Free NSE7_OTS-6.4 Braindumps Download Updated on Nov 17, 2023 with 37 Questions [Q13-Q28
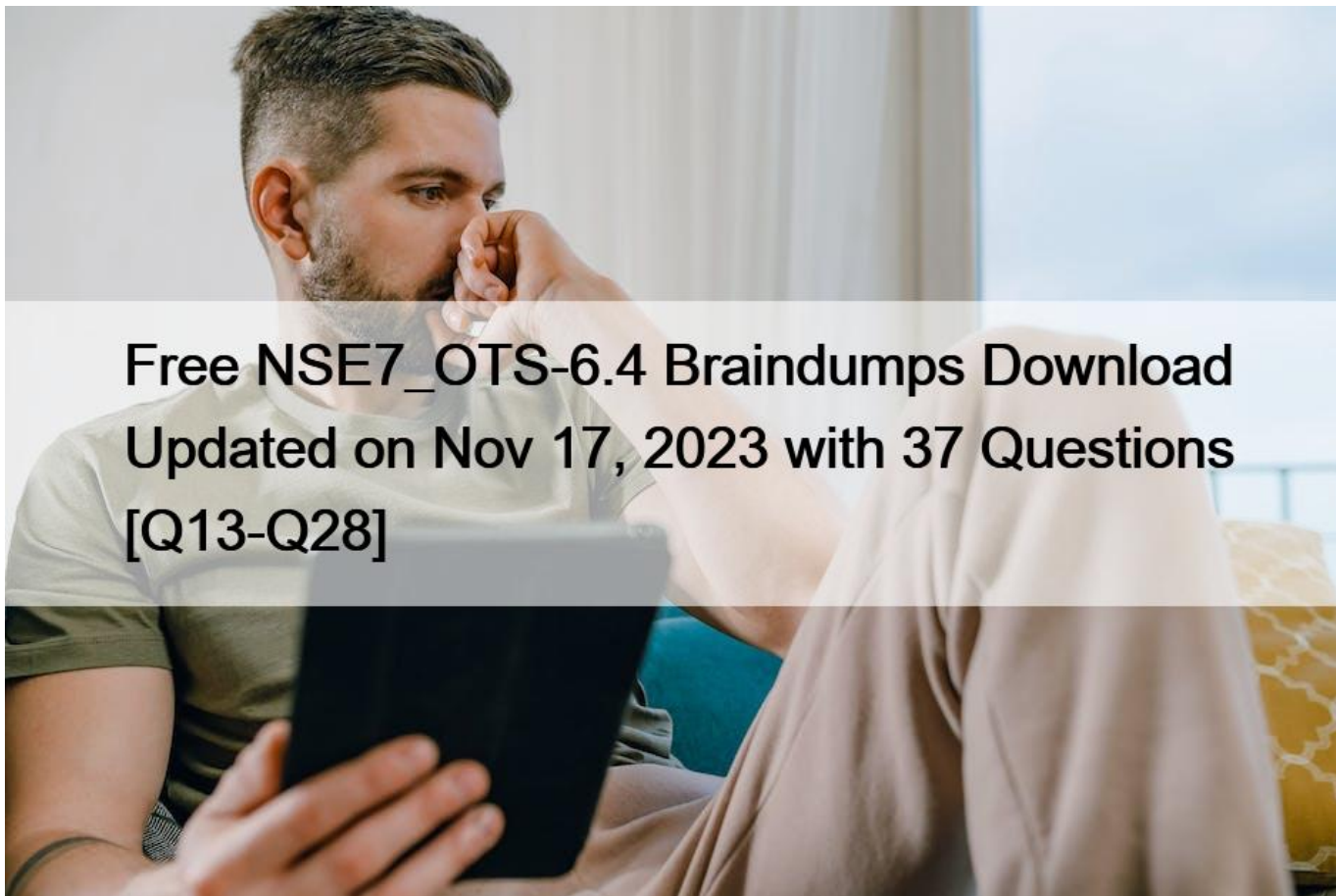

Free NSE7_OTS-6.4 Braindumps Download Updated on Nov 17, 2023 with 37 Questions
Fortinet NSE7_OTS-6.4 Exam Practice Test Questions

Fortinet NSE7_OTS-6.4 (Fortinet NSE 7 - OT Security 6.4) certification exam is designed to test the knowledge and skills of network security professionals who specialize in operational technology (OT) security. Fortinet NSE 7 - OT Security 6.4 certification validates an individual's ability to design, implement and manage OT security solutions using Fortinet's products and technologies.

The NSE7_OTS-6.4 certification is ideal for security professionals who have experience working with OT systems and want to demonstrate their expertise in this area. It is also a valuable certification for IT professionals who want to expand their skills and knowledge to include OT security. By earning the NSE7_OTS-6.4 certification, candidates can position themselves as experts in OT security and increase their value to employers who are looking for skilled professionals to help protect their critical infrastructure.

NEW QUESTION 13

Which three Fortinet products can be used for device identification in an OT industrial control system (ICS)? (Choose three.)
* FortiNAC
* FortiManager
* FortiAnalyzer
* FortiSIEM
* FortiGate

NEW QUESTION 14

Refer to the exhibit.

Given the configurations on the FortiGate, which statement is true?
* FortiGate is configured with forward-domains to reduce unnecessary traffic.
* FortiGate is configured with forward-domains to forward only domain controller traffic.
* FortiGate is configured with forward-domains to forward only company domain website traffic.
* FortiGate is configured with forward-domains to filter and drop non-domain controller traffic.

NEW QUESTION 15

An OT network architect needs to secure control area zones with a single network access policy to provision devices to any number of different networks.

On which device can this be accomplished?
* FortiGate
* FortiEDR
* FortiSwitch
* FortiNAC

NEW QUESTION 16

In a wireless network integration, how does FortiNAC obtain connecting MAC address information?
* RADIUS
* Link traps
* End station traffic monitoring
* MAC notification traps
FortiNAC can integrate with RADIUS servers to obtain MAC address information for wireless clients that authenticate through the RADIUS server.

Reference:

Fortinet NSE 7 – OT Security 6.4 Study Guide, Chapter 4: OT Security Devices, page 4-28.

NEW QUESTION 17

Which three methods of communication are used by FortiNAC to gather visibility information? (Choose three.)
* SNMP
* ICMP
* API
* RADIUS
* TACACS

NEW QUESTION 18

When you create a user or host profile, which three criteria can you use? (Choose three.)
* Host or user group memberships
* Administrative group membership
* An existing access control policy
* Location
* Host or user attributes
https://docs.fortinet.com/document/fortinac/9.2.0/administration-guide/15797/user-host-profiles

NEW QUESTION 19

An administrator wants to use FortiSoC and SOAR features on a FortiAnalyzer device to detect and block any unauthorized access to FortiGate devices in an OT network.
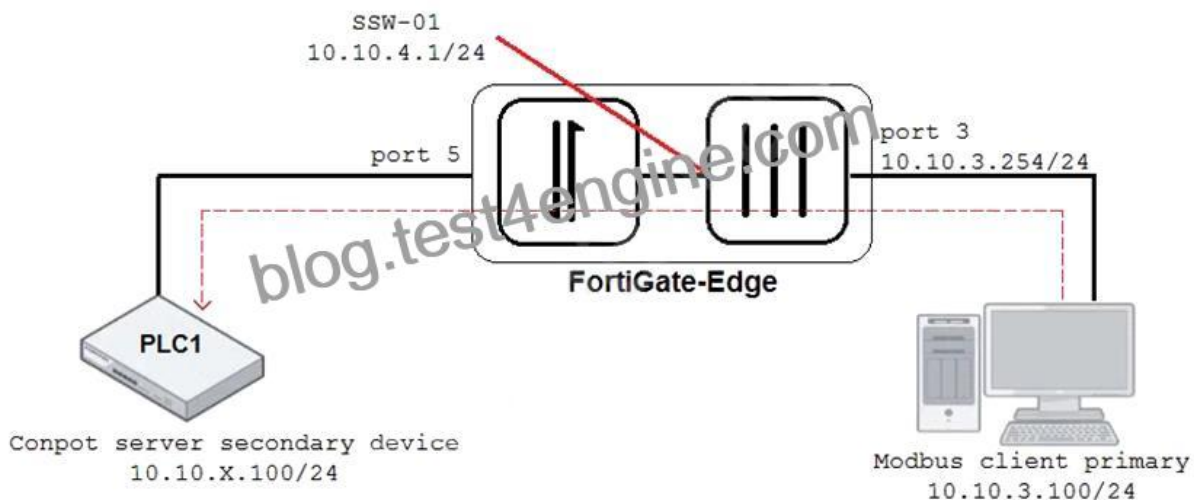
Which two statements about FortiSoC and SOAR features on FortiAnalyzer are true? (Choose two.)
* You must set correct operator in event handler to trigger an event.
* You can automate SOC tasks through playbooks.
* Each playbook can include multiple triggers.
* You cannot use Windows and Linux hosts security events with FortiSoC.
Ref: https://docs.fortinet.com/document/fortianalyzer/7.0.0/administration-guide/268882/fortisoc

NEW QUESTION 20

Refer to the exhibit.

SSW-01
10.10.4.1/24

port 5

port 3
10.10.3.254/24

FortiGate-Edge

PLC1

Conpot server secondary device
10.10.X.100/24

Modbus client primary
10.10.3.100/24

An OT architect has implemented a Modbus TCP with a simulation server Conpot to identify and control the Modus traffic in the OT network. The FortiGate-Edge device is configured with a software switch interface ssw-01.

Based on the topology shown in the exhibit, which two statements about the successful simulation of traffic between client and server are true? (Choose two.)
* The FortiGate-Edge device must be in NAT mode.
* NAT is disabled in the FortiGate firewall policy from port3 to ssw-01.
* The FortiGate devices is in offline IDS mode.
* Port5 is not a member of the software switch.

NEW QUESTION 21

Refer to the exhibit.
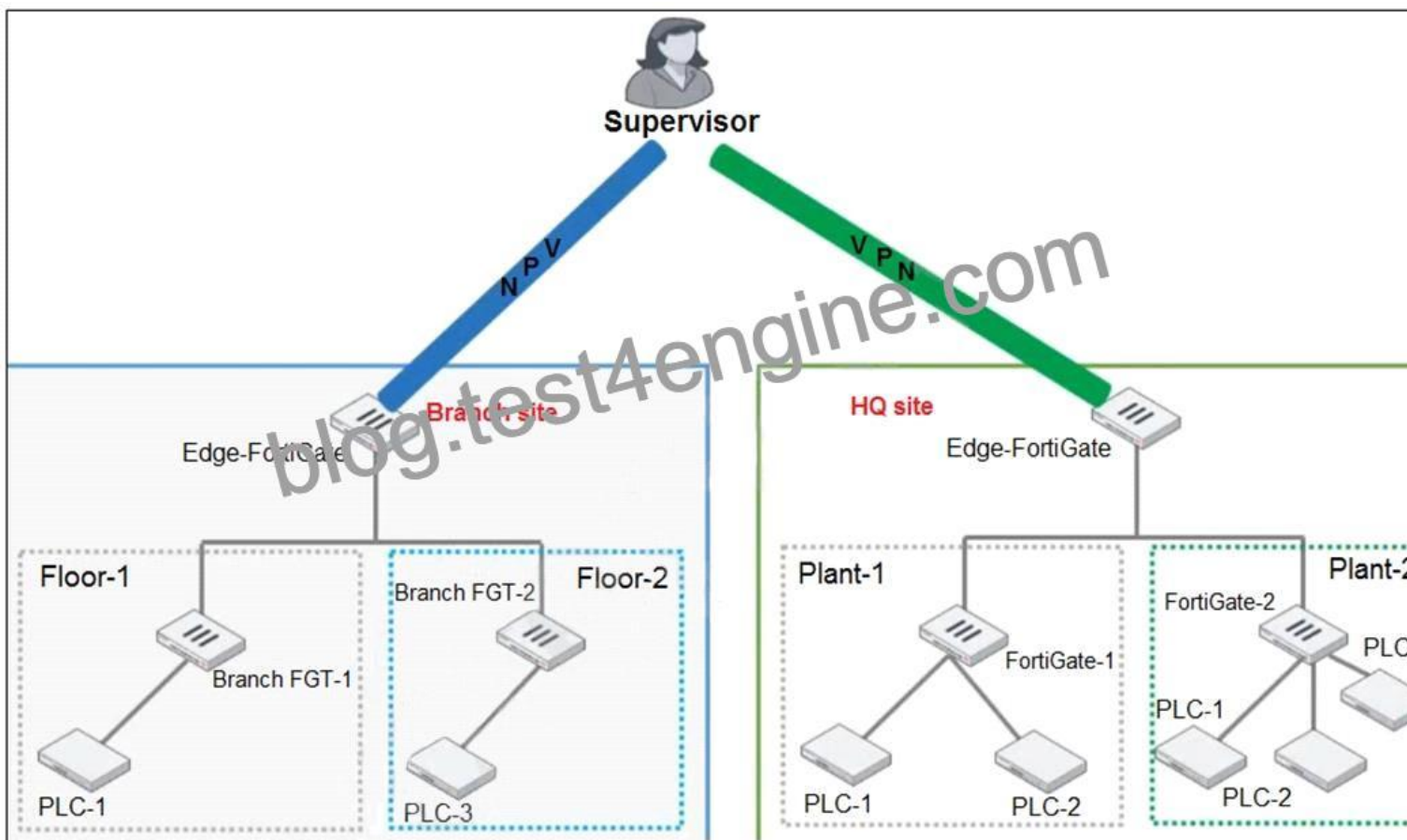
You need to configure VPN user access for supervisors at the breach and HQ sites using the same soft FortiToken. Each site has a FortiGate VPN gateway.

What must you do to achieve this objective?
* You must use a FortiAuthenticator.
* You must register the same FortiToken on more than one FortiGate.

* You must use the user self-registration server.
* You must use a third-party RADIUS OTP server.

NEW QUESTION 22

An OT network architect must deploy a solution to protect fuel pumps in an industrial remote network. All the fuel pumps must be closely monitored from the corporate network for any temperature fluctuations.

How can the OT network architect achieve this goal?
* Configure a fuel server on the remote network, and deploy a FortiSIEM with a single pattern temperature security rule on the corporate network.
* Configure a fuel server on the corporate network, and deploy a FortiSIEM with a single pattern temperature performance rule on the remote network.
* Configure a fuel server on the remote network, and deploy a FortiSIEM with a single pattern temperature performance rule on the corporate network.
* Configure both fuel server and FortiSIEM with a single-pattern temperature performance rule on the corporate network.

NEW QUESTION 23

An OT supervisor has configured LDAP and FSSO for the authentication. The goal is that all the users be authenticated against passive authentication first and, if passive authentication is not successful, then users should be challenged with active authentication.

What should the OT supervisor do to achieve this on FortiGate?
* Configure a firewall policy with LDAP users and place it on the top of list of firewall policies.
* Enable two-factor authentication with FSSO.
* Configure a firewall policy with FSSO users and place it on the top of list of firewall policies.
* Under config user settings configure set auth-on-demand implicit.
The OT supervisor should configure a firewall policy with FSSO users and place it on the top of list of firewall policies in order to achieve the goal of authenticating users against passive authentication first and, if passive authentication is not successful, then challenging them with active authentication.

NEW QUESTION 24

When you create a user or host profile, which three criteria can you use? (Choose three.)
* Host or user group memberships
* Administrative group membership
* An existing access control policy
* Location
* Host or user attributes

NEW QUESTION 25

An OT administrator configured and ran a default application risk and control report in FortiAnalyzer to learn more about the key application crossing the network. However, the report output is empty despite the fact that some related real-time and historical logs are visible in the FortiAnalyzer.

What are two possible reasons why the report output was empty? (Choose two.)
* The administrator selected the wrong logs to be indexed in FortiAnalyzer.
* The administrator selected the wrong time period for the report.

* The administrator selected the wrong devices in the Devices section.
* The administrator selected the wrong hcache table for the report.
https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/32cb817d-a307-11eb-b70b-00505692583a/FortiAnalyzer-7
.0.0-Administration_Guide.pdf

NEW QUESTION 26

Refer to the exhibit.
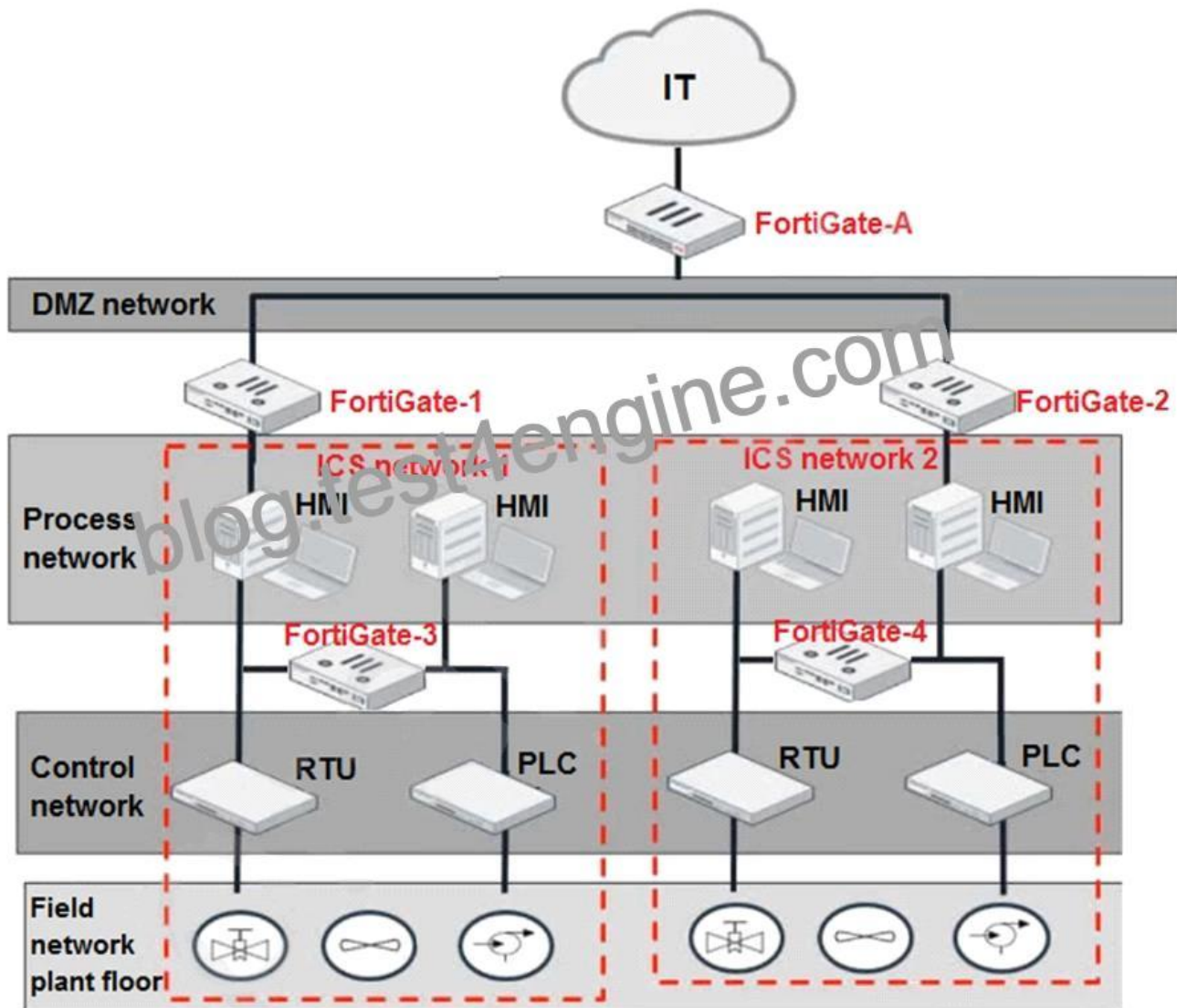
Based on the topology designed by the OT architect, which two statements about implementing OT security are true? (Choose two.)
* Firewall policies should be configured on FortiGate-3 and FortiGate-4 with industrial protocol sensors.
* Micro-segmentation can be achieved only by replacing FortiGate-3 and FortiGate-4 with a pair of FortiSwitch devices.
* IT and OT networks are separated by segmentation.
* FortiGate-3 and FortiGate-4 devices must be in a transparent mode.

NEW QUESTION 27

Which three criteria can a FortiGate device use to look for a matching firewall policy to process traffic? (Choose three.)

* Services defined in the firewall policy.
* Source defined as internet services in the firewall policy
* Lowest to highest policy ID number
* Destination defined as internet services in the firewall policy
* Highest to lowest priority defined in the firewall policy

The three criteria that a FortiGate device can use to look for a matching firewall policy to process traffic are:

1. Services defined in the firewall policy – FortiGate devices can match firewall policies based on the services defined in the policy, such as HTTP, FTP, or DNS.

2. Destination defined as internet services in the firewall policy – FortiGate devices can also match firewall policies based on the destination of the traffic, including destination IP address, interface, or internet services.

3. Highest to lowest priority defined in the firewall policy – FortiGate devices can prioritize firewall policies based on the priority defined in the policy. The device will process traffic against the policy with the highest priority first and move down the list until it finds a matching policy.

Reference:

Fortinet NSE 7 – Enterprise Firewall 6.4 Study Guide, Chapter 4: Policy Implementation, page 4-18.

NEW QUESTION 28

Refer to the exhibit and analyze the output.

```
[PH_DEV_MON_NET_INTF_UTIL] : [eventSeverity] =PHL_INFO, [filename] =phPerfJob.cpp,
[lineNumber] =6646, [intfName]= Intel [R] PRO_100 MT Network
Connection, [intfAlias] =, [hostname] =WIN2K8PC.[hostIpAddr] = 192.168.69.6,
[pollIntv] =56, [recvBytes64] =
44273, [recvBitsPerSec] = 6324.011266, [inIntfUtil] = 0.000632, [sentBytes64] =
82014, [sentBitsPerSec] = 1171
6.285714, [outIntfUtil] = 0.001172, [recvPkts64] = 449, [sentPkts64] = 255,
[inIntfPktErr] = 0, [inIntfPktErrPct] = 0.000000, [outIntfPktErr] =0,
[outIntfPktErrPct] = 0.000000, [inIntfPktDiscarded] =0, [inIntfPktDiscardedPct] =
```

Which statement about the output is true?

* This is a sample of a FortiAnalyzer system interface event log.
* This is a sample of an SNMP temperature control event log.
* This is a sample of a PAM event type.
* This is a sample of FortiGate interface statistics.

The Importance of Fortinet NSE7_OTS-6.4 Exam

Fortinet NSE7_OTS-6.4 Exam is one of the most important exams that you should pass before you can apply for a job with Fortinet. You should be able to pass the exam before you apply for a job because passing the exam will help you gain credibility with your future employers and will help you show them that you have the knowledge and experience to be successful in your job. The NSE7_OTS-6.4 certification exam can be very useful for some people, especially for IT professionals. There are many IT professionals who want to get the Fortinet NSE7_OTS-6.4 Certification Exam after preparing with **NSE7_OTS-6.4 exam dumps**, so they can have better job opportunities and earn more money in the future. Braindumps customer material is a very important part of the Fortinet NSE7_OTS-6.4 training material. The experts have designed the updated Fortinet NSE7_OTS-6.4 Certification Exam questions, which will bring you the confidence to pass the Fortinet NSE7_OTS-6.4 exam for the first time. Unique multiple assured answers, pass rate guarantee.

Updated Verified NSE7_OTS-6.4 dumps Q&As - Pass Guarantee or Full Refund:

https://www.test4engine.com/NSE7_OTS-6.4_exam-latest-braindumps.html]