

Fortinet

NSE6_FNC_AD-7.6

Fortinet NSE 6 - FortiNAC-F 7.6 Administrator



For More Information – Visit link below:

<https://www.examsboost.com/>

Product Version

- ✓ Up to Date products, reliable and verified.
- ✓ Questions and Answers in PDF Format.

Latest Version: 6.0

Question: 1

When performing a wireless integration, what must be configured for FortiNAC-F to provide the MAC address information of a connecting device?

- A. MAC notification traps
- B. Link traps
- C. RADIUS
- D. Syslog messaging

Answer: C

Question: 2

A user had full corporate network and internet access for most of the day but has now been isolated and is redirected to a quarantine/remediation webpage. What would cause this behavior?

- A. The logged on user is not found in the active directory.
- B. The host has been marked as failed for an admin scan.
- C. The host has been administratively disabled.
- D. The host was removed from the Registered Hosts group.

Answer: B

Question: 3

Two FortiNAC-F devices have been configured in a 1+1 active-passive HA configuration. Which condition would cause the primary FortiNAC-F to shut down the NAC process and change the management status to down?

- A. The primary misses five heartbeats and fails to ping the gateway.
- B. The secondary takes control of the primary.
- C. An administrator changes the status of the secondary to Running – In Control.
- D. The primary fails to poll the secondary while the gateway responds successfully.

Answer: A

Question: 4

How are logical networks assigned to endpoints?

- A. Through device profiling rules
- B. Through FortiGate IPv4 policies
- C. Through model configuration settings
- D. Through network access policies

Answer: D

Question: 5

An administrator wants to incorporate a third-party security device to generate security events and alarms. The third-party device is configured to send syslog messages to FortiNAC-F. Which two items must be completed? (Choose two.)

- A. A security incident rule
- B. A compliance policy
- C. A security event parser
- D. A trap MIB file

Answer: A,CC

Question: 6

During an initial installation, which configuration must be applied to allow for the modeling of infrastructure devices?

- A. set allowaccess dns
- B. set allowaccess snmp
- C. set allowaccess radius-auth
- D. set allowaccess dhcp

Answer: B

Question: 7

An administrator wants to use FortiNAC-F to collect an application inventory for hosts. Which two options would satisfy this requirement?
(Choose two.)

- A. Agent technology
- B. MDM integration
- C. Device profiling rules
- D. Portal page on-boarding options

Answer: A,B

Question: 8

Refer to the exhibit.

Device Profiling Rules - Total: 17							
Rank:		Set Rank		Enable:		Rogue Evaluation Queue Size: 0 Detail Flush	
Enabled	Rank	Name	Type	Registration	Methods	Register as Device	
	1	Printer (DHCP)	Printer	Manual	DHCP	Host View	
	2	APC - UPS	UPS	Automatic	Active, HTTP, Vendor OUI	Host View	
	3	Medical Device	Health Care Device	Automatic	Vendor OUI	Host View	
	4	FortiCamera (ONVIF)	Camera	Automatic	ONVIF	Host View	
	5	Printer (TCP:80,515,9100)	Printer	Manual	TCP	Host View	
	6	Android (DHCP)	Android	Automatic	DHCP	Host View	

If a device connects to the network for the first time, and FortiNAC-F does not receive a DHCP fingerprint, what would be the next step in the device profiling process?

- A. The device would be modeled as a generic device.
- B. After 5 minutes, the device would be evaluated against the next rule.
- C. The FortiNAC-F would attempt to get a session fingerprint from a modeled firewall.
- D. The device would be added to the database as a rogue.

Answer: D

Question: 9

A network administrator wants to use network access policies to define access for different types of hosts. Which group must be populated with all the possible points of connection?

- A. Forced Registration
- B. Role-Based access
- C. Authorized access points
- D. Forced Remediation

Answer: B

Question: 10

Refer to the exhibit.

Edit Action

Name

Disable Host Action

Stop on Activity Failure

☒

Delay Secondary Task(s)

☐

Activities

+ Create New

Edit

Delete

+ Search

Rank	Activity
1	Disable Host - Secondary Task: Enable Host
2	Mark Host at Risk for "Guest No Access"

2 | Updated: 13:18:59

An administrator adds an action to a security rule. What happens to the host that triggers the security rule?

- A. The host is marked at risk.
- B. The host is disabled but is not marked at risk until an administrator manually executes the secondary task.
- C. The host is disabled, but no further action is taken.
- D. The host is disabled and then marked at-risk.

Answer: D

Thank You for Trying Our Product

For More Information – **Visit link below:**

<https://www.examsboost.com/>

15 USD Discount Coupon Code:

G74JA8UF

FEATURES

- ✓ **90 Days Free Updates**
- ✓ **Money Back Pass Guarantee**
- ✓ **Instant Download or Email Attachment**
- ✓ **24/7 Live Chat Support**
- ✓ **PDF file could be used at any Platform**
- ✓ **50,000 Happy Customer**



Visit us at: <https://www.examsboost.com/test/nse6-fnc-ad-7-6>