NSE5_SSE_AD-7.6 Study Material, Testking NSE5_SSE_AD-7.6 Exam Questions

Considering that our customers are from different countries, there is a time difference between us, but we still provide the most thoughtful online after-sale service twenty four hours a day, seven days a week, so just feel free to contact with us through email anywhere at any time. Our commitment of helping you to Pass NSE5_SSE_AD-7.6 Exam will never change. Considerate 24/7 service shows our attitudes, we always consider our candidates' benefits and we guarantee that our NSE5_SSE_AD-7.6 test questions are the most excellent path for you to pass the exam.

Our Fortinet NSE 5 - FortiSASE and SD-WAN 7.6 Core Administrator (NSE5_SSE_AD-7.6) web-based practice exam software also simulates the Fortinet NSE 5 - FortiSASE and SD-WAN 7.6 Core Administrator (NSE5_SSE_AD-7.6) environment. These Fortinet NSE5_SSE_AD-7.6 mock exams are also customizable to change the settings so that you can practice according to your preparation needs. NewPassLeader web-based Fortinet NSE 5 - FortiSASE and SD-WAN 7.6 Core Administrator (NSE5_SSE_AD-7.6) practice exam software is usable only with a good internet connection.

>> NSE5_SSE_AD-7.6 Study Material <<

Testking NSE5_SSE_AD-7.6 Exam Questions - NSE5_SSE_AD-7.6 PDF Questions

As long as you insist on using our NSE5_SSE_AD-7.6 learning prep, you can get the most gold certificate in the shortest possible time! Want to see how great your life will change after that! You can make more good friends and you can really live your fantasy life. Don't hesitate, the future is really beautiful! If you are still not sure if our product is useful, you can free download the free demos of ourNSE5_SSE_AD-7.6 practice quiz. It is easy and fast.

Fortinet NSE5_SSE_AD-7.6 Exam Syllabus Topics:

Topic	Details
Topic 1	• Analytics: This domain covers analyzing SD-WAN and FortiSASE logs to monitor traffic behavior, identify security threats, and generate reports.

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	- Rules and Routing: This section addresses configuring SD-WAN rules and routing policies to control and direct traffic flow across different links.
Topic 4	- Decentralized SD-WAN: This domain covers basic SD-WAN implementation including configuring members, zones, and performance SLAs to monitor network quality.
Topic 5	- SASE Deployment: This domain covers FortiSASE administration settings, user onboarding methods, and integration with SD-WAN infrastructure.

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

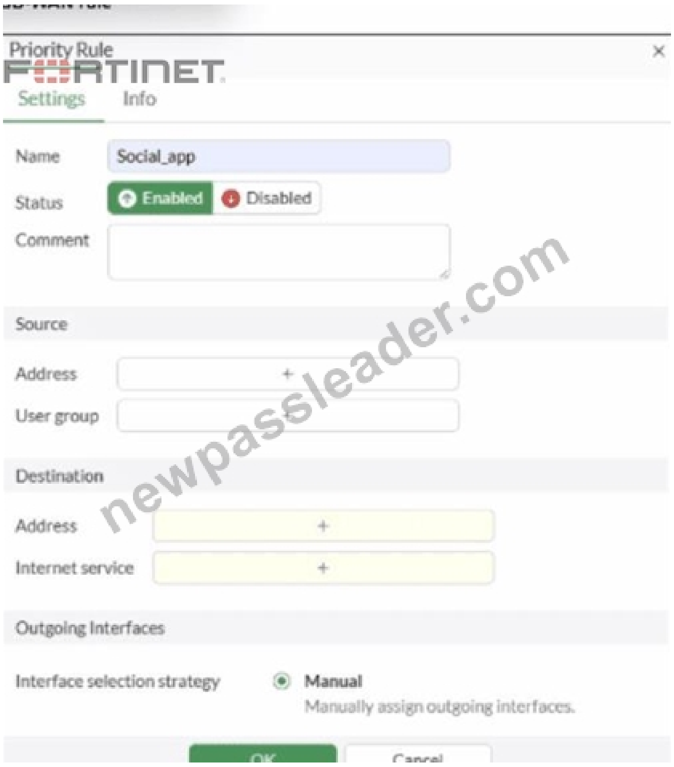
NEW QUESTION # 13
Which two statements about configuring a steering bypass destination in FortiSASE are correct? (Choose two.)

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

Answer: B,D

Explanation:
According to theFortiSASE 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), orSubnet(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 areOn-net(inside the office),Off- net(remote), orBoth. 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 # 14
Refer to the exhibit.



Priority Rule

Name: Social_app

Status: Enabled | Disabled

Comment:

Source

Address: +

User group:

Destination

Address: +

Internet service: +

Outgoing Interfaces

Interface selection strategy: ● Manual
Manually assign outgoing interfaces.

You configure SD-WAN on a standalone FortiGate device. You want to create an SD-WAN rule that steers traffic related to Facebook and LinkedIn through the less costly internet link. What must you do to set Facebook and LinkedIn applications as destinations from the GUI?

- A. Enable the visibility of the applications field as destinations of the SD-WAN rule.
- B. Install a license to allow applications as destinations of SD-WAN rules.
- C. You cannot configure applications as destinations of an SD-WAN rule on a standalone FortiGate device.
- D. In the Internet service field, select Facebook and LinkedIn.

Answer: D

Explanation:
According to theSD-WAN 7.6 Core Administratorcurriculum and theFortiOS 7.6 Administration Guide, setting common web-based services like Facebook and LinkedIn as destinations in an SD-WAN rule is primarily accomplished through theInternet Service Database (ISDB).
* Internet Service vs. Application Control: In FortiOS, there is a distinction betweenInternet Services (which use a database of known IP addresses and ports to identify traffic at the first packet) and Applications(which require the IPS engine to inspect deeper into the packet flow to identify Layer 7 signatures).
* SD-WAN Efficiency: Fortinet recommends using theInternet service fieldfor services like Facebook and LinkedIn in SD-WAN rules because it allows the FortiGate to steer the traffic immediately upon the first packet. If the "Application" signatures were used instead, the first session might be misrouted because the application is not identified until after the initial handshake.
* GUI Configuration: As shown in the exhibit (image_b3a4c2.png), the "Destination" section of an SD- WAN rule includes anInternet servicefield by default. To steer Facebook and LinkedIn traffic, the administrator simply clicks the "+" icon in that field and selects the entries for Facebook and LinkedIn from the database.
* Feature Visibility (Alternative): While youcanenable a specific "Application" field inSystem > Feature Visibility(by enabling "Application Detection Based SD-WAN"), this is typically used for less common applications that do not have dedicated ISDB entries. For the specific "applications" mentioned (Facebook and LinkedIn), they are natively available in theInternet servicefield, making Option B the most direct and common implementation.
Why other options are incorrect:
* Option A: Licensing for application signatures is part of the standard FortiGuard services and is not a prerequisite specific only to "applications as destinations" in SD-WAN rules.
* Option C: Standalone FortiGate devices fully support application-based and ISDB-based steering in SD-WAN rules.
* Option D: While enabling feature visibility would add anadditionalfield for L7 applications, it is not a "must" for Facebook and LinkedIn, which are already accessible via the Internet Service field provided in the default GUI layout.

NEW QUESTION # 15

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 configure different access policies for users based on their geographical location.
- C. To enable or disable user authentication for external network access.
- D. To determine if an endpoint is connecting from a trusted network or untrusted location.

Answer: D

Explanation:
According to theFortiSASE 24.4 Administration Guideand theFortiSASE Core Administratortraining materials, theOn-net detectionrule setting is a critical component for determining the "trust status" of an endpoint's physical location.
* Endpoint Location Verification: On-net rule sets are used to determine if FortiSASE considers an endpoint to beon-net(trusted) oroff-net(untrusted). An endpoint is considered on-net when it is physically located within the corporate network, which is assumed to already have on-premises security measures (like a FortiGate NGFW).
* Operational Impact: When an endpoint is detected as on-net, FortiSASE can be configured toexempt the endpoint from automatically establishing a VPN tunnel to the SASE cloud. This optimization prevents redundant security inspection and conserves SASE bandwidth since the user is already protected by the local corporate firewall.
* Detection Methods: To classify an endpoint as on-net, administrators configure rule sets that look for specific environmental markers, such as:
* Known Public (WAN) IP: If the endpoint's public IP matches the corporate headquarters' egress IP.
* DHCP Server: If the endpoint receives an IP from a specific corporate DHCP server.
* DNS Server/Subnet: Matching internal DNS infrastructure or specific internal IP ranges.
* Dynamic Policy Application: By accurately determining if an endpoint is on or off-net, FortiSASE ensures that theFortiClientagent only initiates its secure internet access (SIA) tunnel when the user is in an untrusted location (e.g., a home network or public Wi-Fi).
Why other options are incorrect:
* Option A: User authentication is a separate process and is not controlled by the on/off-net detection rules, which focus on the network environment rather than user credentials.
* Option B: While on-net status affectshowtraffic is routed (VPN vs. local), these rules specifically determine the statusitself rather than defining the routing tables for private vs. cloud resources.
* Option D: Geographical location (Geo-location) is a different filtering criterion often used in firewall policies; on-net detection is specifically about the proximity to the trusted corporate perimeter.

NEW QUESTION # 16
What is a key use case for FortiSASE Secure Internet Access (SIA) in an agentless deployment? (Choose one answer)

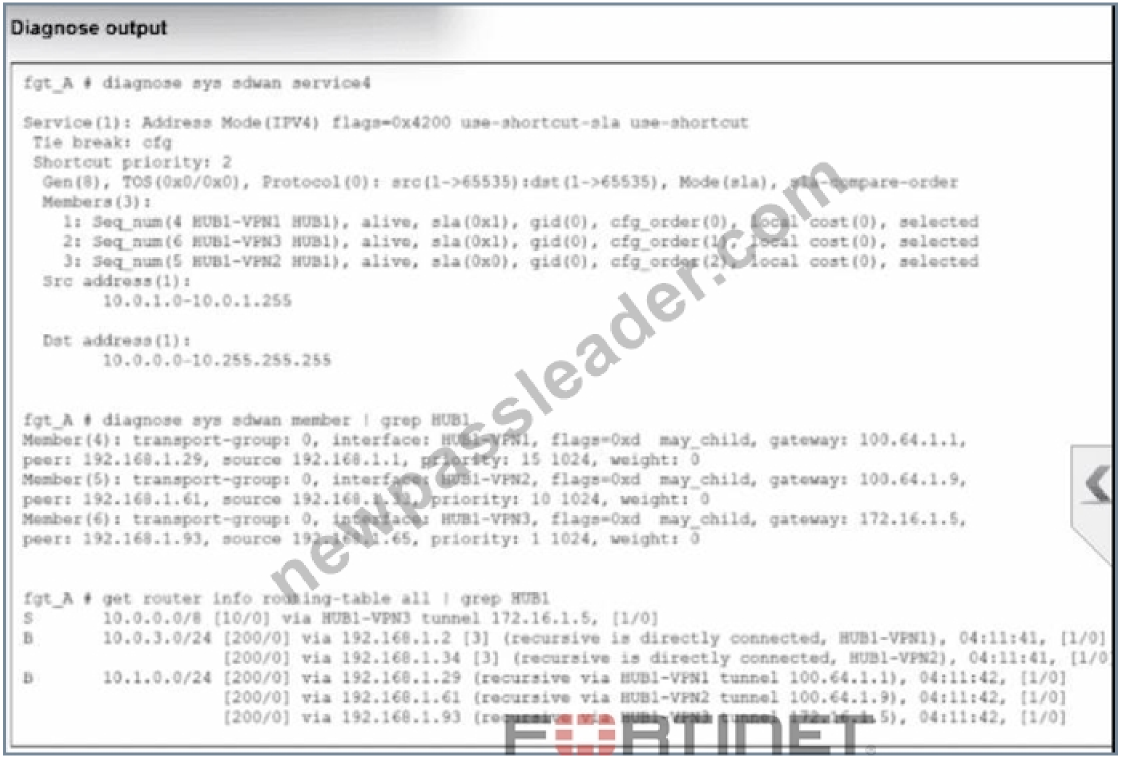
- A. It requires FortiClient endpoints and supports ZTNA tags to secure all network traffic for unmanaged endpoints.
- B. It acts as a secure web gateway (SWG) distributing a PAC file for explicit web proxy use, securing HTTP and HTTPS traffic with a full security stack, and is ideal for unmanaged endpoints like contractors.
- C. It provides secure web browsing by isolating browser sessions and enforcing data loss prevention for temporary employees.
- D. It distributes a PAC file to secure non-web traffic protocols and applies antivirus protection only for managed endpoints.

Answer: B

Explanation:
According to theFortiSASE 7.6 Administration Guideand theFCP - FortiSASE 24/25 Administrator curriculum, the Agentless deployment mode-commonly referred to asSecure Web Gateway (SWG)mode- is a vital component of the Secure Internet Access (SIA) framework.
* Deployment Mechanism: In an agentless deployment, FortiSASE functions as an explicit web proxy.
This is achieved by distributing aPAC (Proxy Auto-Configuration) fileto the user's browser, which instructs the device to send its web traffic to the nearest FortiSASE Point of Presence (PoP).
* Target Use Case: This mode is specifically designed forunmanaged endpoints, such as those used by contractors, partners, or temporary workers, where the organization does not have the authority or capability to install the FortiClient agent.
* Security Capabilities: Even without an agent, FortiSASE applies afull security stackto the redirected traffic. This includesWeb Filtering,Anti-Malware,SSL Inspection, andInline-CASBto secure HTTP and HTTPS sessions.
* Protocol Limitations: Because it relies on proxy settings, this mode is limited to web protocols (HTTP
/HTTPS) and does not inherently secure non-web traffic like ICMP, DNS, or custom TCP/UDP applications unless they are specifically proxied.
Why other options are incorrect:

* Option A: While it provides secure browsing, session isolation (RBI) is a specific feature that can be used in either mode; the defining characteristic of the agentless use case is the proxy-based redirection for unmanaged devices.
* Option C: A PAC file can only secure web traffic (protocols that support proxying), not non-web traffic protocols.
* Option D: Agentless mode is the opposite of requiring FortiClient; ZTNA tags generally require the FortiClient agent to provide the necessary telemetry for tag evaluation.

NEW QUESTION # 17



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

Answer: C,D

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 # 18
......

Highlight a person's learning effect is not enough, because it is difficult to grasp the difficulty of testing, a person cannot be effective information feedback, in order to solve this problem, our NSE5_SSE_AD-7.6 real exam materials provide a powerful platform for users, allow users to exchange of experience. Here, the all users of our NSE5_SSE_AD-7.6 learning reference files can through own id to login to the platform, realize the exchange and sharing with other users, even on the platform and more users to become good friends, encourage each other, to deal with the difficulties encountered in the process of preparation each other. Our NSE5_SSE_AD-7.6 learning reference files not only provide a single learning environment for users, but also create a learning atmosphere like home, where you can learn and communicate easily.

Testking NSE5_SSE_AD-7.6 Exam Questions: https://www.newpassleader.com/Fortinet/NSE5_SSE_AD-7.6-exam-preparation-materials.html

- Reliable NSE5_SSE_AD-7.6 Braindumps Sheet □ Valid NSE5_SSE_AD-7.6 Study Plan □ NSE5_SSE_AD-7.6 Exam Simulator Fee □ Search for ✔ NSE5_SSE_AD-7.6 □✔□ and easily obtain a free download on " www.prep4away.com " □NSE5_SSE_AD-7.6 Online Tests
- 2026 100% Free NSE5_SSE_AD-7.6 –Efficient 100% Free Study Material | Testking Fortinet NSE 5 - FortiSASE and SD-WAN 7.6 Core Administrator Exam Questions □ Search for ☀ NSE5_SSE_AD-7.6 □☀□ and download exam materials for free through （ www.pdfvce.com ） □NSE5_SSE_AD-7.6 Valid Exam Vce
- NSE5_SSE_AD-7.6 Discount Code □ NSE5_SSE_AD-7.6 Materials □ NSE5_SSE_AD-7.6 Online Tests □ Open [www.vce4dumps.com] and search for [NSE5_SSE_AD-7.6] to download exam materials for free □Free NSE5_SSE_AD-7.6 Updates
- 2026 Professional NSE5_SSE_AD-7.6 Study Material | Fortinet NSE 5 - FortiSASE and SD-WAN 7.6 Core Administrator 100% Free Testking Exam Questions □ Search for { NSE5_SSE_AD-7.6 } on 「 www.pdfvce.com 」 immediately to obtain a free download □NSE5_SSE_AD-7.6 Materials
- Latest NSE5_SSE_AD-7.6 VCE Torrent - NSE5_SSE_AD-7.6 Pass4sure PDF - NSE5_SSE_AD-7.6 Latest VCE □ Simply search for □ NSE5_SSE_AD-7.6 □ for free download on □ www.prep4sures.top □ □Valid NSE5_SSE_AD-7.6 Exam Bootcamp
- Reliable NSE5_SSE_AD-7.6 Exam Book □ Latest NSE5_SSE_AD-7.6 Test Fee □ NSE5_SSE_AD-7.6 Valid Exam Vce ↗ Search for ➥ NSE5_SSE_AD-7.6 □ and obtain a free download on [www.pdfvce.com] □Latest NSE5_SSE_AD-7.6 Learning Material
- Pass Guaranteed Quiz NSE5_SSE_AD-7.6 - Reliable Fortinet NSE 5 - FortiSASE and SD-WAN 7.6 Core Administrator Study Material □ Search for 《 NSE5_SSE_AD-7.6 》 and obtain a free download on 【 www.dumpsmaterials.com 】 □Free NSE5_SSE_AD-7.6 Updates
- 2026 Authoritative NSE5_SSE_AD-7.6 Study Material Help You Pass NSE5_SSE_AD-7.6 Easily □ Simply search for ➤ NSE5_SSE_AD-7.6 □ for free download on ➠ www.pdfvce.com □ □Free NSE5_SSE_AD-7.6 Updates
- Valid NSE5_SSE_AD-7.6 Test Notes □ Reliable NSE5_SSE_AD-7.6 Exam Book □ NSE5_SSE_AD-7.6 Exam Simulator Fee □ Copy URL 【 www.dumpsmaterials.com 】 open and search for □ NSE5_SSE_AD-7.6 □ to download for free □Latest NSE5_SSE_AD-7.6 Exam Preparation
- 2026 100% Free NSE5_SSE_AD-7.6 –Efficient 100% Free Study Material | Testking Fortinet NSE 5 - FortiSASE and SD-WAN 7.6 Core Administrator Exam Questions □ Open ➠ www.pdfvce.com □ enter ☀ NSE5_SSE_AD-7.6 □☀□ and obtain a free download □Latest NSE5_SSE_AD-7.6 Test Fee
- Latest NSE5_SSE_AD-7.6 Braindumps □ NSE5_SSE_AD-7.6 Online Tests □ Free NSE5_SSE_AD-7.6 Updates □ □ Open { www.dumpsmaterials.com } enter □ NSE5_SSE_AD-7.6 □ and obtain a free download □NSE5_SSE_AD-7.6 Discount Code
- 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, myportal.utt.edu.tt, www.stes.tyc.edu.tw, study.stcs.edu.np, www.stes.tyc.edu.tw, www.connectantigua.com, myportal.utt.edu.tt, study.stcs.edu.np, 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, myportal.utt.edu.tt, Disposable vapes