

Fortinet

Exam Questions NSE6_FNC-7.2

Fortinet NSE 6 - FortiNAC 7.2



NEW QUESTION 1

Which three of the following are components of a security rule? (Choose three.)

- A. Security String
- B. Methods
- C. Action
- D. User or host profile
- E. Trigger

Answer: CDE

Explanation:

Reference: <https://docs.fortinet.com/document/fortinac/8.8.0/administration-guide/167668/add-or-modify-a-rule>

NEW QUESTION 2

During an evaluation of state-based enforcement, an administrator discovers that ports that should not be under enforcement have been added to enforcement groups. In which view would the administrator be able to determine who added the ports to the groups?

- A. The Alarms view
- B. The Admin Auditing view
- C. The Event Management view
- D. The Security Events view

Answer: B

NEW QUESTION 3

By default, if after a successful Layer 2 poll, more than 20 endpoints are seen connected on a single switch port simultaneously, what happens to the port?

- A. The port becomes a threshold uplink
- B. The port is disabled
- C. The port is added to the Forced Registration group
- D. The port is switched into the Dead-End VLAN

Answer: A

Explanation:

If more than 20 endpoints are seen connected on a single switch port simultaneously after a successful Layer 2 poll, the port is designated as an uplink. FortiNAC will ignore all physical addresses learned on an uplink port and will not perform any control operations on it

NEW QUESTION 4

In a wireless integration, what method does FortiNAC use to obtain connecting MAC address information?

- A. SNMP traps
- B. RADIUS
- C. Endstation traffic monitoring
- D. Link traps

Answer: B

Explanation:

In a wireless integration, FortiNAC uses RADIUS to obtain connecting MAC address information. This includes RADIUS requests to FortiNAC and subsequent RADIUS responses from FortiNAC to the requesting device

NEW QUESTION 5

How are logical networks assigned to endpoints?

- A. Through device profiling rules
- B. Through network access policies
- C. Through Layer 3 polling configurations
- D. Through FortiGate IPv4 policies

Answer: A

Explanation:

Logical networks are assigned to endpoints through device profiling rules in FortiNAC. These networks appear in device Model Configuration views and are used for endpoint isolation based on the endpoint's state or status

NEW QUESTION 6

Which group type can have members added directly from the FortiNAC Control Manager?

- A. Administrator
- B. Device
- C. Port
- D. Host

Answer: B

Explanation:

The study guide explains that there are six different types of groups in FortiNAC, including device, host, IP phone, port, user, and administrator groups. Groups created by administrative users or imported as a result of an LDAP integration can be used to organize elements but do not enforce any type of control or functionality directly

NEW QUESTION 7

Which three are components of a security rule? (Choose three.)

- A. Methods
- B. Security String
- C. Trigger
- D. User or host profile
- E. Action

Answer: CDE

Explanation:

Components of a security rule in FortiNAC include:

? Trigger: The condition or event that initiates the evaluation of the rule.

? User or Host Profile: A requirement that can be added to a rule to specify the user or host profile that must be matched.

? Action: The activities or responses that FortiNAC performs when the rule is matched.

References

? FortiNAC 7.2 Study Guide, page 419

NEW QUESTION 8

By default, if more than 20 hosts are seen connected on a single port simultaneously, what will happen to the port?

- A. The port is switched into the Dead-End VLAN.
- B. The port becomes a threshold uplink.
- C. The port is disabled.
- D. The port is added to the Forced Registration group.

Answer: B

Explanation:

Admin Guide p. 754: Threshold Uplink—The Uplink mode has been set as Dynamic and FortiNAC has determined that the number of MAC addresses on the port exceeds the System Defined Uplink count. All hosts read on this port are ignored.

NEW QUESTION 9

An administrator wants the Host At Risk event to generate an alarm. What is used to achieve this result?

- A. A security trigger activity
- B. A security filter
- C. An event to alarm mapping
- D. An event to action mapping

Answer: C

Explanation:

To generate an alarm from a Host At Risk event, an administrative user must create an Event to Alarm Mapping for the Vulnerability Scan Failed event. Within this alarm mapping, a host security action must be designated to mark the host at risk

NEW QUESTION 10

What method of communication does FortiNAC use to control VPN host access on FortiGate?

- A. RSSO
- B. Security Fabric
- C. RADIUS accounting
- D. SAMLSSO

Answer: B

NEW QUESTION 10

Which command line shell and scripting language does FortiNAC use for WinRM?

- A. Linux
- B. Bash
- C. DOS
- D. Powershell

Answer: D

Explanation:

Open Windows PowerShell or a command prompt. Run the following command to determine if you already have WinRM over HTTPS configured.

Reference: <https://docs.fortinet.com/document/fortinac/8.7.0/administration-guide/246310/winrm-device-profile-requirements-and-setup>

Admin Guide on p. 362, "Matches if the device successfully responds to a WinRM client session request. User name and password credentials are required. If there are multiple credentials, each set of credentials will be attempted to find a potential match. The commands are used to automate interaction with the device. Each command is run via Powershell."

NEW QUESTION 15

Which three capabilities does FortiNAC Control Manager provide? (Choose three.)

- A. Global visibility
- B. Global authentication security policies
- C. Global infrastructure device inventory
- D. Global version control
- E. Pooled licenses

Answer: ADE

NEW QUESTION 19

Which system group will force at-risk hosts into the quarantine network, based on point of connection?

- A. Physical Address Filtering
- B. Forced Quarantine
- C. Forced Isolation
- D. Forced Remediation




Answer: D

Explanation:

Forced Quarantine, study guide 7.2 pag 245 and 248

NEW QUESTION 23

Refer to the exhibit.

Adapters - Total: 12				
Status	Host Status	Physical Address	Connected Container	Rule Name
		00:03:E3:C9:81:52	Wired Infrastructure	
		00:06:D6:AC:7F:17	Wired Infrastructure	Lab Hosts

Considering the host status of the two hosts connected to the same wired port, what will happen if the port is a member of the Forced Registration port group?

- A. The port will be provisioned for the normal state host, and both hosts will have access to that VLAN.
- B. The port will not be managed, and an event will be generated.
- C. The port will be provisioned to the registration network, and both hosts will be isolated.
- D. The port will be administratively shut down.

Answer: C

Explanation:

The exhibit shows the status of two hosts connected to a wired infrastructure and indicates their respective MAC addresses and the rule name associated with them. When a port is a member of the Forced Registration port group, and multiple hosts with different statuses are connected to that port, FortiNAC will provision the port to the registration network, which is designed to isolate hosts until they are verified or registered. This ensures that unregistered or unauthorized hosts do not gain access to the network. Therefore, both hosts will be isolated in the registration network according to FortiNAC policy for such scenarios.

NEW QUESTION 28

Two FortiNAC devices have been configured in an HA configuration. After five failed heartbeats between the primary device and secondary device, the primary device fail to ping the designated gateway. What happens next?

- A. The primary device continues to operate as the in-control device and changes the status of secondary device to contact lost.
- B. The primary device changes its designation to secondary, and the secondary device changes to primary.
- C. The primary device shuts down NAC processes and changes to a management down status.
- D. The primary device waits 3 minutes and attempts to re-establish the HA heartbeat before attempting a second ping of the gateway.

Answer: C

NEW QUESTION 33

What agent is required in order to detect an added USB drive?

- A. Persistent
- B. Dissolvable
- C. Mobile
- D. Passive

Answer: A

Explanation:

Expand the Persistent Agent folder. Select USB Detection from the tree.

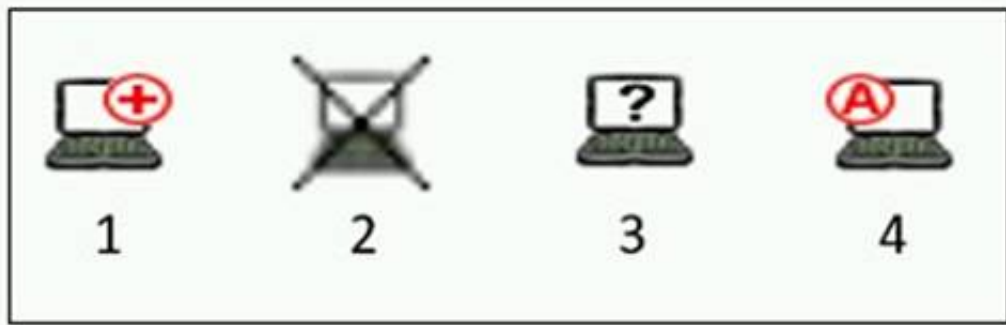
Reference: <https://docs.fortinet.com/document/fortinac/7.2.2/administration-guide/814147/usb-detection>

* 1. Click System > Settings.

- * 2. Expand the Persistent Agent folder.
- * 3. Select USB Detection from the tree.
- * 4. Click Add or select an existing USB drive and click Modify.

NEW QUESTION 36

Refer to the exhibit, and then answer the question below.



Which host is rogue?

- A. 1
- B. 3
- C. 2
- D. 4

Answer: B

Explanation:

Reference: <https://docs.fortinet.com/document/fortinac/8.6.0/administration-guide/283146/evaluating-rogue-hosts>

NEW QUESTION 41

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

Answer: C

Explanation:

https://training.fortinet.com/pluginfile.php/1912463/mod_resource/content/26/FortiNAC_7.2_Study_Guide-Online.pdf C. Page 327 - moved to the quarantine isolation network

NEW QUESTION 45

How does FortiGate update FortiNAC about VPN session information?

- A. API calls to FortiNAC
- B. Syslog messages
- C. SNMP traps
- D. Security Fabric Integration

Answer: B

NEW QUESTION 49

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

NSE6_FNC-7.2 Practice Exam Features:

- * NSE6_FNC-7.2 Questions and Answers Updated Frequently
- * NSE6_FNC-7.2 Practice Questions Verified by Expert Senior Certified Staff
- * NSE6_FNC-7.2 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * NSE6_FNC-7.2 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The NSE6_FNC-7.2 Practice Test Here](#)