

Exam Questions NSE7_SDW-7.0

Fortinet NSE 7 - SD-WAN 7.0

https://www.2passeasy.com/dumps/NSE7_SDW-7.0/



NEW QUESTION 1

Which diagnostic command can you use to show the member utilization statistics measured by performance SLAs for the last 10 minutes?

- A. diagnose sys sdwan intf-sla-log
- B. diagnose sys sdwan health-check
- C. diagnose sys sdwan log
- D. diagnose sys sdwan sla-log

Answer: D

Explanation:

SD-WAN 7.2 Study Guide page 321 You can view the stored member metrics by running the diagnose sys sdwan sla-log command. Note that you must include the name of the performance SLA followed by the member configuration index number. To display the SLA logs per interface, you run the diagnose sys sdwan intf-sla-log command.

NEW QUESTION 2

Which are two benefits of using CLI templates in FortiManager? (Choose two.)

- A. You can reference meta fields.
- B. You can configure interfaces as SD-WAN members without having to remove references first.
- C. You can configure FortiManager to sync local configuration changes made on the managed device, to the CLI template.
- D. You can configure advanced CLI settings.

Answer: AD

NEW QUESTION 3

Refer to the exhibit.

```
config system virtual-wan-link
  set status enable
  set load-balance-mode source-ip-based
  config members
    edit 1
      set interface "port1"
      set gateway 100.64.1.254
      set source 100.64.1.1
      set cost 15
    next
    edit 2
      set interface "port2"
      set gateway 100.64.2.254
      set priority 10
    next
  end
end
```

Based on the output shown in the exhibit, which two criteria on the SD-WAN member configuration can be used to select an outgoing interface in an SD-WAN rule? (Choose two.)

- A. Set priority 10.
- B. Set cost 15.
- C. Set load-balance-mode source-ip-ip-based.
- D. Set source 100.64.1.1.

Answer: AB

NEW QUESTION 4

Which two statements describe how IPsec phase 1 main mode is different from aggressive mode when performing IKE negotiation? (Choose two)

- A. A peer ID is included in the first packet from the initiator, along with suggested security policies.
- B. XAuth is enabled as an additional level of authentication, which requires a username and password.
- C. A total of six packets are exchanged between an initiator and a responder instead of three packets.
- D. The use of Diffie Hellman keys is limited by the responder and needs initiator acceptance.

Answer: BC

NEW QUESTION 5

What are two reasons for using FortiManager to organize and manage the network for a group of FortiGate devices? (Choose two)

- A. It simplifies the deployment and administration of SD-WAN on managed FortiGate devices.
- B. It improves SD-WAN performance on the managed FortiGate devices.

- C. It sends probe signals as health checks to the beacon servers on behalf of FortiGate.
- D. It acts as a policy compliance entity to review all managed FortiGate devices.
- E. It reduces WAN usage on FortiGate devices by acting as a local FortiGuard server.

Answer: AE

NEW QUESTION 6

Refer to the exhibits.
 Exhibit A

The screenshot shows the following details for an SD-WAN event:

- Service:** Critical-DIA
- Identity:** Device ID: FGVM01TM22000077, Device Name: branch1_fgt
- Type:** Sub Type: sdwan, Type: event
- Alerts:** Level: notice
- General:** Log Description: SDWAN status, Log ID: 0113022923, Message: Service prioritized by performance metric will be redirected in sequence order., Sequence Number: 2,1, Virtual Domain: root
- Others:** Date/Time: 23:57:29, Destination End User ID: 3, Destination Endpoint ID: 3, Device Time: 2022-03-04 14:57:27, Event Time: 1646434647595788893, Event Type: Service, Metric: latency, Service ID: 1, Time Stamp: 2022-03-04 23:57:29, Time Zone: -0800, UEBA Endpoint ID: 3, UEBA User ID: 3, logger: 700030237

Exhibit B

```
branch1_fgt # diagnose sys sdwan member
Member(1): interface: port1, flags=0x0 , gateway: 192.2.0.2, priority: 0 1024, weight: 0
Member(2): interface: port2, flags=0x0 , gateway: 192.2.0.10, priority: 0 1024, weight: 0

config service
  edit 1
    set name "Critical-DIA"
    set mode priority
    set src "LAN-net"
    set internet-service enable
    set internet-service-app-ctrl 16354 41468 16920
    set health-check "Level3_DNS"
    set priority-members 1 2
  next
end
```

Exhibit A shows an SD-WAN event log and exhibit B shows the member status and the SD-WAN rule configuration. Based on the exhibits, which two statements are correct? (Choose two.)

- A. FortiGate updated the outgoing interface list on the rule so it prefers port2.
- B. Port2 has the highest member priority.
- C. Port2 has a lower latency than port1.
- D. SD-WAN rule ID 1 is set to lowest cost (SLA) mode.

Answer: AC

NEW QUESTION 7

Refer to the exhibit.

```

session info: proto=6 proto_state=11 duration=242 expire=3349 timeout=3600
flags=00000000 socktype=0 sockport=0 av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log dirty may_dirty ndr f00 app_valid
statistic(bytes/packets/allow_err): org=3421/20/1 reply=3777/17/1 tuples=3
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=7->3/3->7 gwy=0.0.0.0/0.0.0.0
hook=post dir=org act=snat 10.0.1.101:34676->128.66.0.1:22(192.2.0.1:34676)
hook=pre dir=reply act=dnat 128.66.0.1:22->192.2.0.1:34676(10.0.1.101:34676)
hook=post dir=reply act=noop 128.66.0.1:22->10.0.1.101:34676(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=2 pol_uuid_idx=14721 auth_info=0 chk_client_info=0 vd=0
serial=000032d9 tos=ff/ff app_list=2000 app=16060 url_cat=0
sdwan_mbr_seq=1 sdwan_service_id=2
rpdb_link_id=ff000002 rpdb_svc_id=0 ngfwid=n/a
npu_state=0x001008

```

Which statement explains the output shown in the exhibit?

- A. FortiGate performed standard FIB routing on the session.
- B. FortiGate will not re-evaluate the session following a firewall policy change.
- C. FortiGate used 192.2.0.1 as the gateway for the original direction of the traffic.
- D. FortiGate must re-evaluate the session due to routing change.

Answer: D

NEW QUESTION 8

Refer to the exhibits.

Exhibit A

```

branch1_fgt # diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
Gen(8), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(manual)
Members(2):
  1: Seq_num(1 port1), alive, selected
  2: Seq_num(2 port2), alive, selected
Internet Service(3): GoToMeeting(4294836966,0,0,0 16354)
Microsoft.Office.365.Portal(4294837474,0,0,0 41468) Salesforce(4294837976,0,0,0 16920)
Src address(1):
  10.0.1.0-10.0.1.255

Service(2): Address Mode(IPV4) flags=0x200 use-shortcut-sla
Gen(7), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(manual)
Members(1):
  1: Seq_num(2 port2), alive, selected
Internet Service(2): Facebook(4294836806,0,0,0 15832) Twitter(4294838278,0,0,0 16001)
Src address(1):
  10.0.1.0-10.0.1.255

branch1_fgt # diagnose sys sdwan internet-service-app-ctrl-list

Facebook(15832 4294836806): 157.240.229.35 6 443 Tue Mar  8 12:24:04 2022
GoToMeeting(16354 4294836966): 23.205.106.86 6 443 Tue Mar  8 12:24:04 2022
GoToMeeting(16354 4294836966): 23.212.249.144 6 443 Tue Mar  8 12:24:39 2022
Salesforce(16920 4294837976): 23.212.249.11 6 443 Tue Mar  8 12:24:04 2022

branch1_fgt # get router info routing-table all
...
S*      0.0.0.0/0 [1/0] via 192.2.0.2, port1
        [1/0] via 192.2.0.10, port2
...

```

Exhibit B

Destination IP	Service	Application	Security Event List	SD-WAN Rule Name	Destination Interface
23.212.248.205	HTTPS	GoToMeeting	APP: 2		port2
23.205.106.86	HTTPS	GoToMeeting	APP: 2	Critical-DIA	port1
23.205.106.86	HTTPS	GoToMeeting	APP: 2	Critical-DIA	port1
23.205.106.86	HTTPS	GoToMeeting	APP: 2	Critical-DIA	port1
23.212.249.144	HTTPS	GoToMeeting	APP: 2	Critical-DIA	port1
23.212.249.144	HTTPS	GoToMeeting	APP: 2		port1
23.212.249.144	HTTPS	GoToMeeting	APP: 2		port2
23.205.106.86	HTTPS	GoToMeeting	APP: 2		port2

Security	APP Count	2
Level	notice	
General	Log ID	000000013
Session ID	769	
Tran Display	snat	
Virtual Domain	root	
Source	Country	Reserved
Device ID	FGVM01TM22000077	
Device Name	branch1_fgt	
IP	10.0.1.101	
Interface	port5	
Interface Role	undefined	
NAT IP	192.2.0.9	
NAT Port	51042	
Port	51042	
Source	10.0.1.101	
UEBA Endpoint ID	1025	
UEBA User ID	3	
Destination	Country	United States
End User ID	3	
Endpoint ID	101	
Host Name	www.gotomeeting.com	
IP	23.212.248.205	
Interface	port2	

An administrator is testing application steering in SD-WAN. Before generating test traffic, the administrator collected the information shown in exhibit A. After generating GoToMeeting test traffic, the administrator examined the respective traffic log on FortiAnalyzer, which is shown in exhibit B. The administrator noticed that the traffic matched the implicit SD-WAN rule, but they expected the traffic to match rule ID 1. Which two reasons explain why the traffic matched the implicit SD-WAN rule? (Choose two.)

- A. FortiGate did not refresh the routing information on the session after the application was detected.
- B. Port1 and port2 do not have a valid route to the destination.
- C. Full SSL inspection is not enabled on the matching firewall policy.
- D. The session 3-tuple did not match any of the existing entries in the ISDB application cache.

Answer: AC

NEW QUESTION 9

Refer to the exhibit.

```
branch1_fgt # diagnose firewall proute list
list route policy info(vf=root):

id=1 dscp_tag=0xff 0xff flags=0x0 tos=0x00 tos_mask=0x00 protocol=17 sport=0-65535 iif=7
dport=53 path(1) oif=3(port1)
source wildcard(1): 0.0.0.0/0.0.0.0
destination wildcard(1): 4.2.2.1/255.255.255.255
hit_count=0 last_used=2022-03-25 10:53:26

id=2131165185(0x7f070001) vwl_service=1(Critical-DIA) vwl_mbr_seq=1 2 dscp_tag=0xff 0xff
flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 sport=0-65535 iif=0 dport=1-65535 path(2)
oif=3(port1) oif=4(port2)
source(1): 10.0.1.0-10.0.1.255
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(3): GoToMeeting(4294836966,0,0,0, 16354)
Microsoft.Office.365.Portal(4294837474,0,0,0, 41468) Salesforce(4294837976,0,0,0, 16920)
hit_count=0 last_used=2022-03-24 12:18:16

id=2131165186(0x7f070002) vwl_service=2(Non-Critical-DIA) vwl_mbr_seq=2 dscp_tag=0xff
0xff flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 sport=0-65535 iif=0 dport=1-65535
path(1) oif=4(port2)
source(1): 10.0.1.0-10.0.1.255
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(2): Facebook(4294836806,0,0,0, 15832) Twitter(4294838278,0,0,0, 16001)
hit_count=0 last_used=2022-03-24 12:18:16

id=2131165187(0x7f070003) vwl_service=3(all_rules) vwl_mbr_seq=1 dscp_tag=0xff 0xff
flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 sport=0-65535 iif=0 dport=1-65535 path(1)
oif=3(port1)
source(1): 0.0.0.0-255.255.255.255
destination(1): 0.0.0.0-255.255.255.255
hit_count=0 last used=2022-03-25 10:58:12
```

Based on the output, which two conclusions are true? (Choose two.)

- A. There is more than one SD-WAN rule configured.
- B. The SD-WAN rules take precedence over regular policy routes.
- C. The all_rules rule represents the implicit SD-WAN rule.
- D. Entry 1(id=1) is a regular policy route.

Answer: AD

NEW QUESTION 10

Refer to the exhibit.

```
branch1_fgt # diagnose sys sdwan service 3

Service(3): Address Mode(IPV4) flags=0x200 use-shortcut-sla
Gen(5), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(priority), link-cost-
factor(latency), link-cost-threshold(10), health-check(VPN_PING)
Members(3):
  1: Seq_num(3 T_INET_0_0), alive, latency: 101.349, selected
  2: Seq_num(4 T_INET_1_0), alive, latency: 151.278, selected
  3: Seq_num(5 T_MPLS_0), alive, latency: 200.984, selected
Src address(1):
  10.0.1.0-10.0.1.255

Dst address(1):
  10.0.0.0-10.255.255.255

branch1_fgt (3) # show
config service
  edit 3
    set name "Corp"
    set mode priority
    set dst "Corp-net"
    set src "LAN-net"
    set health-check "VPN_PING"
    set priority-members 3 4 5
  next
end
```

The exhibit shows the SD-WAN rule status and configuration.

Based on the exhibit, which change in the measured latency will make T_MPLS_0 the new preferred member?

- A. When T_INET_0_0 and T_MPLS_0 have the same latency.
- B. When T_MPLS_0 has a latency of 100 ms.
- C. When T_INET_0_0 has a latency of 250 ms.
- D. When T_MPLS_0 has a latency of 80 ms.

Answer: D**NEW QUESTION 10**

Refer to the exhibit.

```
config system sdwan
  set status enable
  set load-balance source-dest-ip-based
  config zone
    edit "virtual-wan-link"
    next
    edit "SASE"
    next
    edit "underlay"
    next
  end
  config members
    edit 1
      set interface "port1"
      set zone "underlay"
      set gateway 192.2.0.2
    next
    edit 2
      set interface "port2"
      set zone "underlay"
      set gateway 192.2.0.10
    next
  end
  ...
end
```

Which algorithm does SD-WAN use to distribute traffic that does not match any of the SD-WAN rules?

- A. All traffic from a source IP to a destination IP is sent to the same interface.
- B. All traffic from a source IP is sent to the same interface.
- C. All traffic from a source IP is sent to the most used interface.

D. All traffic from a source IP to a destination IP is sent to the least used interface.

Answer: A

NEW QUESTION 15

Which two conclusions for traffic that matches the traffic shaper are true? (Choose two.)

```
# diagnose firewall shaper traffic-shaper list name VoIP_Shaper
name VoIP_Shaper
maximum-bandwidth 6250 KB/sec
guaranteed-bandwidth 2500 KB/sec
current-bandwidth 93 KB/sec
priority 2
overhead 0
tos ff
packets dropped 0
bytes dropped 0
```

- A. The traffic shaper drops packets if the bandwidth is less than 2500 KBps.
- B. The measured bandwidth is less than 100 KBps.
- C. The traffic shaper drops packets if the bandwidth exceeds 6250 KBps.
- D. The traffic shaper limits the bandwidth of each source IP to a maximum of 6250 KBps.

Answer: BC

NEW QUESTION 18

Which two tasks are part of using central VPN management? (Choose two.)

- A. You can configure full mesh, star, and dial-up VPN topologies.
- B. You must enable VPN zones for SD-WAN deployments.
- C. FortiManager installs VPN settings on both managed and external gateways.
- D. You configure VPN communities to define common IPsec settings shared by all VPN gateways.

Answer: AD

NEW QUESTION 21

What are two benefits of using forward error correction (FEC) in IPsec VPNs? (Choose two.)

- A. FEC supports hardware offloading.
- B. FEC improves reliability of noisy links.
- C. FEC transmits parity packets that can be used to reconstruct packet loss.
- D. FEC can leverage multiple IPsec tunnels for parity packets transmission.

Answer: BC

NEW QUESTION 23

Refer to the exhibit.

```
branch1_fgt # diagnose sys sdwan service 1

Service(3): Address Mode(IPV4) flags=0x200 use-shortcut-sla
Gen(6), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(manual)
Members(2):
  1: Seq_num(3 T_INET_0_0), alive, selected
  2: Seq_num(4 T_INET_1_0), alive, selected
Src address(1):
  10.0.1.0-10.0.1.255

Dst address(1):
  10.0.0.0-10.255.255.255

branch1_fgt # diagnose sys sdwan member | grep T_INET_
Member(3): interface: T_INET_0_0, flags=0x4 , gateway: 100.64.1.1, priority: 10 1024,
weight: 0
Member(4): interface: T_INET_1_0, flags=0x4 , gateway: 100.64.1.9, priority: 0 1024,
weight: 0

branch1_fgt # get router info routing-table all | grep T_INET_
S      10.0.0.0/8 [1/0] via T_INET_1_0 tunnel 100.64.1.9
```

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 T_INET_0_0. However, the traffic is routed over T_INET_1_0.

Based on the output shown in the exhibit, which two reasons can cause the observed behavior? (Choose two.)

- A. The traffic matches a regular policy route configured with T_INET_1_0 as the outgoing device.
- B. T_INET_1_0 has a lower route priority value (higher priority) than T_INET_0_0.
- C. T_INET_0_0 does not have a valid route to the destination.
- D. T_INET_1_0 has a higher member configuration priority than T_INET_0_0.

Answer: AC

Explanation:

<https://community.fortinet.com/t5/FortiGate/Technical-Tip-Assigning-Priority-to-SD-WAN-Members-for-Defau>

NEW QUESTION 26

Which statement about using BGP for ADVPN is true?

- A. IBGP is preferred over EBGP, because IBGP preserves next hop information.
- B. You must use BGP to route traffic for both overlay and underlay links.
- C. You must configure BGP communities.
- D. You must configure AS path prepending.

Answer: A

NEW QUESTION 31

Refer to the exhibit.

```
config vpn ipsec phase1-interface
  edit "FIRST_VPN"
    set type dynamic
    set interface "port1"
    set peertype any
    set proposal aes128-sha256 aes256-sha38
    set dhgrp 14 15 19
    set xauthtype auto
    set authusrgrp "first-group"
    set psksecret fortinet1
  next
  edit "SECOND_VPN"
    set type dynamic
    set interface "port1"
    set peertype any
    set proposal aes128-sha256 aes256-sha38
    set dhgrp 14 15 19
    set xauthtype auto
    set authusrgrp "second-group"
    set psksecret fortinet2
  next
edit
```

FortiGate has multiple dial-up VPN interfaces incoming on port1 that match only FIRST_VPN.

Which two configuration changes must be made to both IPsec VPN interfaces to allow incoming connections to match all possible IPsec dial-up interfaces? (Choose two.)

- A. Specify a unique peer ID for each dial-up VPN interface.
- B. Use different proposals are used between the interfaces.
- C. Configure the IKE mode to be aggressive mode.
- D. Use unique Diffie Hellman groups on each VPN interface.

Answer: AC

NEW QUESTION 32

Refer to the exhibits.

Exhibit A

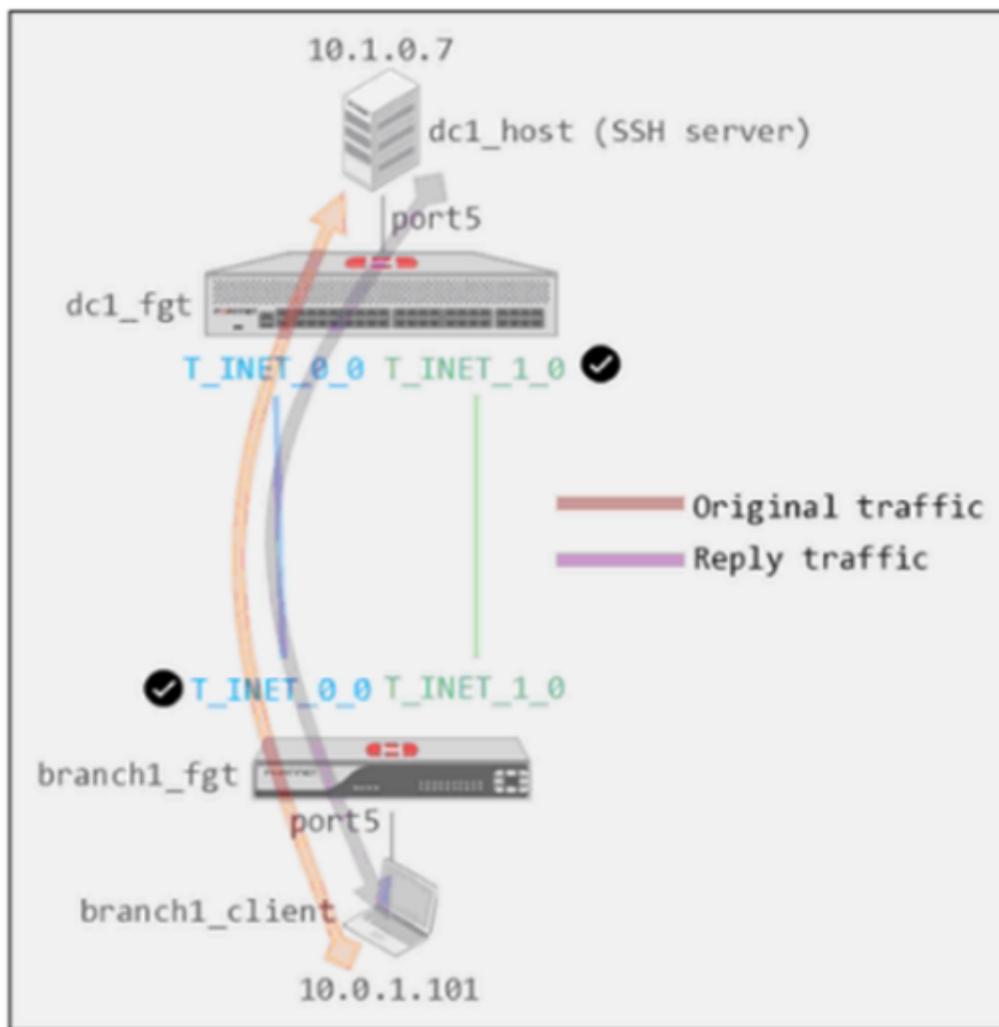


Exhibit B

```

dc1_fgt # show system global
config system global
    set admin-https-redirect disable
    set admintimeout 480
    set alias "FortiGate-VM64"
    set hostname "dc1_fgt"
    set timezone 04
end

dc1_fgt # show system settings
config system settings
    set tcp-session-without-syn enable
    set allow-subnet-overlap enable
    set gui-allow-unnamed-policy enable
    set gui-multiple-interface-policy enable
end
    
```

Exhibit A shows a site-to-site topology between two FortiGate devices: branch1_fgt and dc1_fgt. Exhibit B shows the system global and system settings configuration on dc1_fgt.

When branch1_client establishes a connection to dc1_host, the administrator observes that, on dc1_fgt, the reply traffic is routed over T_INET_0_0, even though T_INET_1_0 is the preferred member in the matching SD-WAN rule.

Based on the information shown in the exhibits, what configuration change must be made on dc1_fgt so dc1_fgt routes the reply traffic over T_INET_1_0?

- A. Enable auxiliary-session under config system settings.
- B. Disable tcp-session-without-syn under config system settings.
- C. Enable snat-route-change under config system global.
- D. Disable allow-subnet-overlap under config system settings.

Answer: A

Explanation:

Controlling return path with auxiliary session When multiple incoming or outgoing interfaces are used in ECMP or for load balancing, changes to routing, incoming, or return traffic interfaces impacts how an existing sessions handles the traffic. Auxiliary sessions can be used to handle these changes to traffic patterns.
<https://docs.fortinet.com/document/fortigate/7.0.11/administration-guide/14295/controlling-return-path>

NEW QUESTION 35

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual NSE7_SDW-7.0 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the NSE7_SDW-7.0 Product From:

https://www.2passeasy.com/dumps/NSE7_SDW-7.0/

Money Back Guarantee

NSE7_SDW-7.0 Practice Exam Features:

- * NSE7_SDW-7.0 Questions and Answers Updated Frequently
- * NSE7_SDW-7.0 Practice Questions Verified by Expert Senior Certified Staff
- * NSE7_SDW-7.0 Most Realistic Questions that Guarantee you a Pass on Your First Try
- * NSE7_SDW-7.0 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year