

# Fortinet

## Exam Questions NSE6\_FNC-7.2

Fortinet NSE 6 - FortiNAC 7.2



### NEW QUESTION 1

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 2

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 3

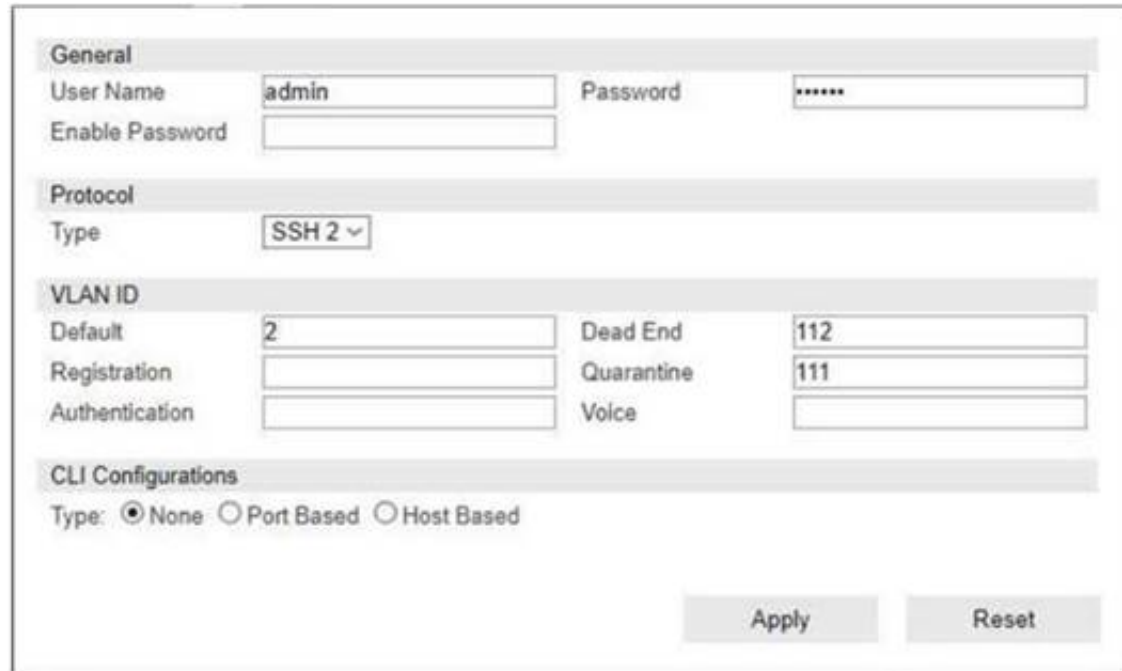
Which two are required for endpoint compliance monitors? (Choose two.)

- A. Custom scan
- B. ZTNA agent
- C. Persistent agent
- D. MDM integration

**Answer: AC**

### NEW QUESTION 4

Refer to the exhibit.



If you are forcing the registration of unknown (rogue) hosts, and an unknown (rogue) host connects to a port on the switch, what occurs?

- A. The host is moved to VLAN 111.
- B. The host is moved to a default isolation VLAN.
- C. No VLAN change is performed.
- D. The host is disabled.

**Answer: A**

#### Explanation:

The exhibit shows a configuration panel where VLAN IDs are specified for different states, such as Default, Registration, and Authentication. When forcing the registration of unknown (rogue) hosts, if an unknown host connects to a port on the switch, the FortiNAC system will move the host to the VLAN designated for Registration. In the exhibit, the VLAN ID for Registration is set to 111, hence the host would be moved to VLAN 111 to undergo the registration process.

### NEW QUESTION 5

What would occur if both an unknown (rogue) device and a known (trusted) device simultaneously appeared on a port that is a member of the Forced Registration port group?

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

D. The port would be administratively shut down.

**Answer:** C

**Explanation:**

When a rogue device connects to a port in the Forced Registration port group, FortiNAC's response is to isolate that device by moving it to a registration captive network. This is part of FortiNAC's state-based control mechanism, where the system acts based on the state of the device (normal, rogue, etc.) and the group or port it is connected to. In this specific scenario, the focus is on the isolation of the rogue device, and the guide does not explicitly detail the simultaneous handling of the normal device.

References: FortiNAC 7.2 Study Guide, State-Based Control section.

**NEW QUESTION 6**

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

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

**Answer:** D

**Explanation:**

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-11e9-81a4-00505692583a/FortiNAC\\_Device\\_Profiler\\_Configuration.pdf](https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/9529d49c-892c-11e9-81a4-00505692583a/FortiNAC_Device_Profiler_Configuration.pdf)

Based on FortiNAC's approach to device profiling and rule evaluation, rogue devices are evaluated against enabled device profiling rules each time they connect. This consistent evaluation ensures that rogue devices are properly classified and handled according to the latest network policies each time they attempt to access the network.

References

FortiNAC documentation on device profiling and rule evaluation.

**NEW QUESTION 7**

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 8**

Which devices would be evaluated by device profiling rules?

- A. Rogue devices, each time they connect
- B. All hosts, each time they connect
- C. Known trusted devices, each time they change location
- D. Rogue devices, only when they are initially added to the database

**Answer:** B

**Explanation:**

Device profiling rules in FortiNAC are used to evaluate and classify rogue devices. These rules can be configured to automatically, manually, or through sponsorship evaluate and classify unknown untrusted devices as they are identified and created. References

? FortiNAC 7.2 Study Guide, page 98

**NEW QUESTION 9**


When FortiNAC is managing FortiGate VPN users, why is an endpoint compliance policy necessary?

- A. To confirm installed security software
- B. To validate the VPN user credentials
- C. To designate the required agent type
- D. To validate the VPN client being used

**Answer:** A

**NEW QUESTION 10**

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 10**

Which agent can receive and display messages from FortiNAC to the end user?

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

**Answer: B**

**Explanation:**

The persistent agent has the ability to display messages on the desktop of an endpoint. These messages can target an individual host, a group of hosts, or all hosts with the persistent agent installed. The messaging options include sending a message content with an optional web address link

**NEW QUESTION 11**

What would happen if a port was placed in both the Forced Registration and the Forced Remediation port groups?

- A. Only rogue hosts would be impacted.
- B. Both enforcement groups cannot contain the same port.
- C. Only al-risk hosts would be impacted.
- D. Both types of enforcement would be applied.

**Answer: B**

**Explanation:**

Reference: <https://docs.fortinet.com/document/fortinac/8.3.0/administration-guide/837785/system-groups>

**NEW QUESTION 12**

Which two of the following are required for endpoint compliance monitors? (Choose two.)

- A. Persistent agent
- B. Logged on user
- C. Security rule
- D. Custom scan

**Answer: AD**

**Explanation:**

DirectDefense's analysis of FireEye Endpoint attests that the products help meet the HIPAA Security Rule.

In the menu on the left click the + sign next to Endpoint Compliance to open it.

Reference: <https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/cg-pci-and-hipaa-compliances.pdf>

<https://docs.fortinet.com/document/fortinac/7.2.2/administration-guide/92047/add-or-modify-a-scan>

**NEW QUESTION 16**

Which agent is used only as part of a login script?

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

**Answer: B**

**Explanation:**

In the context of network access control systems like FortiNAC, a dissolvable agent is typically a piece of software that is executed on the endpoint as part of a login script or when a user accesses a captive portal. It runs once to gather information or enforce policies and then removes itself from the system, hence the term

"dissolvable." References

? FortiNAC documentation on agent deployment and types of agents.

#### NEW QUESTION 21

An administrator is configuring FortiNAC to manage FortiGate VPN users. As part of the configuration, the administrator must configure a few FortiGate firewall policies.

What is the purpose of the FortiGate firewall policy that applies to unauthorized VPN clients?

- A. To deny access to only the production DNS server
- B. To allow access to only the FortiNAC VPN interface
- C. To allow access to only the production DNS server
- D. To deny access to only the FortiNAC VPN interface

**Answer: B**

#### NEW QUESTION 25

View the output.

```
yams.CampusManager INFO :: 2021-07-15 11:37:58:137 :: masterLoaderPID = 10285 nessusLoaderPID = 10372
yams.CampusManager INFO :: 2021-07-15 11:37:58:137 :: sendToNetwork verb Start Processes standbyenabled true inControl true controlServer true
yams.CampusManager INFO :: 2021-07-15 11:37:58:137 :: sendToNetwork() servers = {192.168.10.10, 192.168.10.110, ,
yams.CampusManager INFO :: 2021-07-15 11:37:58:137 :: skip sending verb to 192.168.10.10.
yams.CampusManager INFO :: 2021-07-15 11:37:58:137 :: sendPacket() 192.168.10.10 verb Start Processes retval = null
yams.CampusManager INFO :: 2021-07-15 11:37:58:221 :: sendPacket() 192.168.10.110 verb Start Processes retval = Running - Not In Control
```

Examine the communication between a primary FortiNAC (192.168.10.10) and a secondary FortiNAC (192.166.10.110) configured as an HA pair What is the current state of the FortiNAC HA pair?

- A. The primary server Is running and in control.
- B. The database replication failed.
- C. The secondary server is running and in control.
- D. Fallover from the primary server to the secondary server is in progress.

**Answer: A**

#### NEW QUESTION 30

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 34

Refer to the exhibit.



If a host is connected to a port in the Building 1 First Floor Ports group, what must also be true to match this user/host profile?

- A. The host must have a role value of contractor, an installed persistent agent or a security access value of contractor, and be connected between 6 AM and 5 PM.
- B. The host must have a role value of contractor or an installed persistent agent, a security access value of contractor, and be connected between 9 AM and 5 PM.
- C. The host must have a role value of contractor or an installed persistent agent and a security access value of contractor, and be connected between 6 AM and 5 PM.
- D. The host must have a role value of contractor or an installed persistent agent or a security access value of contractor, and be connected between 6 AM and 5 PM.

**Answer:** D

**Explanation:**

Looking at the provided exhibit which shows the Modify User/Host Profile window, the following must be true for a host to match the user/host profile:

? The host must be connected to a port within the "Building 1 First Floor Ports" group.

? The host must fulfill at least one of the following attributes:

? The host must be connected between the specified times of 6 AM and 5 PM on any day of the week.

The profile specifies that the host can match the profile by having any one of the listed attributes (Role as Contractor, Persistent Agent installed with specific security & access value), and the time condition must also be met. Therefore, the correct answer is D, which includes "or" conditions for the role value and persistent agent and specifies the correct time frame.

**NEW QUESTION 36**

When you create a user or host profile; which three criteria can you use? (Choose three.)

- A. An applied access policy
- B. Administrative group membership
- C. Location
- D. Host or user group memberships
- E. Host or user attributes

**Answer:** CDE

**Explanation:**

Fortinac-admin-operations, P. 391

**NEW QUESTION 37**

In which view would you find who made modifications to a Group?

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

**Answer:** D

**Explanation:**

It's important to audit Group Policy changes in order to determine the details of changes made to Group Policies by delegated users.

Reference: <https://www.lepide.com/how-to/audit-changes-made-to-group-policy-objects.html>

**NEW QUESTION 40**

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 43**

Which two agents can validate endpoint compliance transparently to the end user? (Choose two.)

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

**Answer:** AD

**Explanation:**

Both dissolvable and persistent agents can be used to validate endpoint compliance transparently to the end user. The persistent agent stays resident on the endpoint and performs scheduled scans in the background. The dissolvable agent is a run- once agent that dissolves after reporting its results, leaving no footprint on the endpoint

**NEW QUESTION 48**

.....



## 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](#)**