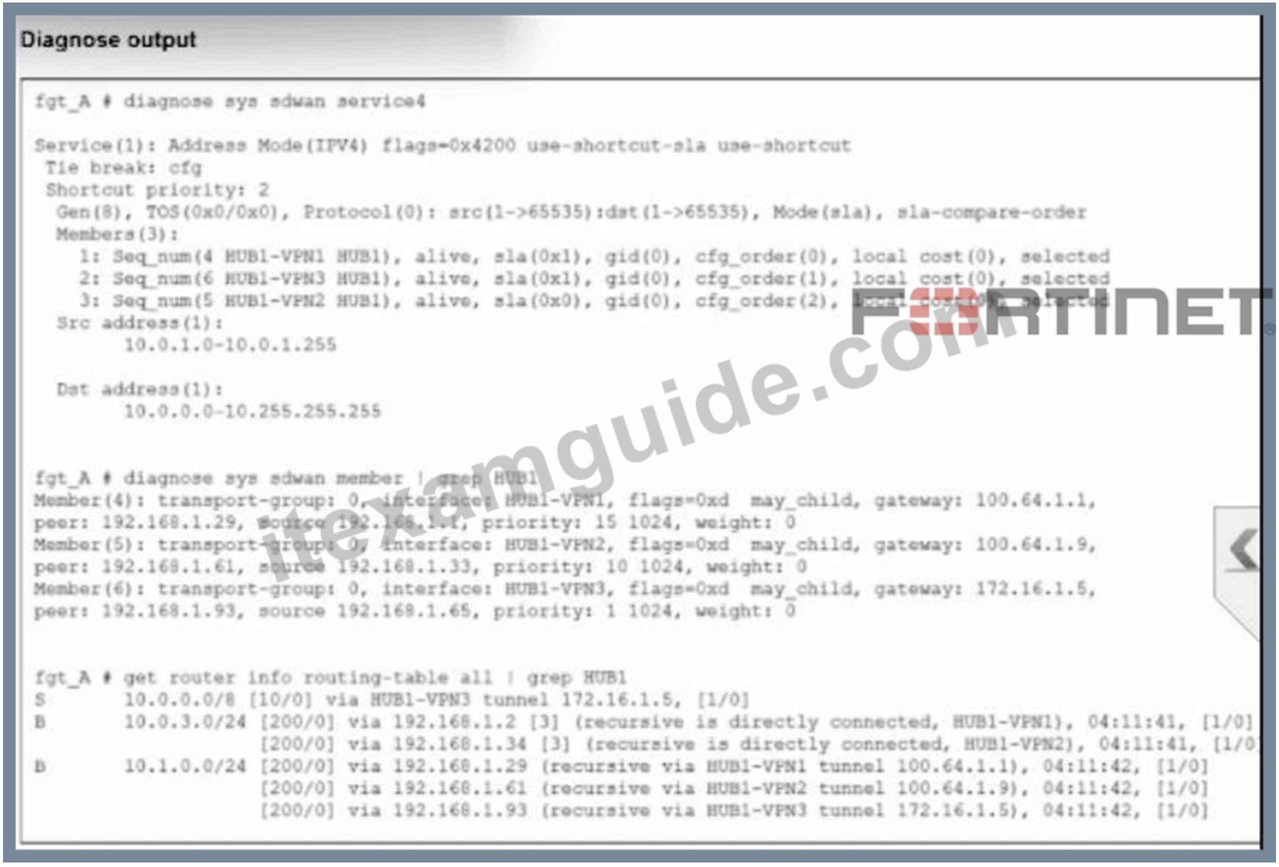
- A. SLA targets are used only by SD-WAN rules that are configured with a Lowest Cost (SLA) strategy.
- B. When configuring an SD-WAN rule, you can select multiple SLA targets if they are from the same performance SLA.
- C. Member metrics are measured only if a rule uses the SLA target.
- D. SD-WAN rules 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 from different performance SLAs.

Answer: A,B,D

Explanation:
According to theSD-WAN 7.6 Core Administratorstudy guide and theFortinet Document Library, the interaction between SD-WAN rules and SLA targets is governed by specific selection and measurement logic:
* Usage by Strategy (Option B): SLA targets are fundamentally used by theLowest Cost (SLA)strategy to determine which links are currently healthy enough to be considered for traffic steering. While other strategies likeBest Qualityuse a "Measured SLA" to monitor metrics, they do not typically use the
"Required SLA Target" to disqualify links unless specifically configured in a hybrid mode. In most curriculum contexts, the "Required SLA Target" field is specifically associated with the Lowest Cost and Maximize Bandwidth strategies.
* SLA Compliance Checking (Option D): SD-WAN rules utilize SLA targets as a "pass/fail" gatekeeper. The engine checks if thepreferred membersmeet the defined SLA requirements (latency, jitter, or packet loss thresholds). If a preferred member fails the SLA, the rule will move to the next member in the priority list that does meet the SLA.
* Single SLA Binding (Option E): When configuring an SD-WAN rule, the GUI and CLI allow you to selectmultiple SLA targets, but they must all belong to thesame Performance SLAprofile. You cannot mix and match targets from different health checks (e.g.,

Target 1 from "Google_HC" and Target 2 from "Amazon_HC") within a single SD-WAN rule.
Why other options are incorrect:
* Option A: This is incorrect because a single SD-WAN rule can only be associated with one specific Performance SLA profile at a time; therefore, you cannot select targets fromdifferentSLAs.
* Option C: This is incorrect because member metrics (latency, jitter, packet loss) are measured by the Performance SLAprobes regardless of whether an SD-WAN rule is currently using that SLA target for steering decisions. Measurement is a function of the health-check, not the rule matching process.

NEW QUESTION # 15



Diagnose output

```
fgt_A # diagnose sys sdwan service4

Service(1): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(8), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(sla), sla-compare-order
  Members(3):
    1: Seq_num(4 HUB1-VPN1 HUB1), alive, sla(0x1), gid(0), cfg_order(0), local cost(0), selected
    2: Seq_num(6 HUB1-VPN3 HUB1), alive, sla(0x1), gid(0), cfg_order(1), local cost(0), selected
    3: Seq_num(5 HUB1-VPN2 HUB1), alive, sla(0x0), gid(0), cfg_order(2), 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


fgt_A # diagnose sys sdwan member | grep HUB1
Member(4): transport-group: 0, interface: HUB1-VPN1, flags=0xd  may_child, gateway: 100.64.1.1,
peer: 192.168.1.29, source 192.168.1.1, priority: 15 1024, weight: 0
Member(5): transport-group: 0, interface: HUB1-VPN2, flags=0xd  may_child, gateway: 100.64.1.9,
peer: 192.168.1.61, source 192.168.1.33, priority: 10 1024, weight: 0
Member(6): transport-group: 0, interface: HUB1-VPN3, flags=0xd  may_child, gateway: 172.16.1.5,
peer: 192.168.1.93, source 192.168.1.65, priority: 1 1024, weight: 0


fgt_A # get router info routing-table all | grep HUB1
S       10.0.0.0/8 [10/0] via HUB1-VPN3 tunnel 172.16.1.5, [1/0]
B       10.0.3.0/24 [200/0] via 192.168.1.2 [3] (recursive is directly connected, HUB1-VPN1), 04:11:41, [1/0]
                    [200/0] via 192.168.1.34 [3] (recursive is directly connected, HUB1-VPN2), 04:11:41, [1/0]
B       10.1.0.0/24 [200/0] via 192.168.1.29 (recursive via HUB1-VPN1 tunnel 100.64.1.1), 04:11:42, [1/0]
                    [200/0] via 192.168.1.61 (recursive via HUB1-VPN2 tunnel 100.64.1.9), 04:11:42, [1/0]
                    [200/0] via 192.168.1.93 (recursive via HUB1-VPN3 tunnel 172.16.1.5), 04:11:42, [1/0]
```

An administrator is troubleshooting SD-WAN on FortiGate. A device behind branch1_fgt generates traffic to the 10.0.0.0/8 network. The administrator expects the traffic to match SD-WAN rule ID 1 and be routed over HUB1-VPN1. However, the traffic is routed over HUB1-VPN3.
Based on the output shown in the exhibit, which two reasons, individually or together, could explain the observed behavior? (Choose two.)

- A. HUB1-VPN3 has a lower route priority value (higher priority) than HUB1-VPN1.
- B. HUB1-VPN1 does not have a valid route to the destination.
- C. HUB1-VPN3 has a higher member configuration priority than HUB1-VPN1.
- D. The traffic matches a regular policy route configured with HUB1-VPN3 as the outgoing device.

Answer: A,B

Explanation:
According to theSD-WAN 7.6 Core Administratorcurriculum and the diagnostic outputs shown in the exhibit, the reason traffic is steered toHUB1-VPN3instead of the expectedHUB1-VPN1(defined in SD-WAN rule ID 1) can be explained by two core routing principles in FortiOS:
* Valid Route Requirement (Option A): In thediagnose sys sdwan service 4output (which corresponds to Rule ID 1), it shows the rule has membersHUB1-VPN1,HUB1-VPN2, andHUB1-VPN3. A key principle of SD-WAN steering is that for a member to be "selectable" by a rule, itmust have a valid route to the destinationin the routing table (RIB/FIB). If the routing table output (the third section of the exhibit) shows a route to 10.0.0.0/8 viaHUB1-VPN3butnotthroughHUB1-VPN1, the SD-WAN engine will skip HUB1-VPN1 entirely because it is considered a "non-reachable" path for that specific destination.
* Policy Route Precedence (Option D): In the FortiOS route lookup hierarchy,Regular Policy Routes (PBR)are evaluatedbeforeSD-WAN rules. If an administrator has configured a traditional Policy Route (found underNetwork > Policy Routes) that matches traffic

destined for 10.0.0.0/8 and specifiesHUB1- VPN3as the outgoing interface, the FortiGate will forward the packet based on that policy route and will never evaluate the SD-WAN rulesfor that session. This "bypass" occurs regardless of whether the SD- WAN rule would have chosen a "better" link.

Why other options are incorrect:

* Option B: While member configuration priority (cfg_order) is a tie-breaker in some strategies, the SD- WAN rule logic is only applied if the routing table allows it or if a higher-priority policy route doesn't intercept the traffic first.

* Option C: Lower route priority (which means higher preference in the RIB) affects theImplicit Rule (standard routing). However, SD-WAN rules are designed tooverrideRIB priority for matching traffic.

If HUB1-VPN1 was a valid candidate and no Policy Route existed, the SD-WAN rule would typically ignore RIB priority to enforce its own steering strategy.

NEW QUESTION # 16

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

Answer: B,D

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 # 17
Which statement about security posture tags in FortiSASE is correct?

- A. Multiple tags can be assigned to an endpoint, but only one is used for evaluation.
- B. Only one tag can be assigned to an endpoint.
- C. Multiple tags can be assigned to an endpoint and used for evaluation.
- D. Tags are static and do not change with endpoint status.

Answer: C

Explanation:
According to theFortiSASE 7.6 Administration GuideandFCP - FortiSASE 24/25 Administrator curriculum, security posture tags (often referred to as ZTNA tags) are the fundamental building blocks for identity-based and posture-based access control.
* Multiple Tag Assignment: A single endpoint can be assigned multiple tags at the same time. For example, an endpoint might simultaneously have the tags"OS-Windows-11","AV-Running", and
"Corporate-Domain-Joined".
* Evaluation Logic: During the policy evaluation process (for both SIA and SPA), FortiSASE or the FortiGate hub considers all tags assigned to the endpoint. Security policies can be configured to use these tags as source criteria. If an administrator defines a policy that requires both "AV-Running" and
"Corporate-Domain-Joined," the system evaluates both tags to decide whether to permit the traffic.
* Dynamic Nature: Contrary to Option C, these tags are highly dynamic. They are automatically applied or removed in real-time based on the telemetry data sent by theFortiClientto the SASE cloud. If a user disables their antivirus, the "AV-Running" tag is removed immediately, and the endpoint's access is revoked by the next policy evaluation.
* Scalability: While the system supports many tags, documentation recommends a baseline of custom tags for optimal performance, though it confirms that multiple tags are standard for reflecting a comprehensive security posture.
Why other options are incorrect:
* Option A: This is incorrect because the system does not pick just one tag; it evaluates the collection of tags against the policy's requirements (e.g., matching any or matching all).
* Option C: This is incorrect because tags are dynamic and change as soon as the endpoint's status (like vulnerability count or software presence) changes.
* Option D: This is incorrect because the architectural advantage of ZTNA is the ability to layer multiple security "checks" (tags) for a single user.

NEW QUESTION # 18
......

Do you want to have a new change about your life? If your answer is yes, it is high time for you to use the NSE5_SSE_AD-7.6 question torrent from our company. As the saying goes, opportunities for those who are prepared. If you have made up your mind to get respect and power, the first step you need to do is to get the NSE5_SSE_AD-7.6 Certification, because the certification is a reflection of your ability. If you have the NSE5_SSE_AD-7.6 certification, it will be easier for you to get respect and power. Our company happened to be designing the NSE5_SSE_AD-7.6 exam question.

NSE5_SSE_AD-7.6 Latest Test Labs: https://www.itexamguide.com/NSE5_SSE_AD-7.6_braindumps.html

- Hot Reliable NSE5_SSE_AD-7.6 Test Guide | Well-Prepared NSE5_SSE_AD-7.6 Latest Test Labs: Fortinet NSE 5 - FortiSASE and SD-WAN 7.6 Core Administrator □ The page for free download of ➽ NSE5_SSE_AD-7.6 □ on ➥ www.prepawayete.com □ will open immediately □Exam NSE5_SSE_AD-7.6 Guide
- New Reliable NSE5_SSE_AD-7.6 Test Guide 100% Pass | Professional NSE5_SSE_AD-7.6: Fortinet NSE 5 - FortiSASE and SD-WAN 7.6 Core Administrator 100% Pass □ Copy URL { www.pdfvce.com } open and search for ✔ NSE5_SSE_AD-7.6 □✔□ to download for free □Pdf NSE5_SSE_AD-7.6 Pass Leader
- Hot Reliable NSE5_SSE_AD-7.6 Test Guide | Well-Prepared NSE5_SSE_AD-7.6 Latest Test Labs: Fortinet NSE 5 - FortiSASE and SD-WAN 7.6 Core Administrator □ Search for ⇛ NSE5_SSE_AD-7.6 ⇚ on 「 www.verifieddumps.com 」 immediately to obtain a free download □Latest NSE5_SSE_AD-7.6 Dumps Sheet
- Hot Reliable NSE5_SSE_AD-7.6 Test Guide | Well-Prepared NSE5_SSE_AD-7.6 Latest Test Labs: Fortinet NSE 5 - FortiSASE and SD-WAN 7.6 Core Administrator □ Search for “ NSE5_SSE_AD-7.6 ” on ➡ www.pdfvce.com □□□ immediately to obtain a free download □Latest NSE5_SSE_AD-7.6 Dumps Sheet

- Your Ultimate Resource Actual of Fortinet NSE5_SSE_AD-7.6 Questions □ Search for ➡ NSE5_SSE_AD-7.6 □□□ and download exam materials for free through ▶ www.examcollectionpass.com ◀ □NSE5_SSE_AD-7.6 Relevant Answers
- NSE5_SSE_AD-7.6 Latest Test Braindumps □ NSE5_SSE_AD-7.6 Valid Test Labs □ NSE5_SSE_AD-7.6 Real Torrent □ Open 【 www.pdfvce.com 】 enter 【 NSE5_SSE_AD-7.6 】 and obtain a free download □Latest NSE5_SSE_AD-7.6 Dumps Sheet
- Perfect NSE5_SSE_AD-7.6 Exam Brain Dumps give you pass-guaranteed Study Materials - www.exam4labs.com □ Download ▶ NSE5_SSE_AD-7.6 ◀ for free by simply entering ✔ www.exam4labs.com □✔□ website □Accurate NSE5_SSE_AD-7.6 Study Material
- Your Ultimate Resource Actual of Fortinet NSE5_SSE_AD-7.6 Questions □ Open website { www.pdfvce.com } and search for 「 NSE5_SSE_AD-7.6 」 for free download □Accurate NSE5_SSE_AD-7.6 Study Material
- Valid NSE5_SSE_AD-7.6 Test Syllabus □ NSE5_SSE_AD-7.6 Latest Exam Forum □ NSE5_SSE_AD-7.6 Dumps Torrent □ Search for ⇛ NSE5_SSE_AD-7.6 ⇚ on ▷ www.dumpsmaterials.com ◁ immediately to obtain a free download □Exam NSE5_SSE_AD-7.6 Guide
- Hot Reliable NSE5_SSE_AD-7.6 Test Guide | Well-Prepared NSE5_SSE_AD-7.6 Latest Test Labs: Fortinet NSE 5 - FortiSASE and SD-WAN 7.6 Core Administrator □ Open □ www.pdfvce.com □ enter ➠ NSE5_SSE_AD-7.6 □ and obtain a free download □NSE5_SSE_AD-7.6 Latest Exam Forum
- NSE5_SSE_AD-7.6 Exam Training □ Pdf NSE5_SSE_AD-7.6 Braindumps □ Pdf NSE5_SSE_AD-7.6 Pass Leader □ Search on ➠ www.examcollectionpass.com □ for 【 NSE5_SSE_AD-7.6 】 to obtain exam materials for free download □NSE5_SSE_AD-7.6 Latest Test Braindumps
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, lms.ait.edu.za, www.stes.tyc.edu.tw, myportal.utt.edu.tt, cobe2go.com, www.stes.tyc.edu.tw, Disposable vapes