



NSE6_FNC-8.5^{Q&As}

Fortinet NSE 6 - FortiNAC 8.5





Pass Fortinet NSE6_FNC-8.5 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/nse6_fnc-8-5.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers





QUESTION 1

During the on-boarding process through the captive portal, why would a host that successfully registered remain stuck in the Registration VLAN? (Choose two.)

- A. The wrong agent is installed.
- B. Bridging is enabled on the host.
- C. There is another unregistered host on the same port.
- D. The ports default VLAN is the same as the Registration VLAN.

Correct Answer: AD

Scenario 4: NAT detection disabled, using endpoint compliance policy and agent.

Reference: <https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/868f1267-7299-11e981a4-00505692583a/fortinac-admin-operation-85.pdf>

QUESTION 2

Which three circumstances trigger Layer 2 polling of infrastructure devices? (Choose three.)

- A. A matched security policy
- B. Scheduled poll timings
- C. Linkup and Linkdown traps
- D. Manual polling
- E. A failed Layer 3 poll

Correct Answer: BCD

QUESTION 3

Which connecting endpoints are evaluated against all enabled device profiling rules?

- A. Known trusted devices each time they change location
- B. Rogues devices, each time they connect
- C. Rogues devices, only when they connect for the first time
- D. All hosts, each time they connect

Correct Answer: A

FortiNAC process to classify rogue devices and create an organized inventory of known trusted registered devices.



Reference: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/9529d49c-892c-11e981a4-00505692583a/FortiNAC_Device_Profiler_Configuration.pdf

QUESTION 4

How should you configure MAC notification traps on a supported switch?

- A. Configure them only on ports set as 802.1q trunks
- B. Configure them on all ports except uplink ports
- C. Configure them on all ports on the switch
- D. Configure them only after you configure linkup and linkdown traps

Correct Answer: B

Configure SNMP MAC Notification traps on all access ports (do not include uplinks).

Reference: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/be7fcde9-9685-11e981a4-00505692583a/Configuring_Traps_for_MAC_Notification.pdf

QUESTION 5

With enforcement for network access policies and at-risk hosts enabled, what will happen if a host matches a network access policy and has a state of "at risk"?

- A. The host is provisioned based on the network access policy.
- B. The host is provisioned based on the default access defined by the point of connection.
- C. The host is isolated.
- D. The host is administratively disabled.

Correct Answer: A

Reference: <https://docs.fortinet.com/document/fortinac/8.6.0/administration-guide/49701/policy-assignment>

[NSE6_FNC-8.5 Study Guide](#)

[NSE6_FNC-8.5 Exam Questions](#)

[NSE6_FNC-8.5 Braindumps](#)